



governmentattic.org

"Rummaging in the government's attic"

Description of document: Office of Personnel Management (OPM) Inspector General (OIG) Office of Audits Audit Manual (2018) and Office of Investigations Investigation Manual (2015)

Requested date: 2019

Release date: 24-July-2020

Posted date: 18-January-2021

Source of document: Attention: FOIA Request
U.S. Office of Personnel Management
Office of the Inspector General
FOIA Requester Service Center
1900 E Street, N.W.
Room 1H41
Washington, D.C. 20415-7900
Email: foia@opm.gov

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Office of the
Inspector General

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

July 24, 2020

FOIA Request # 2019-03423

This is in response to the Freedom of Information Act (FOIA) request submitted to the U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) in which you requested (1) a copy of the OPM OIG Audit Manual and (2) a copy of the OPM OIG Investigation Manual. For your reference, a copy of your request is attached.

The OPM OIG conducted a thorough search for responsive records and located 879 pages, responsive to both items of your request. Six hundred and ninety-two of these pages are being released in full, and 187 are being released in part. Certain information has been redacted to withhold inter-agency memorandums, letters, or documents that would not be available by law to a party in litigation with the agency, *see* 5 U.S.C. § 552(b)(5); to avoid the unwarranted invasion of personal privacy, *see* 5 U.S.C. §§ 552(b)(6) and (b)(7)(C); to protect either (1) records or information compiled for law enforcement purposes, the release of which would disclose either certain techniques or procedures used in OIG law enforcement investigations or (2) certain operational guidelines, the disclosure of which could reasonably risk circumvention of the law, *see* 5 U.S.C. § 552(b)(7)(E); and to protect records or information compiled for law enforcement purposes, the release of which could reveal the identities of confidential sources of information or employees and/or agents of law enforcement agencies, *see* 5 U.S.C. § 552(b)(7)(F).

Please note that these manuals are intended as training materials and include hypothetical scenarios.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

I trust that this information fully satisfies your request. If you need any further assistance or would like to discuss any aspect of your request, please do not hesitate to contact me at opmoigfoia@opm.gov or (202) 606-1200.

FOIA Request # 2019-03423

Additionally, you may contact the Office of Government Information Services (OGIS) to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, Maryland 20740
Email: ogis@nara.gov
Telephone: 202-741-5770
Toll-free: 1-877-684-6448
Facsimile: 202-741-5769

If you are not satisfied with the response to this request, you may administratively appeal by emailing opmoigfoia@opm.gov.

Please include a copy of your initial request, a copy of this letter, and a statement explaining why you disagree with our decision. You should write "Freedom of Information Act Appeal" in the subject line of the email. Your appeal must be electronically transmitted within 90 days of the date of the response to your request.

Due to COVID-19, the OIG is not accepting Freedom of Information/Privacy Act appeals via standard mail. We apologize for this inconvenience and appreciate your understanding.

Regards,

A handwritten signature in black ink, appearing to read "Andrew Kirby". The signature is stylized with a large "A" and "K".

Andrew P. Kirby
Attorney-Advisor

Attachments

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

AUDIT MANUAL

February 2018

(Pages 1 to 616)

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
SERIES 2000: AUDIT MANUAL

TABLE OF CONTENTS

CHAPTERS

20XX	AUDIT ADMINISTRATION
2000	Introduction (Pages 5 – 7)
2005	Audit Reference Materials (Pages 8 – 24)
2010	Audit Terminology (Pages 25 – 67)
2020	Development of Audit Universe and Agenda (Pages 68 – 84)
21XX	GOVERNMENT AUDITING STANDARDS
2100	Government Auditing Standards (Pages 85 – 87)
2120	Using the Work of a Specialist (Pages 88 – 99)
22XX	GENERAL AUDIT REQUIREMENTS
2205	Quality Control and Quality Assurance (Pages 100 – 217)
2210	Audit Planning (Pages 219 – 255)
2215	Managing the Audit (Pages 256 – 267)
2220	Audit Documentation and Files (Pages 268 – 309)
2230	Auditing Information Systems (Pages 310 – 334)
23XX	SPECIAL AUDIT REQUIREMENTS
2315	Review of Internal Controls (Pages 335 – 353)
2325	Fraud, Illegal Acts, and Abuse (Pages 354 – 375)
2330	Ethical Principles in Government Auditing (Pages 376 – 381)
2335	Independence in Government Auditing (Pages 382 – 392)
24XX	AUDIT REPORTING REQUIREMENTS
2400	Audit Report Preparation and Standards (Pages 393 – 452)
2410	Report Organization and Processing (Pages 453 – 468)
2415	Indexing and Independent Referencing (Pages 469 – 481)
2420	Non-Standard Audit Reports (Pages 482 – 489)

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
SERIES 2000: AUDIT MANUAL

TABLE OF CONTENTS (continued)

CHAPTERS

25XX	AUDIT TECHNIQUES
2505	Sampling Techniques (Pages 490 – 500)
29XX	ADMINISTRATIVE AND OTHER MATTERS
2905	Release of Official Information (Pages 501 – 563)
2910	Office of Audits Subpoena Issuances (Pages 564 – 581)
2915	Requesting Legal Opinions and Interpretations (Pages 582 – 586)
2920	Career Enhancement (Pages 587 – 596)
2925	Travel Policies and Procedures (Pages 597 – 609)
2930	The Audit Report and Receivable Tracking System (Pages 610 – 616)

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2000

Introduction

CHAPTER 2000 - INTRODUCTION

CONTENTS

Page

SECTION 1. GENERAL

1-1. Purpose..... 1

CHAPTER 2000 - INTRODUCTIONSECTION 1. GENERAL

- 1-1. PURPOSE. This Audit Manual establishes uniform policies and procedures to be followed by the Office of Personnel Management (OPM), Office of the Inspector General (OIG), Office of Audits. The Manual serves to implement and supplement generally accepted Government Auditing Standards prescribed by the Comptroller General of the United States and to prescribe and implement the policies and procedures of the OIG's Office of Audits.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2005

Audit Reference Materials

CHAPTER 2005 - AUDIT REFERENCE MATERIALS

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
SECTION 2. REFERENCE MATERIALS	
2-1. General.....	2
2-2. Federal Laws and Regulations.....	2
2-3. U. S. Government Accountability Office Pronouncements.....	6
2-4. Office of Management and Budget Circulars and Bulletins.....	7
2-5. Agency Manuals, Supplements, Circulars, Bulletins, and Transmittal Letters.....	9
2-6. Audit Guides.....	11
2-7. Federal Employees Health Benefits and Life Insurance Program Publications.....	12

SECTION 1. GENERAL

- 1-1. PURPOSE This chapter identifies reference materials to be used by the OIG Office of Audits to examine all government organizations, programs, activities, and functions.

SECTION 2. REFERENCE MATERIALS

2-1. GENERAL The reference materials outlined in this section will be utilized during the normal audit process. The items listed are not all-inclusive; additional reference materials may be required to perform an audit.

2-2. FEDERAL LAWS AND REGULATIONS

- a. Public Law 95-452, Inspector General Act of 1978, October 12, 1978, as amended. <http://www.usda.gov/oig/webdocs/igact1978.pdf>

This Act creates the Offices of Inspector General at federal agencies. The Act also requires federal employees who conduct audits and investigations to comply with the standards established by the Comptroller General for audits of Federal establishments, organizations, programs, activities, and functions and to assure that any work performed by non-federal auditors complies with these standards.

- b. Public Law 101-12, Whistleblower Protection Act of 1989, April 10, 1989.

This Act strengthens and improves the protection of federal employees' rights to prevent reprisals and to help eliminate wrongdoing within the government.

- c. Public Law 89-487, Freedom of Information Act, July 4, 1966, as amended. <http://www.ilsdc.org/attachments/files/184/FOIA-LH.pdf>

This Act clarifies and protects the rights of the public to information.

- d. Public Law 93-579, Privacy Act of 1974, December 31, 1974, as amended. <http://www.ilsdc.org/attachments/wysiwyg/544/PL093-579.pdf>

This Act safeguards an individual's privacy regarding access to records maintained by federal agencies and also establishes a Privacy Protection Study Commission.

- e. Public Law 83-598, Federal Employees Group Life Insurance Act of 1954, August 17, 1954, as amended.

This Act authorizes OPM to make group life insurance available to civilian officers and employees in the federal service.

- f. Public Law 86-382, Federal Employees Health Benefits Act of 1959, September 28, 1959, as amended. <http://www4.law.cornell.edu/uscode/5/pIIIsGch89.html>

This Act furnishes a health insurance program for government employees.

- g. Public Law 86-724, Retired Federal Employees Health Benefits Act, September 8, 1960, as amended.

This Act provides a health insurance program for certain retired employees of the government.

- h. Public Law 101-576, Chief Financial Officers Act of 1990, November 15, 1990. <http://www.llsdc.org/attachments/wysiwyg/544/PL101-576.pdf>

This act reforms general and financial management in the federal government. The major provisions of the Act establish the Office of Management and Budget Deputy Director for Management and Controller to head the Office of Federal Financial Management, and Deputy and Chief Financial Officers in 23 departments and agencies to direct, lead and oversee financial management. This Act requires the Office of Management and Budget, beginning January 31, 1992, to submit to Congress a government-wide financial management status report and a five-year plan. Beginning in FY 2004, this Act requires agencies, each November 15th and annually thereafter, to develop financial statements for the previous fiscal year for each fund and account which performs substantial commercial activities. These financial statements are to be audited by the Inspector General or independent external auditors.

- i. Public Law 97-255, Federal Managers' Financial Integrity Act of 1982, September 8, 1982. <http://www.whitehouse.gov/omb/financial/fmfia1982.html>

This Act requires ongoing evaluations and reports on the adequacy of the systems of internal accounting and administrative control of each executive agency.

- j. Public Law 97-258, Anti-Deficiency Act, September 13, 1982.

This Act contains certain general and permanent laws of the United States related to money and finance.

- k. Public Law 97-365, Debt Collection Act of 1982, September 13, 1982, as amended.

This Act increases the efficiency of government-wide efforts to collect debts owed the United States and to provide additional procedures for the collection of these debts.

- l. Public Law 104-134, Debt Collection Improvement Act of 1996, April 1996. <http://www.fms.treas.gov/debt/regulations2.html>

This Act is within the Omnibus Consolidated Rescissions and Appropriations Act of 1996. This Act provides an opportunity for the Federal government to increase its use of electronic commerce and improve its cash and debt collection.

- m. Public Law 104-156, Single Audit Act of 1996, July 1996, amends the Single Audit Act of 1984. http://www.whitehouse.gov/sites/default/files/omb/assets/about_omb/104-156.pdf

This Act establishes uniform audit requirements for state and local governments receiving financial assistance. The amended act raises the threshold for Single Audit to \$300,000 in Federal assistance.

- n. Public Law 103-62, Government Performance and Results Act of 1993, August 3, 1993. <http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html>

The Government Performance and Results Act of 1993 helps federal agencies plan more effectively and focus on results rather than on processes and program activities. GPRA requires each agency to prepare a five-year strategic plan, and to issue annual performance plans and reports.

- o. 18 USC, Part I, Chapter 93, Section 1905, Disclosure of confidential information generally. <http://www4.law.cornell.edu/uscode/18/1905.html>

This regulation prohibits employees, under the threat of fines or imprisonment, from disclosing any information (such as trade secrets, statistical data, profits, operations, or sources of income, etc.) obtained during the course of their employment, except as provided by law.

- p. Federal Information Security Management Act of 2002, December 17, 2002. http://www.cio.gov/documents/e_gov_act_2002.pdf (See page 48 of 72)

The Federal Information Security Management Act (FISMA) permanently reauthorizes the Government Information Security Reform Act of 2000 (GISRA). GISRA expired November 29, 2002. FISMA seeks to strengthen the information security management infrastructure of the federal government by streamlining GISRA's provisions and requiring that agencies use information security best practices that will ensure the integrity, confidentiality and availability of federal information systems. The Act also seeks to strengthen the role of the National Institute of Standards and Technology in developing and maintaining standards and guidelines for minimum information security controls.

- q. Title 4, Code of Federal Regulations (Accounts).
<http://www.law.cornell.edu/cfr/text/4>

These regulations establish policy for the U.S. Government Accountability Office personnel system, prescribe the federal claims collection standards, and describe the Cost Accounting Standards Board.

- r. Title 5, United States Code.
<http://www.law.cornell.edu/uscode/text/5>

This title contains general and permanent laws of the United States in force as of a stated date.

- r. Title 5, Code of Federal Regulations (Administrative Personnel).
<http://www.law.cornell.edu/cfr/text/5>

These regulations set forth administrative policies and procedures relating to government organizations and employees.

- t. Title 41, Code of Federal Regulations (Public Contracts and Property Management). <http://www.law.cornell.edu/cfr/text/41>

These government-wide property management regulations pertain to property management, information resources management and travel regulation systems.

- u. Title 48, Code of Federal Regulations (Federal Acquisition Regulation).
<http://www.law.cornell.edu/cfr/text/48>

These regulations prescribe the requirements for the procurement of goods and services. In conjunction with specific contract terms, these regulations are the

basis for determining the allowability of costs charged to the health and life insurance programs and other OPM contracts.

2-3. U.S. GOVERNMENT ACCOUNTABILITY OFFICE PRONOUNCEMENTS

- a. Comptroller General of the United States Booklet, Government Auditing Standards, December 2011 Revision. <http://www.gao.gov/assets/590/587281.pdf>

The Comptroller General's "Yellow Book" presents generally accepted government auditing standards (GAGAS) for use by government auditors and nongovernment auditors performing government work. The "Yellow Book" outlines the standards pertaining to the auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports.

- b. Government Auditing Standards, Guidance on GAGAS Requirements for Continuing Professional Education, effective April 2005. [Government Auditing Standards: Guidance on GAGAS Requirements for Continuing Professional Education](#)
- c. Amendments to the 1994 Revision of Government Auditing Standards: Amendment No.1, Documentation Requirements when Assessing Risk at Maximum for Controls Significantly Dependent upon Computerized Information Systems, effective May 1999. <http://www.gao.gov/govaud/agagas1.pdf>
- d. Amendments to the 1994 Revision of Government Auditing Standards: Amendment No.2, Auditor Communication, effective July 1999. <http://www.gao.gov/govaud/agagas2.pdf>
- e. Amendments to the 1994 Revision of Government Auditing Standards: Amendment No.3, Independence, effective October 2002. <http://www.gao.gov/govaud/agagas3.pdf>
- f. General Accounting Office's Standards for Internal Control in the Federal Government, November 1999. <http://www.gao.gov/special.pubs/ai00021p.pdf>

These GAO standards define the minimum level of quality acceptable for internal control in government and provide the basis against which internal controls are to be evaluated.

- g. General Accounting Office's Federal Information System Controls Audit Manual (FISCAM), Volume I: Financial Statement Audits, February 2009.

<http://www.gao.gov/special.pubs/fiscam.html>

The manual is primarily designed for evaluations of general and application controls over financial information systems that support agency business operations. Also, it could be used when evaluating the general and application controls over computer-processed data from agency program information systems, as called for in GAS.

- h. Government Accountability Office's/President's Council on Integrity and Efficiency's, Financial Audit Manual - Volume II, July 2008.

<http://www.gao.gov/assets/80/77097.pdf>

GAO/PCIE task force added new sections and updated existing sections of volume II of the FAM, which provides tools to assist the auditor in complying with audit standards.

2-4. OFFICE OF MANAGEMENT AND BUDGET CIRCULARS AND BULLETINS

<http://www.whitehouse.gov/omb/>

- a. A-11, Preparation and Submission of Budget Estimates.

http://www.whitehouse.gov/omb/circulars_all_current_year_all_toc

This circular provides detailed instructions and guidance in the preparation and submission of annual budgets and related materials.

- b. A-21, Principles for Determining Costs Applicable to Grants, Contracts, and Other Agreements with Educational Institutions.

http://www.whitehouse.gov/omb/circulars_a021_2004/

This circular provides principles for determining the costs relating to research and development, training and other sponsored work performed by colleges and universities under grants, contracts, and other agreements with the federal government.

- c. A-50, Audit Follow-up. http://www.whitehouse.gov/omb/circulars_a050/

This circular provides the policies and procedures to be followed for resolving audit recommendations, monitoring the implementation of promised corrective

action of resolved recommendations, and establishing accounting and collection controls over amounts due the government as the result of claims arising from audits.

- d. A-76, Performance of Commercial Activities.
http://www.whitehouse.gov/omb/circulars_a076_a76_incl_tech_correction/

This circular establishes federal policy regarding the operation of commercial activities. The supplement to the circular sets forth procedures for determining whether commercial activities should be operated under contract with commercial sources or in-house by government personnel.

- e. A-122, Cost Principles for Nonprofit Organizations.
http://www.whitehouse.gov/omb/circulars_a122_2004/

This circular established principles for determining costs of grants, contracts and other agreements with nonprofit organizations.

- f. A-123, Management Accountability and Control, (Revised December 2004)
(Replaces A-123 Internal Control System)
http://www.whitehouse.gov/omb/circulars_a123_rev

This circular prescribes policies and procedures to be followed by executive departments and agencies in establishing, maintaining, evaluating, improving and reporting on internal controls in their program and administrative activities.

- g. A-127, Financial Management Systems. http://www.whitehouse.gov/omb/circulars_a127/

This circular prescribes policies and procedures to be followed in developing, operating, evaluating, and reporting on financial management systems.

- h. A-129, Managing Federal Credit Programs.
http://www.whitehouse.gov/omb/circulars_a129rev/

This circular prescribes policies and procedures for managing federal credit programs and collecting loans and other receivables. The circular sets standards for extending credit, servicing accounts, collecting delinquent receivables, and writing off uncollectible accounts.

- i. A-130, Management of Federal Information Resources.
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

This circular establishes policies for management of federal information resources and includes procedural and analytical guidelines for implementing specific aspects of these policies.

2-5. AGENCY MANUALS, SUPPLEMENTS, CIRCULARS, BULLETINS, AND TRANSMITTAL LETTERS

- a. U.S. Office of Personnel Management's Publications, Periodicals and Operating Manuals. <http://apps.opm.gov/publications/>

These documents provide guidance for administering the Office of Personnel Management. The manual contains basic information with detailed explanations and procedural instructions in separate supplements for selected areas.

- b. U.S. Office of Personnel Management's Federal Employees Retirement System. <http://www.opm.gov/retire/index.asp>

These U.S. Office of Personnel Management publications identify laws, rules, regulations, and instructions pertaining to the Federal Employees Retirement System.

- b. U.S. Office of Personnel Management Supplement, Federal Personnel Manual System Supplement 870-1, Life Insurance. <http://www.opm.gov/retire/pubs/handbook/C083.pdf>

This supplement contains procedures and instructions for the operation of the Federal Employees' Group Life Insurance Program.

- d. U.S. Office of Personnel Management Federal Employees Health Benefits Program Handbook (formerly U.S. Office of Personnel Management Supplement, Federal Personnel Manual System Supplement 890-1, Federal Employees' Health Benefits). <http://www.opm.gov/insure/health/reference/handbook/fehb05.asp>

This handbook contains procedures and instructions for the operation of the Federal Employees' Health Benefits Program.

- e. Financial Management Service of the Fiscal Service, Department of the Treasury Manual, Treasury Financial Manual, Circulars, Bulletins, and Transmittal Letters. <http://fms.treas.gov/index.html>

These documents provide fiscal management instructions for the guidance of departments and agencies of the Federal Government.

- f. Retirement and Insurance Group Publications, and Other Policies and Procedures. <http://www.opm.gov/retire/pubs/pamphlets/index.asp>
<http://www.opm.gov/retire/pubs/handbook/hod.htm>

These documents provide information on policies and procedures to be followed by Retirement Services and the Healthcare and Insurance Office.

- g. Benefits Administration Letters. <http://www.opm.gov/retire/pubs/bals/index.asp>

The U.S. Office of Personnel Management has Government-wide responsibility and oversight for Federal benefits administration. These pages contain the *Benefits Administration Letters (BALs)* used for program administration. The *BALs* provide guidance to agencies on various aspects of Federal benefits administration.

- h. Retirement and Insurance Group Manual, Policy Guidelines on the Disposition of Civil Service Retirement Overpayments, November 1987.

These guidelines are intended to ensure that Civil Service Retirement overpayments are handled in an efficient and effective manner.

- i. United States Government Printing Office, United States Government Printing Office Style Manual, 2008. <http://www.gpoaccess.gov/stylemanual/browse.html>

This manual is intended to standardize the form and style of Government printing.

- j. U.S. Office of Personnel Management Guide, The Office of Personnel Management Good Writers' Guide, July 26, 1993.

This brief guide is to be used in conjunction with the OIG Style Manual for writing reports and correspondence.

- k. U. S. Office of Personnel Management's Financial Policies.
<http://theo.opm.gov/policies/financial.asp>

These financial policy directives and financial information bulletins provide financial guidance to ensure consistent application throughout the agency.

- l. U. S. Office of Personnel Management's Information Technology Guidance, Plans, Policies, and Procedures. <http://theo.opm.gov/policies/it.asp>

The policies and procedures related to IT security, web accessibility, use of government equipment, and guidance and handbooks provides guidance to ensure consistent application throughout the agency.

2-6. AUDIT GUIDES

- a. Council of the Inspectors General on Integrity and Efficiency Pamphlet, Quality Standards for Federal Offices of Inspector General, August 2012.
<https://www.ignet.gov/sites/default/files/files/Silver%20Book%20Revision%20-%208-20-12r.pdf>

This document contains quality standards for the management, operation and conduct of the federal Offices of Inspector General who are members of the Council of the Inspectors General on Integrity and Efficiency.

- b. Council of the Inspectors General on Integrity and Efficiency Pamphlet, Office of Inspector General Quality Standards for Inspection and Evaluation, January 2012.
<https://www.ignet.gov/sites/default/files/files/committees/inspect-eval/iestds12r.pdf>

This document contains standards to be used within the Offices of Inspector General community for inspections programs.

- c. Control Objectives for Information and Related Technology (COBIT).
<http://www.isaca.org/cobit.htm>

COBIT has been developed by the Information Systems Audit and Control Association (ISACA) as a generally applicable and accepted standard for good IT security and control practices that provides a reference framework for management, users, and information systems audit, control, and security practitioners.

- d. National Institute of Standards and Technology (NIST).
<http://csrc.nist.gov/index.html>

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. One of NIST's laboratories, the Information Technology Laboratory (ITL) conducts research and develops test methods and standards for emerging and rapidly changing information technologies. Within the ITL is the Computer Security Division which raises awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies.

- e. General Accounting Office Booklet, Assessing the Reliability of Computer-Processed Data. October 2002 (Supplement to the 1994 Revision of Government Auditing Standards). <http://www.gao.gov/new.items/d03273g.pdf>

This guide provides information to assist in assessing the reliability of computer-based data. It also provides a conceptual framework to expedite job performance and addresses standards for assessing internal controls and compliance with applicable laws and regulations.

- f. Department of Defense Contract Audit Agency Manual DCAAM 7640.1, Contract Audit Manual. <http://www.dcaa.mil/cam.htm>

This manual prescribes DCAA auditing policies and procedures and furnishes guidance in auditing techniques.

2-7. FEDERAL EMPLOYEES HEALTH BENEFITS AND LIFE INSURANCE PROGRAM PUBLICATIONS

- a. Contracts.
 - 1. Fee-for-Service Plans.
<http://www.opm.gov/insure/health/reference/handbook/fehb05.asp#top>
 - (a) Service Benefit Plan Contract No. 1039 administered by Blue Cross and Blue Shield Association.
 - (b) Employee Organization Plan Contracts (for each Plan).
 - 2. Prepaid Plans (Comprehensive Medical Plans/Health Maintenance Organizations).
<http://www.opm.gov/insure/health/reference/handbook/fehb05.asp#top>

- (a) Group Practice Plan Contracts (for each Plan).
 - (b) Individual Practice Plan Contracts (for each Plan).
 - (c) Mixed Model Plan Contracts (for each Plan).
 3. Point of Service.
<http://www.opm.gov/insure/health/reference/handbook/fehb05.asp#top>

Some fee-for-service plans and HMOs offer a point of service product. Subscribers have the choice of using a designated or non-designated network of providers at an additional cost.
 4. Retired Employees Health Benefits Plan Contract No. GC-68, 000 administered by Aetna Life Insurance Company.
 5. Group Life Insurance Plans.
 - (a) Life Insurance Plan Contract Group Policy No.17000-G administered by Metropolitan Life Insurance Company.
 - (b) Life Insurance Plan Contract Group Policy No. 900-G for Federal employees insured under certain employees beneficial associations administered by Shenandoah Life Insurance Company.
- b. Benefits and Rates.
1. Brochures.
 - (a) Federal Employees Health Benefits Program Brochures (for each Plan). (Form RI XX-XXX) <http://www.opm.gov/insure/03/html/brochure.asp>
 - (b) FEGLI Program Booklet. (Booklet RI 76-21)
<http://www.opm.gov/insure/life/reference/federal/index.asp>
 - (c) Uniform Plan Basic Plus Major Medical Coverage Benefits (RETFE) Brochure Form RI 78-5 Revised May 1989.

2. U.S. Office of Personnel Management's Guide to Federal Employees Health Benefits Plans for Federal Civilian Employees. (Open Season). <http://www.opm.gov/insure/health/index.asp>
 3. U.S. Office of Personnel Management's 20XX FEHB Premiums for Non-Postal and Postal Plan Premium Rates for the Federal Employees Health Benefits Program. <http://www.opm.gov/insure/>
- c. Enrollment.
1. U.S. Office of Personnel Management Report, Health Benefits Recap Semiannual Headcount Health Benefits by Plan Codes and Payroll Offices as of ____.
 2. U.S. Office of Personnel Management Report, (Table 1) Summary of FEHBP Enrollment For the Quarter Ended ____ (for each Plan).
 3. U.S. Office of Personnel Management Report, (Table 2) Enrollment by Payroll Office for Period Ending ____ (for each Plan).
 4. U.S. Office of Personnel Management Report, (Table 3) Summary of Open Season Transactions (for each Plan).
 5. U.S. Office of Personnel Management Report, Federal Employees Health Benefit Program Summary of Enrollment as of 12/20XX as Reported on Carriers' Table 1 Total Enrollment.
 6. U.S. Office of Personnel Management Report, REHB Enrollment by Payroll Office (RETFE).
- d. Insurance and Financial Reports.
1. U.S. Office of Personnel Management Report, Federal Employees Health Benefits Program Summary of Carrier Financial Data January 1, 20XX-December 31, 20XX.
- e. Procedures.
1. U.S. Office of Personnel Management Letter to Carriers, 20XX Rate Instructions Community-Rated Plans (for each Plan).

2. U.S. Office of Personnel Management Letter to Carriers, Reconciliation Instructions for 20XX Rates Community-Rated Plans (for each Plan).
3. Blue Cross and Blue Shield Publications. <http://www.fepblue.org/index.html>
<http://www.bluecares.com/>
 - a. Blue Cross and Blue Shield, Provider Directory. <http://provider.bcbs.com/>
 - b. Blue Cross and Blue Shield, FEP Administrative Manual.
 - c. Blue Cross and Blue Shield, Financial Policies and Procedures Bulletins.
 - d. Blue Cross and Blue Shield, Federal Employee Program Benefits Training Manual 20XX.
- f. Other Audit Reference Guides.
 1. Code It Right, an on-line coding tool provided by Decision Health – offers access to Dorland’s Medical Dictionary, Physicians Current Procedural Terminology (CPT), Internal Classification of Diseases, Clinical Modification (ICD.9.CM and ICD.10.CM), and Healthcare Common Procedure Coding System (HCPCS).

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2010

Audit Terminology

CHAPTER 2010 - AUDIT TERMINOLOGY

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. AUDIT TERMINOLOGY	
2-1. General.....	2
2-2. Terms.....	2
2-3. Acronyms.....	36

CHAPTER 2010 - AUDIT TERMINOLOGYSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides a comprehensive list of audit terms designed to assist the OIG Office of Audits staff when auditing OPM operations and programs.
- 1-2. POLICY. All OIG professional staff members will become familiar with current audit terminology prior to beginning an audit.

SECTION 2. AUDIT TERMINOLOGY

2-1. GENERAL. This section contains a list of words, phrases, acronyms, and definitions relevant to OPM operations and programs. It is to be used as a reference when performing audits.

2-2. TERMS.

A Abuse. Furnishing excessive services to beneficiaries; or performing what may be considered improper practices, none of which involves noncompliance with laws and regulations. Also willful misrepresentation by an individual of a fact inflicting damage on another person.

Accounting periods. Time periods used by a business concern to report operating results and changes in assets and liabilities. All FEHBP carriers account for their FEHBP operations on a calendar year (January 1 through December 31) basis. The federal government and some other benefit programs (i.e., FEGLI and the FLTCIP) report on a fiscal year (October 1 through September 30) basis.

Accounting system. The methods and records used to identify, assemble, classify, analyze, record, and report on an entity's transactions and to maintain accountability for the related assets and liabilities. This is one element of an entity's internal control structure.

Accrual basis of accounting. The basis of accounting under which revenues are recorded when earned and expenditures are recorded as soon as they result in liabilities for benefits received, notwithstanding that the cash receipts or the cash disbursements may take place in another accounting period. The FEHBP carriers' annual accounting statements are on the accrual basis.

Accrued claims reserve. A liability account for insurance carriers representing benefits received by subscribers during the accounting period, but not yet paid by the carrier.

Accrued subscription income. Premiums earned by insurance carriers during the accounting period, but not yet paid by OPM.

Additional optional life insurance. Encompasses three additional life insurance options an employee may elect if they are already enrolled in the Basic life insurance option. Employees are responsible for paying the full cost of the optional insurance.

Ad Hoc. Being concerned with a particular end or purpose, e.g., an ad hoc committee established to handle a specific subject.

Adjudication. The processing of health and life insurance claims in accordance with law and/or contract provisions.

Adjusted community rate (ACR). A community rate that has been adjusted for expected utilization of a specific group. This is a prospective rate and cannot be retroactively revised to reflect actual experience or costs of the group.

Administrative expenses. Allocable, allowable and reasonable expenses incurred in the adjudication of subscriber benefit claims or incurred in the carrier's overall operation of the business.

Administrative reserve. As provided by FEHB law, an amount not to exceed 1 percent of premium payments set aside to pay OPM's cost for administering the health insurance program. Each year, the funds not needed for administrative expenses are credited to the carrier's contingency reserve.

Adverse opinion. An auditor's negative opinion rendered when the auditor determines that the financial position, results of operations, or cash flows of the entity are not fairly presented in conformity with generally accepted accounting principles or the contract terms.

Affordable Care Act (ACA). Health care law passed in 2010 that establishes a multitude of new health care standards. These include the coverage of dependents until age 26, minimum benefit levels for insurance plans, and establishes the marketplace exchanges that allow individual and small business customers to purchase insurance plans. These exchanges may be administered by the federal government or the individual states.

Allocable. A contract cost that is chargeable to one or more cost objectives based on benefits received or other equitable relationship.

Allotment. An authorization by the head of an agency or other authorized employee to subordinate organizations to incur obligations within a specified amount.

Allowable. A contract cost that is reasonable, allocable, meets appropriate standards and regulations, and is in compliance with the terms of the contract.

Alternative Internal Control Review. As defined by OMB Circular No. A-123 Revised, an alternative internal control review is a process which allows the use of existing management reporting and review processes, and management and consultant studies as a substitute for the review otherwise required under the Federal Managers' Financial Integrity Act.

American Institute of Certified Public Accountants (AICPA). The AICPA is an association of members who hold a valid and unrevoked certified public accountant certificate. The AICPA issues authoritative and binding pronouncements that establish professional standards regulating the accounting and auditing profession.

American Society for Public Administration (ASPA). A non-profit, educational and professional organization established to improve management in public service through the exchange, development and dissemination of information about public administration.

Annual accounting statements. The annual statement of financial operations and supporting schedules required by OPM for health and life insurance contracts. These statements are the basis for the audits performed by the Experience-Rated Audits Group. The Special Audits Group also reviews them as part of their audits of the other insurance related contracts (non-FEHBP).

Annuitant. A former federal or District of Columbia employee who has retired on an annuity (pension) under the Civil Service Retirement System (CSRS), the Federal Employees' Retirement System (FERS) and/or other qualifying retirement systems.

Application Controls. Application controls relate to the transaction and standing data pertaining to each computer-based application system and are therefore specific to each such application. The objectives of application controls, which may be manual or programmed, are to ensure the completeness and accuracy of the records and the validity of the entries made therein resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch totals, encryption of data transmitted, etc.

Application programmer. A computer programmer who writes software programs that perform a service or relate to a user's work, such as inventory control or payroll.

Apportionment. A distribution by the Office of Management and Budget of amounts available for allotment in an appropriation or fund account for specified time periods (usually quarters), activities, projects, objects or a combination thereof.

Appropriated funds. Funds authorized by the U.S. Congress for specified purposes against which apportionments, allotments, and obligations may be incurred and subsequent expenditures made.

Appropriation. An authorization by the U.S. Congress that permits a federal agency to incur obligations and have payments made by the U.S. Treasury for specified purposes.

Armed Services Board of Contract Appeals (ASBCA). An administrative board that adjudicates contract disputes between the Department of Defense and its contractors. The ASBCA has been designated by OPM to hear appeals associated with contract disputes between OPM and the FEHBP carriers.

Association of Government Accountants (AGA). A national organization of individuals who are interested in improving financial management practices of federal, state and local governments.

Attributes sampling. The sampling process used to estimate the number of times a characteristic or situation occurs in a population. It is usually expressed as a percentage of the total. Attributes can be counted, but not measured.

Attrition. A reduction in numbers usually as a result of resignation, retirement, or death.

Audit methodology. The methods and techniques used to gather and analyze data needed to accomplish the audit objectives.

Audit objective. A statement of the purpose of the audit; the questions the audit will answer.

Audit program. A document listing the steps and procedures to be followed in conducting audits and preparing audit reports.

Audit resolution (AR). The organization within OPM which resolves audit findings.

Audit results. The conclusions reached as a consequence of performing the audit.

Audit scope impairments. Internal and external factors that can restrict the auditors' ability to render objective opinions and conclusions.

Audit software. Computer programs designed to assist in examining and testing clients' accounting records. Different audit software packages accomplish varying objectives. Some packages assist in gathering evidence, conducting analytical tests, sampling data, evaluating internal control, documenting the audit, scheduling the audit, printing exception reports (e.g., employee salary exceeding a prescribed limit), preparing audit reports, sending out confirmations and management letters.

Audit team. The individuals assigned to perform a specific audit.

Auditing Standards Board (ASB). The senior technical body of the American Institute of Certified Public Accountants designated to issue pronouncements on auditing matters.

Auditor's opinion. A statement in the audit report of the auditor's position on whether the financial information of the entity is presented fairly, in all material aspects, in conformity with generally accepted accounting standards.

Automatic data processing (ADP). A reference to the use of computers to process data. This term is often interchanged with Electronic Data Processing (EDP)

B Backups. An alternate system, device, file or facility that can be used in the event of a malfunction or loss of data.

Bid and proposal (B&P) cost. The cost incurred for preparing, submitting, and supporting bids and proposals (whether or not solicited) on potential government or nongovernment contracts.

BlueCross (BC). A confederation of independent, the majority for profit corporations, that provides inpatient hospital care coverage.

BlueCross BlueShield Association (BCBS). The organization that owns the BlueCross and BlueShield trademark. This organization contracts with OPM to provide the Governmentwide Service Benefit Plan to enrolled federal subscribers. The association provides program guidance and performs certain centralized management functions for the FEHB. Health benefits are provided by local BlueCross and BlueShield member plans.

BlueShield (BS). A confederation of independent, the majority for profit corporations, that provides doctor, outpatient hospital and other medical benefits coverage.

Brochure. An FEHB or FEGLI booklet describing health and life insurance benefits, exclusions, and limitations offered by each health and life insurance carrier.

Browser. Client based software program providing capability to view Internet resources.

Burden. The amount added to the price of goods and services to account for indirect costs. Burden is usually synonymous with Overhead and/or General and Administrative cost.

C Capitation. See per member per month revenue requirement.

Carrier. A voluntary association, corporation, partnership or other nongovernmental organization which is lawfully engaged in providing, paying for or reimbursing the costs of health services and life insurance under group insurance policies or contracts, medical or hospital service agreements, membership or subscription contracts or similar group arrangements.

Cash basis of accounting. The basis of accounting under which revenues are recorded when received in cash and expenditures are recorded when paid in cash.

Central Personnel Data File (CPDF). An OPM database which contains general personnel data for most government employees.

Central processing unit (CPU). The part of a computer that controls the interpretation and execution of instructions.

Certified Fraud Examiner (CFE). A credential awarded by the Association of Certified Fraud Examiners (ACFE). It combines knowledge of complex financial transactions with an understanding of methods, law, and how to resolve allegations of fraud.

Certified Information Systems Auditor (CISA). A globally recognized certification in the field of audit, control and security of information systems.

Certified Internal Auditor (CIA). A globally recognized certification for internal auditors and is a standard by which individuals may demonstrate their competency and professionalism in the internal audit field.

Certified Public Accountant (CPA). The statutory title of qualified accountants in the United States who have passed the Uniform Certified Public Accountant Examination and have met additional state education and experience requirements for certification as a CPA.

Chart of Accounts. A list of ledger account names and associated numbers arranged in the order in which they normally appear in the financial statements.

Chief Executive Officer (CEO). The CEO is the principal individual responsible for the activities of a company, organization or in government.

Chief Financial Officer (CFO). The CFO is the officer in government or a corporation responsible for managing the funds, signing the checks, keeping the financial records, and financial planning of the organization or company.

Chief Information Officer (CIO). The CIO is the officer in government or a corporation responsible for managing all information systems operations.

Civil act. An illegal act for which penalties do not include incarceration. Penalties may include monetary payments and corrective actions.

Civil Service Retirement System (CSRS). CSRS has provided retirement, disability, and survivor benefits for most civilian employees in the United States federal government since 1920. Upon the creation of a new Federal Employees Retirement System (FERS) in 1987, those newly hired after that date cannot participate in CSRS. CSRS continues to provide retirement benefits to those eligible to receive them.

Claims processing system. The system developed by each health and life insurance carrier to adjudicate health benefit and life insurance claims.

Coaching notes. Within TeamMate, any questions or comments are created and contained in coaching notes. Coaching notes are paperless questions or comments supervisors may want to write to an auditor about his or her TeamMate audit work.

Code of Federal Regulations (CFR). The codification of the rules published in the Federal Register by the executive departments and agencies of the federal government.

Coinsurance. A cost-sharing arrangement whereby an enrollee/subscriber assumes a portion of the costs of covered charges.

Combined Federal Campaign (CFC). The annual federal government charity drive. The CFC is administered by OPM.

Commercial Off-The-Shelf software (COTS). Commercially available specialized software designed for specific applications (such as legal or medical billing, chemical analysis, and statistical analysis) that can be used with little or no modification.

Committee of Sponsoring Organizations (COSO). In the midst of the Savings and Loan scandals of 1985, the National Commission on Fraudulent Reporting, also known as the Treadway Commission, was created. Its major objective was to identify causal factors of fraudulent financial reporting and make recommendations. COSO was formed and conducted a review, which resulted in a report recommending a project to provide practical, broadly accepted criteria for establishing internal control and evaluating effectiveness. The COSO project resulted in the 1992 study titled “Internal Control – Integrated Framework”, which provided a core definition for internal controls.

Community rate. A rate of payment based on a per member per month capitation rate or its equivalent that applies to any subscriber group of a comprehensive medical plan that purchases the same level of benefits.

Community-rated plan. A health benefits provider that establishes fully-insured rates for different employer groups based on one of three accepted community-rating methodologies:

- 1) Traditional Community Rating (TCR);
- 2) Community-Rating-by-Class (CRC); and
- 3) Adjusted Community Rating (ACR).

Note: Beginning in 2013 (in 2012 for Pilot Program plans), FEHBP community-rated plans that develop FEHBP rates using CRC or ACR are required to perform a Medical Loss Ratio (MLR) calculation. Plans that use TCR due to state mandates will not be subject to the MLR requirements.

Community-Rating-by-Class (CRC). CRC is a community-rating methodology that uses the cost of providing benefits to the entire community to develop a standard per-member-per-month (or capitation) rate. These standard capitation rates, based on benefit levels, are used as the starting point in the rate development. The standard capitations are adjusted by conversion factors which are determined based on the specific demographics of a group (i.e., contract mix and average family size). The capitation rates will also be adjusted by an age/sex factor that is based on the actual age and gender makeup of a specific group. Further, a factor based on the industry classification of the specific group can be applied.

Competent evidence. Evidence that is valid and reliable.

Compliance audit. An audit that is conducted to determine whether the organization has adhered to contracts, policies, procedures, laws, and regulations.

Compliance tests. Tests made by auditors to determine the extent to which established procedures and controls are functioning as intended.

Compound Interest. Interest calculated from the total of the original principal plus accrued interest.

Comprehensive medical plan (CMP). A prepaid medical plan that provides a full range of health care coverage in exchange for a monthly fixed fee. This type plan is available to subscribers living within a limited geographical area where health care is provided by designated plan physicians, hospitals, and other providers. There are three types of CMP's: group practice plans; individual practice plans; and mixed model plans. Also known as Health Maintenance Organizations.

Computer Assisted Audit Techniques (CAAT). Computer Assisted Audit Techniques are ways in which the auditor may use the computer in a computerized information system to gather, or assist in gathering, audit evidence.

Computer contingency plan. Management policy and procedures designed to maintain or restore computer operations in the event of emergencies, system failure or disaster.

Condition. The factual evidence which the auditor found in the course of the examination (what does exist).

Confidence level. This relates to the probability that a statistical sample will represent the true population average. The confidence level indicates the risk the auditors are willing to take in the sample selection. For example, in choosing a 95 percent confidence level, the auditors believe their estimate will be correct 95 percent of the time.

Congressional, Legislative & Intergovernmental Affairs Office (CLA). This office advocates for the legislative and policy priorities of the Director and the Administration. CLA educates, responds to, interacts with, and advises Congress and State, local, and tribal officials on Federal human resources management policy. CLA counsels and advises the Director and other OPM officials on policy, and congressional and legislative matters.

Consolidated Business Information System (CBIS). CBIS is OPM's current financial system for tracking the Revolving Funds and Salaries and Expenses accounting activity.

Contingency reserve. The statutory reserve under the FEHB which provides that an amount not to exceed 3 percent of premium payments be set aside by OPM. OPM regulates the preferred minimum amount that must be kept in the reserve for each carrier and the disposition of amounts that exceed the minimum.

Contracting Officer. An OPM official who enters into and administers contracts.

Control environment. The overall attitude, awareness, and actions of management concerning control and the emphasis given to it. This is one element of an entity's internal control structure.

Control Objectives for Information and Related Technology (COBIT). COBIT has been developed by the Information Systems Audit and Control Association (ISACA) as a generally applicable and accepted standard for good IT security and control practices that provides a reference framework for management, users, and information systems audit, control, and security practitioners.

Control risk. The risk that a material misstatement could occur and not be prevented or detected on a timely basis by the control structure policies and procedures.

Conversion rights. The right of an enrollee whose health insurance enrollment ends, for any reason other than voluntary cancellation, to convert, without evidence of insurability, to a nongroup health benefits contract offered by the insurance carrier.

Coordination of benefits. The practice of allocating health benefits payments for a subscriber who is covered by more than one insurance carrier. Coordination of benefit rules limit the combined benefits to no more than 100 percent of charges.

Cost Accounting Standards (CAS). Government contract cost accounting rules, regulations and standards developed by the Cost Accounting Standards Board. New statutes will require application to civilian agencies when implemented by regulations.

Cost Center. Non-revenue-producing element of an organization, where costs are separately figured and allocated, and for which someone has formal organizational responsibility.

Cost-of-living adjustment. An increase in an annuity based on the increase in the consumer price index.

Cost-plus-fixed-fee contract. A cost-reimbursement contract that provides for payment to the contractor of a negotiated fee that is fixed at the inception of the contract. The fixed fee does not vary with actual cost, but may be adjusted as a result of changes in the work to be performed under the contract. This contract type permits contracting for work that might otherwise present too great a risk to contractors and provides little incentive to control costs.

Cost proposal. A detailed statement of costs proposed in response to a Request for Proposal. On occasion, the OIG is requested by OPM's contracting office to review cost proposals to determine if they reflect a fair cost.

Cost submission. This is a BCBS form used by local BCBS plans to claim administrative expenses charged to the FEHBP.

Council of the Inspectors General on Integrity and Efficiency (CIGIE). Statutorily established as an independent entity within the executive branch by the "[The Inspector General Reform Act of 2008](#)," P.L. 110-409 to:

- address integrity, economy, and effectiveness issues that transcend individual Government agencies; and
- increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

Prior to the establishment of the CIGIE, the Federal Inspectors General operated under the auspices of two councils, The President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) from the time they were established by [Executive Order 12805](#), May 11, 1992 until the signing of P.L. 110-409.

Criminal act. An illegal act for which incarceration, as well as other penalties, is available if the government obtains a guilty verdict.

Criteria. The standards, measures, or expectations used in making an evaluation and/or verification (what should exist).

Current file. An audit working paper file consisting of materials that support audit conclusions and documents the audit work performed.

Current Procedural Terminology (CPT). A coding system for reporting medical services and procedures performed by physicians.

D Data Warehouse. Data warehouses organize and collect data into databases that can be searched and mined (analyzed) for information. These collections of data serve as the basis for crucial business decisions.

Deductible. The amount of a covered health expense that the subscriber must incur before the insurance plan pays any portion of the covered health benefit.

Deobligation. A downward adjustment of previously obligated funds.

Detection risk. The risk that the auditors will not detect a material misstatement that exists in a financial statement assertion (existence or occurrence, completeness, rights and obligations, valuation and allocation, presentation and disclosure).

Direct cost. Any cost that can be identified specifically with a particular cost objective.

Disallowed cost. A questioned cost that management agrees should not be charged to the government.

Disclaimer of opinion. An auditor's statement that says the auditors "do not express" an opinion regarding the financial statements.

Discovery sampling. A type of sampling where the audit objective is to locate at least one occurrence of a particular event or error.

Distributed computer network. A computer network where some or all of the processing, storage, and control functions are dispersed among sites; sites are typically geographically dispersed.

Dollar unit sampling. A sampling technique where each dollar is a sampling unit. The item (e.g., inventory item, receivable) associated with the dollar selected is subject to audit procedures.

Domain Name. A unique naming system which identifies an Internet site.

Double coverage. A condition when an individual is covered or entitled to benefits under more than one insurance policy.

Due Professional Care. The application of the care and skill expected of a reasonably prudent and competent auditor in the same or similar circumstances.

E Effect. The risk or exposure the auditee organization and/or others encounter because the condition is not the same as the criteria (the impact of the difference).

E-mail. Electronic mail or text messages sent from one individual to another over a computer network.

Employee organization plans. Associations or other organizations of employees which sponsor health benefits plans approved by OPM. These plans are available only to employees who are, or who become members of the sponsoring organization.

Employee Services (ES). ES provides oversight for programs and benefits regarding Federal employees. ES offers policy direction and leadership in designing, developing, and implementing Government-wide human resources systems and programs for

recruitment, pay, leave, performance management and recognition, employee development, work/life/wellness programs, and labor and employee relations.

Entrance conference. An introductory meeting between the OIG audit staff and key auditee officials held at the beginning of an audit. At this meeting, the OIG auditor-in-charge introduces OPM attendees, explains the OIG function including audit authority, identifies the purpose, objectives and anticipated length of the audit, defines the audit process, and outlines the audit reporting process.

Errors. Unintentional noncompliance with applicable laws and regulations and/or misstatements or omissions of amounts or disclosures in financial statements.

Event cycles. The processes used to initiate and perform related activities, create the necessary documentation, and gather and report related data. Identification of the event cycles is the first step in conducting an internal control review.

Evidence. The data and information the auditors obtain during audit fieldwork to document findings and support opinions and conclusions. This information may be categorized and described as: physical evidence (obtained by direct inspection or observation); documentary evidence (created information); testimonial evidence (obtained from others through statements); or analytical evidence (includes computations, comparisons, reasoning, etc.).

Exit conference. The official closeout meeting for the audit between the OIG and the auditee. At the exit conference, the OIG auditor-in-charge discusses findings, conclusions, and recommendations of the audit staff, outlines whether further audit work may be required, explains the audit report process and makes favorable comments on specific auditee operations including cooperation and courtesies. This meeting concludes with questions, answers and/or comments.

Experience rate. A rate for a given group which is the product of that group's actual paid claims, administrative expenses, retentions and estimated claims incurred but not reported, adjusted for benefit modifications, utilization trends, and trends in the economy.

Experience-rated plan. A health benefits plan which establishes different rates for different groups within a community, based on the costs of providing services to these distinguishable groups.

Explanation of benefits or explanation of payments (EOB) or (EOP). A form mailed by the insurance carrier to the subscriber explaining the carrier's determination of payable benefits for claims submitted.

F Federal Acquisition Regulation (FAR). A regulation which prescribes the requirements for the procurement of goods and services by government agencies. In conjunction with

specific contract terms, these regulations are the basis for determining the allowability of costs charged to the health and life insurance programs and other OPM contracts.

Federal Employee Program (FEP). A term used by the BlueCross BlueShield Association to identify the Service Benefit Plan administered by them under the FEHBP.

Federal Employee Program Director's Office. A division of the BCBS Association located in Washington, DC. It provides centralized management for the Governmentwide Service Benefit Plan administered by the Association. The FEP Director's Office coordinates the administration of the contract with the BCBS Association, member BCBS plans, and OPM.

Federal Employees Dental and Vision Program (FEDVIP). This program allows dental and vision insurance to be purchased on a group basis to eligible Federal and Postal employees, retirees, and their eligible family members.

Federal Employees Group Life Insurance program (FEGLI). A fringe benefit program that provides life insurance to federal employees. FEGLI is administered by the Metropolitan Life Insurance Company under contract to OPM.

Federal Employees Health Benefit Acquisition Regulation (FEHBAR). A regulation which describes the method by which OPM implements and supplements the Federal Acquisition Regulation.

Federal Employees Health Benefit Program (FEHBP). A fringe benefit program that provides health insurance to federal employees, their eligible family members, and annuitants.

Federal Employees Retirement System (FERS). FERS is a retirement plan that provides benefits from three different sources: a Basic Benefit Plan, Social Security and the Thrift Savings Plan. This program became effective on January 1, 1987. Since that time, new Federal civilian employees who have retirement coverage are covered by FERS.

Federal Executive Institute (FEI). A facility located in Charlottesville, Virginia that is used by OPM to train government executives.

Federal Information Security Management Act (FISMA). FISMA permanently reauthorizes the Government Information Security Reform Act of 2000 (GISRA). GISRA expired November 29, 2002. FISMA seeks to strengthen the information security management infrastructure of the federal government by streamlining GISRA's provisions and requiring that agencies use information security best practices that will ensure the integrity, confidentiality and availability of federal information systems.

The Act also seeks to strengthen the role of the National Institute of Standards and Technology in developing and maintaining standards and guidelines for minimum information security controls.

Federal Information Systems Controls Audit Manual (FISCAM). FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards.

Federal Investigative Services (FIS). FIS is responsible for helping to ensure that the Federal Government has a workforce that is worthy of the public trust by providing both suitability and security clearance determinations.

Federal Long Term Care Insurance Program (FLTCIP). This program provides long term care insurance to help pay for costs of care when enrollees need help with activities they perform every day, or you have a severe cognitive impairment, such as Alzheimer's disease.

Federal Managers Financial Integrity Act (FMFIA). This Act requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency, and for other purposes.

Federal Procurement Data System (FPDS). A government-wide procurement reporting system that gives the U.S. Congress, executive branch and the private sector needed information regarding Federal procurement.

Federal Procurement Regulations (FPR). These regulations govern the "acquisition process" by which the government purchases ("acquires") goods and services.

FEDVIP enrollment portal (BENEFEDS). A website where eligible Federal and Postal employees, retirees, and their eligible family members can enroll in FEDVIP.

Fee-For-Service plans. An insurance plan whereby the subscriber is reimbursed on the basis of the fee charged by the medical provider for the services rendered.

FEHBP Data Warehouse. OIG collects data from select health insurance carriers and pharmacy benefit managers for analytical purposes and stores this data in a data warehouse system. Auditors, investigators, and others can use the data warehouse to search for fraud, waste, and abuse in the FEHBP.

FEP Administrative Manual. A manual issued by the BCBS Association which provides instructions to local BCBS plans regarding procedures for administering the Service Benefit plan under the FEHBP.

Finalization. When audit working papers and audit reports are completed, signed off, and no need for changes, the file is finalized. A unique feature of TeamMate, finalization of an audit occurs when the option “read only” is checked and no changes are permitted to the audit. Finalization of an audit provides the option of retaining or removing all signoff dates and edits. Finalization provides the option of retaining or removing all coaching notes.

Financial Accounting Standards Board (FASB). An organization within the American Institute of Certified Public Accountants responsible for developing standards for financial reporting.

Financial audits. An audit of an entity's financial statements to determine whether the financial statements present fairly the financial position, results of operations, and cash flows or changes in financial position in accordance with generally accepted accounting principles. These audits also determine whether the entity has complied with laws and regulations for those transactions and events that may have a material effect on the financial statements. Financial related audits include: determining whether financial reports and related items, such as elements, accounts, or funds are fairly presented; whether financial information is presented in accordance with established or stated criteria; and whether the entity had adhered to specific financial compliance requirements.

Financial Policies and Procedures Bulletins. These bulletins, issued by the BCBS Association, set forth the Association's position on the allowability of selected items of costs under the FEHBP contract.

Financial statements. A presentation of financial data and information, including accompanying notes, derived from accounting records to communicate at a point in time an entity's financial position, and for a period of time its results of operations and cash flow or changes in financial position.

Findings. The result of logically pulling together information to arrive at conclusions about an organization, program, activity, function, condition, or other matter which was analyzed or evaluated. A finding will be the basis for conclusions and recommendations for corrective action.

Firm-fixed-price contract. A type of contract where the price is not subject to adjustment on the basis of the contractor's cost experience. This contract type places maximum risk on the contractor. It provides maximum incentive for the contractor to control costs and imposes a minimum administrative burden upon the contracting parties.

Fiscal Year. The declared accounting year for an organization, but not necessarily in conformance to a calendar year. The federal government's fiscal year is October 1 through September 30.

Flexible Spending Account Program for Federal Employees (FSAFeds). A program allowing employees (but not retirees) to contribute pre-tax salary to an account(s) that may be used to pay for out-of-pocket medical and dependent care expenses.

Flowcharts. A graphic representation of a system or part of a system in which symbols are used to represent such things as operations, data, flow and equipment.

Fraud. Irregularities and illegal acts characterized by intentional deception.

G Government Accountability Office (GAO). An agency in the Legislative Branch which establishes accounting principles and financial reporting standards for the federal government. The GAO also performs audits on behalf of the Congress.

General Controls. General controls relate to the environment within which the computer-based application systems are developed, maintained and operated, and which are therefore applicable to all the applications. The objectives of general controls are to ensure the proper development and implementation of applications, and the integrity of program and data files and of computer operations. General controls can either be manual or programmed. Examples of general controls include the development and implementation of an Information System (IS) strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

General standards. This term refers to the first set of Government Auditing Standards. The general standards include the staff qualifications, independence, due professional care, and quality controls.

Generally accepted accounting principles (GAAP). Accounting rules and procedures established by authoritative bodies or conventions that have evolved through custom and common usage.

Generally accepted auditing standards (GAAS). The auditing standards set forth in the AICPA's Statements of Auditing Standards.

Generally accepted government auditing standards (GAGAS) or (GAS). The auditing standards established by the U.S. Government Accountability Office for audits of government organizations, programs, activities, and functions, and of government funds received by contractors, nonprofit organizations, and other nongovernment organizations. The standards include the general standards, fieldwork standards, and reporting standards.

Green Book. GAO's standards for internal control in the Government.

Government On-Line Accounting Link System (GOALS). A system which includes the following applications: the Federal Centralized Trial-Balance Systems which collects

information used to produce the Financial Report of the U.S. Government; the Statement of Differences which provides Federal Program Agencies access to reconciliation data; and Warrants which provides Federal Program Agencies access to appropriation warrant activity processed by the Financial Management Service.

Government Performance and Results Act (GPRA). GPRA requires agencies to engage in project management tasks such as setting goals, measuring results, and reporting their progress.

Governmental Accounting Standards Board (GASB). A board which establishes accounting principles and financial reporting standards for state and local government entities.

Group practice plans. A subcategory of comprehensive medical plans which provide care through the group's own facilities and staff or through special contractual arrangements.

Group specific demographics. The actual composition of a group representing the number of single contracts versus the number of family contracts (contract mix); the average family size or average contract size; the geographic location of subscribers; or the age/sex of the particular group. All or some of these factors can be used in calculating the rate.

H Hands-on. This pertains to a user interacting with a computer.

Health benefit charges. The payments made and liabilities incurred by an insurance carrier for covered health care services on behalf of FEHBP subscribers, less any refunds, rebates, allowances or other credits received.

Health benefits plan. A group insurance policy or contract, medical or hospital service agreement, membership or subscription contract, or similar group arrangements provided by an insurance carrier for the purpose of providing, paying for, or reimbursing expenses for health services.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). Protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

Health maintenance organization (HMO). See comprehensive medical plan.

Healthcare and Insurance Office (HIO). OPM office with overall responsibility for administration of the FEHBP.

Higher-tier contractor. A contractor who uses subcontractors to supply goods and services in the performance of a Government contract. The higher-tier contractor may be a prime contractor or another subcontractor.

Home office. A headquarters entity that allocates cost to other, usually lower-tier, business units. This terminology is used by Cost Accounting Standards (CAS 403).

Home Page. The first page or top page of a World Wide Web site. Provides links to the other pages associated with that particular site.

Human Resources Solutions (HRS). OPM office that provides human resources products and services to meet the dynamic needs of the Federal Government.

Hyperlinks. Within TeamMate, cross-referencing is done using hyperlinks which provides electronic links back and forth to supporting working papers.

Hypertext Markup Language (HTML). A formatting language used to create documents for use on the World Wide Web. HTML documents are used by client browser programs to provide ability to link to other sites or documents on the Internet.

I Illegal acts. Failure to follow requirements of laws or implementing regulations, including intentional and unintentional noncompliance and criminal acts.

Independence. The second general standard for government auditing which provides that in all matters relating to the audit work, the audit organization and the individual auditors should be free from personal and external impairments to independence, should be organizationally independent, and should maintain an independent attitude and appearance.

Indirect costs. Costs not directly identified with a single, final cost objective.

Individual practice plans. A subcategory of comprehensive medical plans which provide care through participating plan physicians who practice in their own offices and arrange for hospital and other care as necessary.

Information System application controls. See Application Controls, page 4.

Information System general controls. See General Controls, page 17.

Information Systems Audit and Control Association. Association of information technology professionals dedicated to the audit, control, and security of information systems. ISACA awards the Certified Information Systems Auditor professional certification.

Information Systems Audits. These are audits that focus on the general and/or application controls environment surrounding an organization's computer-based systems.

Information Technology (IT). The application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

Inherent risk. The susceptibility of an audit subject to material errors assuming there are no internal controls in place.

Inspections. Special program reviews conducted by the Office of the Inspector General. The primary goals of inspections are to encourage efficient, effective, and economical program operations and management throughout the Office of Personnel Management. While not as comprehensive as audits, inspections are constructive in nature and can be a useful tool for management to assess the current operations and to identify and quickly address existing or potential problem areas.

Institute of Internal Auditors (IIA). This voluntary organization develops standards for internal audit practice and encourages internal auditors to review and improve their own internal controls and operating efficiency.

Internal auditing. Internal auditing is an independent function established within an organization to examine and evaluate its activities as a service to the organization.

Internal control procedures. The policies and procedures that management has established to provide reasonable assurance that an entity's established objectives will be achieved and that its assets are protected from fraud, waste and abuse.

Internal control structure. The policies and procedures established by an entity to provide reasonable assurance that specific entity goals and objectives will be achieved and that its assets are protected from fraud, waste and abuse. An entity's internal control structure consists of three elements: control environment; accounting system; and control procedures.

Internal control system. The sum of an organization's plans, methods, measures, policies and procedures used to achieve the objectives of internal or management control.

Internal controls. This term as defined by the U.S. Government Accountability Office includes the plan of organization and methods and procedures adapted by management to ensure that: resource use is consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and that reliable data are obtained, maintained and fairly disclosed in the reports.

Internal Oversight and Compliance (IOC). IOC ensures program managers operate efficiently and effectively in accordance with applicable policy, regulations and standards.

Internal quality control system. The operating policies and procedures established by an audit organization to provide reasonable assurance that it has established and is following adequate audit policies and procedures and has adopted and is following applicable auditing standards.

International Classification of Diseases (ICD). This is a listing of diseases and diagnostic codes used for reporting purposes.

Internet. A global interconnected network of computers using the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is standard software language that allows different type of computers with different operating systems to communicate on the Internet.

Internet Service Provider (ISP). A commercial entity that provides Internet access to individuals usually via a broadband or dial up connection.

Interval sampling. The process of selecting a random sample of items from a population (universe) on a fixed interval basis; for example, every 10th item. The method is useful when the population items are not numbered and to number them solely for the purpose of sampling would be costly.

Irregularities. Intentional noncompliance with applicable laws and regulations and/or misstatements or omissions of amounts or disclosures in financial statements.

Issuer. Under ACA, an insurance company, insurance service, or insurance organization that is contracted to sell insurance products on the marketplace exchanges.

J Joint Financial Management Improvement Program (JFMIP).

Joint venture. An enterprise owned and operated by two or more businesses or individuals as a separate entity (not a subsidiary) for the mutual benefit of the members of the group.

Journal voucher. An accounting document used to record non-cash transactions. Examples are accruals, periodic closings and cost transfers.

Judgmental sampling. This method of exploratory sampling is used when a definite purpose or result (presence/absence) is to be measured. The sample is selected irrespective of any statistical definition of the population. Specific controls are used to select the sample.

- K** Kickback. Any money, fee, commission, credit, gift, gratuity, thing of value or compensation of any kind which is provided, directly or indirectly, in return for preferential or illegal procurement treatment.
- L** Lapping. An irregularity involving the substitution of cash items to cover misappropriated funds and the delayed posting of collections to the detail accounts receivable records.
- Letter of credit (LOC) arrangement for carrier reserves. The OPM regulations, effective January 1, 1989, require the use of LOC arrangements for FEHBP payments to certain experience-rated carriers to enhance OPM's financial management of the FEHBP. This method allows certain carriers and their underwriters to withdraw amounts on deposit in the U.S. Treasury in order to discharge obligations incurred under their FEHBP contract.
- Lobbying costs. Costs incurred in attempting to influence, either directly or indirectly, an employee or officer of the federal government to give consideration or to act in regard to a regulatory or contract matter. These costs are unallowable charges for FEHBP carriers.
- Local Area Network (LAN). Links computer systems, terminals, storage devices, and programs over relatively small geographic areas for rapid communication.
- Logon ID. Log on Identification - same as User ID. A code needed to access computer systems.
- M** Mainframe computer. A large computer to which other computers can be connected.
- Management Development Centers (MDC). Training centers operated by OPM to train middle management government employees. These centers are located in Shepherdstown, West Virginia and Denver, Colorado.
- Master Employee Record (MER). OPM's computerized payroll record showing cumulative pay history and current pay status of each employee.
- Material weakness. Under GAAS, a situation in which the designated internal control procedures or the degree of compliance with the designated procedures do not provide reasonable assurance that the objectives of the controls are being achieved. Under FMFIA, an agency is required to include within its annual statement to the President and Congress a report identifying material weaknesses in internal accounting and administrative control and a schedule for corrections. A material weakness is considered a situation in which the designed procedures or the degree of operational compliance therewith does not provide reasonable assurance that the objectives of internal control specified in FMFIA are being accomplished.

Materiality. The magnitude of an omission or misstatement of accounting information that would influence the judgment of persons relying on the information.

Materially misstated. Financial statements are materially misstated when they contain errors or irregularities whose effect is important enough to cause them not to be presented fairly in accordance with generally accepted accounting principles.

Mean. The sum of all the values in a set of observations divided by the number of observations.

Medical Loss Ratio (MLR). A community-rated plan's ratio of FEHBP health claims costs (plus expenses associated with health improvement activities) to FEHBP premiums. Beginning in 2013 (in 2012 for Pilot Program plans), all non-TCR plans are required to perform an MLR calculation after the end of the contract period. Plans that do not meet the FEHB-specific MLR threshold will be required to pay any premium received in excess of an FEHBP-specific threshold to a fund that will be shared with all plans that met or exceeded the MLR threshold in that same year. OPM will publish the FEHBP-specific MLR threshold in the rate instructions to community rated carriers annually. Plans that use TCR due to state mandates will not be subject to the MLR requirements and will continue to use the SSSG requirements. MLR replaces the SSSG requirements for non-TCR community rated plans.

Medical review. The review of health benefit claims by a qualified medical professional employed by the carrier to ensure that the services provided were consistent with the diagnosis, illness, or injury.

Medically necessary. Services or supplies provided by a hospital or covered provider of health care services which are appropriate to diagnose or treat the patient's condition, illness or injury, consistent with good medical practice in the United States; are not primarily for personal comfort or convenience; and are not part of or associated with scholastic or vocational training.

Medicare. The federally funded program of health care for the aged and disabled.

Medicare loading. The additional cost, less Medicare reimbursements, for covering subscribers over age 65. The loading can be either negative or positive depending on the mix of annuitants with or without Medicare coverage.

Medicare Part A. The part of Medicare that covers inpatient hospital and related services.

Medicare Part B. The part of Medicare that covers physician services and other medical items.

Medicare Part D. The part of Medicare that covers prescription drugs.

Memorandum of Understanding (MOU). A legal document outlining the terms and details of an agreement between parties, including each parties requirements and responsibilities.

Mixed model plans. A subcategory of comprehensive medical plans which provide care through a combination of participating plan physicians in their own offices and through the plan's own facilities and staff or through special contractual arrangements. Participating physicians may arrange for hospital and other care as necessary.

Multi-State Plan. Insurance product offered by an issuer in all 50 states and the District of Columbia. The MSP must offer a minimum of at least 3 plan options, gold, silver, and child only. Any MSP will be licensed by the states, but regulated by OPM.

Multi-State Plan Program. Established under the ACA, directs OPM to contract with private health insurers in each State to offer high-quality, affordable health insurance options called Multi-State Plans in all 50 states and the District of Columbia.

N National Health Care Anti-Fraud Association (NHCAA). This organization is comprised of individuals and organizations from the public and private sectors concerned with eliminating health care fraud.

Negative assurance. A statement made by auditors as a result of compliance testing that states that nothing came to the auditor's attention as a result of specified procedures that caused them to believe that the untested items were not in compliance with applicable laws and regulations.

Negotiation. The procedure for making contracts without formal advertising.

Negotiation memorandum. A report prepared by the Contracting Officer at the conclusion of each contract negotiation describing the negotiation process, decisions and results.

No-fault automobile insurance. Automobile insurance under which benefits are payable by the insurer for the expenses of hospital and medical care for injuries resulting from an automobile accident without regard to negligence.

Nonappropriated funds. Funds not earmarked for a specific purpose.

Nonprofit organization. A business entity organized and operated exclusively for charitable, scientific or educational purposes, of which no part of the net earnings inure to the benefit of any private shareholder or individual.

Notice of Audit Inquiry (NAI). A letter to an auditee alerting them of a planned audit.

- O** Obligation. An order placed, contract awarded, service received, or similar transaction during a given period that will require payments during the same or a future period.

Office of Audits (OA). OA conducts comprehensive and independent audits of U.S. Office of Personnel Management programs, operations, and contractors. OA assists the Director and Congress by providing credibility to the information reported by the agency and providing information to improve accountability and facilitate decision-making.

Office of Inspector General (OIG). An independent office within the Office of Personnel Management (OPM) dedicated to promoting accountability and transparency both within and outside of the agency. Its mission is to provide independent and objective oversight of OPM services and programs by conducting audits, investigations, and evaluations. The OIG provides recommendations to help improve the efficiency and effectiveness of OPM's operations.

Office of Management and Budget (OMB). The OMB assists the President to prepare the budget. The OMB also measures the quality of agency programs, policies, and procedures and to see if they comply with the President's policies.

Office of Personnel Management (OPM). An independent agency of the United States government that manages the civil service of the federal government.

Office of the General Counsel (OGC). OGC provides legal advice and representation to OPM managers and leaders so they can ensure the Federal Government has an effective civilian workforce.

On-line. Pertains to a user ability to interact with a computer system or computer application via a terminal.

On-Line Payment and Collection System (IPAC). This is an automated intergovernmental system used for billing services and supplies.

Open Document Listings (ODL). A computer generated report maintained in OPM's financial office that shows a current record of accounts payables, unliquidated obligations, outstanding travel advances, and accounts receivable.

Open Season. The period when federal employees and annuitants may enroll or change coverage in the FEHB program.

Operating system (OS). The software that controls the execution of computer programs. An OS may provide services such as resource allocation, input/output control, and data management.

Operations Center. A BCBS activity which maintains enrollment files, provides eligibility information, claims history, and various accounting functions for all local BCBS plans on behalf of the Service Benefit Plan.

Option. A level of benefits provided by a plan. Some plans provide a high and a low (standard) option; others provide only one option.

Overage dependent loading (OAD). A charge to account for the differences in coverage between the FEHBP mandated coverage of age 22 and the coverage provided in the plan's community rate. The community rate may cover dependents to an age other than 22, most commonly to age 19. However, as part of the ACA, dependents are covered to age 26 for all health plans effective January 1, 2011. Therefore, the need for this loading will no longer be necessary after the effective date of the change.

P "Paperless" claims. Health benefit claims submitted electronically by the provider to the carrier for payment.

Parameters. The term applies to population or sample characteristics, such as the mean and standard deviation.

Password. A security access code for entering a computer system. Accompanied by a username allows security for logging in to a remote (or local) computer system.

Peer review. An external quality control review of the audit operations of Offices of Inspector General. The objectives of these reviews are to determine whether the organization's internal quality control system is adequate, in place and operating effectively and whether established policies and procedures and applicable auditing standards are being followed.

Per member per month revenue requirement (PMPM). The estimated monthly revenues per person required to cover expenses and profit of an HMO. Community-rated plans sometimes use the word "capitation" interchangeably with per member per month revenue requirement.

Performance audits. An audit where the objective is to determine whether the organization is operating in an economical and efficient manner and/or whether program results are being achieved. Economy and efficiency audits include: determining whether the entity is acquiring, protecting, and using its resources economically and efficiently; the causes of inefficiencies or uneconomical practices; and whether the entity has complied with laws

and regulations concerning matters of economy and efficiency. Program result audits include: determining the extent to which the desired results or benefits are achieved; the effectiveness of organizations, programs, activities, or functions; and, whether the entity is complying with requirements of laws and regulations applicable to the program.

Permanent file. The permanent file is a central repository of information about an organization gathered during an audit. This information has continuing value and is used in subsequent audits of an organization.

Personal computer (PC). A desktop or portable computer designed to give independent computing power to a single user.

Pharmacy Benefit Manager (PBM). A third party administrator of prescription drug programs responsible for processing and paying prescription drug claims.

Planning and Policy Analysis (PPA). PPA provides the Director with reports, information and other analysis assessing program trends and policy issues that affect OPM.

Population. The universe or group of items.

Positive assurance. Statements that the items tested were in compliance with applicable laws and regulations.

Pre-audit summary. A synopsis of the results of the pre-audit review of the entity to be audited. This summary highlights potential areas of concern to be addressed during the on-site audit.

Preferred Provider Organization (PPO). A fee-for-service option allowing an individual to choose plan-selected providers who have agreements with the plan. When one uses a PPO provider, the individual pays less money out-of-pocket for medical services than when one uses a non-PPO provider.

Premium taxes. State taxes assessed on premium income.

Premiums. Payments received by the carrier for enrolled subscribers.

Prepaid plans. These are comprehensive medical plans/health maintenance organizations that provide or arrange for health care services by designated plan physicians. A prepaid plan is open to all Federal employees and annuitants who live within the plan's geographical area.

Prior period adjustment. Corrections of errors for prior periods in the current year.

Probability. The chance that a specific event will occur.

Probability sampling. A sample selected in a manner that assures that each item in the population has an equal chance of being selected.

Programmed edits. Data testing built into a system to ensure data validity.

Projection. The expansion of sampling results to estimate the entire population value.

Public Law (PL). The laws passed by the U.S. Congress.

Q Qualified opinion. A qualified opinion states that, "except for" or "with the exception of" the effects of the matter(s) to which the qualification relates, the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with generally accepted accounting principles.

Quality assurance. This is an evaluative effort to ensure that work performed adheres to the organization's policies and procedures, meets established standards of performance and is carried out economically, efficiently and effectively.

Questioned cost. A cost which the auditors believe was not consistent with law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds, or was not supported by adequate documentation.

R Random sampling. This is a statistical sample, selected randomly from a population (universe) through the use of random numbers, in which each item has an equal chance of being selected.

Rate reconciliation. An OPM approved process that allows a community-rated HMO to adjust its proposed community rate (estimated several months prior to the effective date) to the community rate that is effective on January 1. This is allowed because OPM requires a rate quote prior to the establishment of the plan's community rate.

Reasonable and customary (R&C). The fee a provider most frequently charges for a specific procedure independent of any contractual agreement.

Reasonable assurance. A judgment by management based on all available information that the systems of internal control are operating as intended.

Reasonable cost. When the nature and amount of a cost does not exceed that which would be incurred by a prudent person in the conduct of competitive business.

Recommendation. Action the auditors believe is needed to correct problem areas and to improve operations.

Recommendation that funds be put to better use. A recommendation that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendations, including: reductions in outlays; de-obligation of funds from programs or operations; withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or grantee; avoidance of unnecessary expenditures noted in pre-award reviews of contract or grant agreements; or, any other savings which are specifically identified.

Record retention period. The period of time in which records must be maintained by a contractor. The FEHBP contract requires carriers to retain and make available all records applicable to a contract term that support the annual statement of operations for a period of six years after the end of the contract term to which the records relate. In addition, individual Enrollee and/or patient claim records will be maintained for six years after the end of the contract term to which the claim records relate.

Relevance. Refers to the relationship of evidence to its use.

Replica. Within TeamMate, a replica is an exact copy of a section of the TeamMate master audit file. A replica is separate from the master audit file. An individual can work off a replica and merge their changes into the master audit file.

Report Control File. A file maintained within the OIG controlling audit reports and correspondence pertaining to the reports.

Representative. This is used to indicate that the sample is a reasonable cross section of the population from which it is drawn.

Request for Information (RFI). A request for a contractor to provide information of a specific subject.

Request for Proposal (RFP). A solicitation for bids from contractors.

Request for Quote (RFQ). A request for a contractor to provide a price quotation for services; may be used with sole source solicitations.

Reserves. Under the FEHBP, the subscription charge for each plan is divided into 104 parts. For each employee and annuitant enrolled, 100 parts consist of the rate approved by OPM for payment to the plan. One part is for deposit into an administrative reserve and the remaining three parts are for deposit in the contingency reserve for the plan.

Retired Federal Employees Health Benefits Program (RFEHBP). A program designed to provide health insurance to those employees and survivors who were retired on the effective date of the Federal Employees Health Benefits Act and thus ineligible to participate in the FEHBP. This program provides basic hospital and major medical protection to enrollees and is currently administered through the Aetna Life Insurance Company.

Retirement Services (RS). RS is responsible for the Government-wide administration of retirement benefits and services for Federal employees, retirees, and their families.

Revolving Fund (RF). A fund authorized by the U.S. Congress for a specific purpose. The initial capital of the fund is provided through the normal appropriation process. Thereafter, the fund is self-sustaining, with receipts for sales of goods and services equal to the expenditures incurred in providing those services. Expenditures are replenished by organizations using the services financed by the fund. At OPM, this fund finances field investigations, training, and technical assistance to other government entities.

Risk assessment. A documented review by management of a component's susceptibility to waste, loss, unauthorized use or misappropriation.

Router. A computer or software package that handles network computer connections. Routers review destination address instructions received and determine the route for forwarding.

S Salary and Expenses Appropriation (S&E). This appropriation provides for the normal administrative expenses of OPM.

Sampling precision. Sampling precision is the range within which the estimate of a population characteristic will fall at the stipulated confidence level. Sampling precision is usually expressed in terms of a plus or minus value, such as “3 percent.”

Scope. This refers to the area of audit coverage.

Semiannual reports. These reports are presented semiannually to the U.S. Congress as required by the Inspector General Act of 1978, as amended, and contain the activities of the OIG for a 6 month period.

Service Benefit Plan. This is the government-wide health benefit plan sponsored and administered by the BlueCross BlueShield Association. The plan is available to all Federal employees.

Service charge. Under FEHBP experience-rated contracts, the negotiated amount paid to the carriers for underwriting risk and contract management.

Significance. The importance, in relation to the audit objectives, of an item, event, information, matter, or problem.

Similarly Sized Subscriber Groups (SSSG). A comprehensive medical plan's two employer groups which best meet the following conditions: (1) have the total number of contracts at the time of the rate proposal arithmetically closest in size to the FEHBP; (2) the data should be no later than March 31st; and (3) meet criteria set forth by OPM in the annual rate proposal and reconciliation instructions.

Simple Interest. Interest computed on principal alone, as opposed to compound interest which includes accrued interest in the calculation.

Special plan invoice. A BCBS document used by local plans to recover costs incurred in administering the FEHBP which require special handling.

Special reserve. For experience-rated carriers, a reserve that represents the cumulative premiums due and received from OPM (plus interest) less the cumulative sum of claim charges, expenses and risk charges. In the event of termination of the carrier's contracts, the special reserve is payable to OPM.

Standard deviation. The degree of spread or variability in a set of individual item values about the population mean. The less variation among item values, the smaller the standard deviation. Conversely, the greater the variation, the larger the standard deviation.

Standard optional insurance. Under the Federal Employees Group Life Insurance Program, a \$10,000 life insurance, accidental death and dismemberment option that an employee can elect and pay for in addition to basic life insurance.

Standards for the Professional Practice of Internal Auditing. Institute of Internal Auditors "Red Book," the Standards are the criteria by which the operations of an internal auditing department are evaluated and measured.

State statutory reserve. A requirement imposed upon insurance carriers by State law to set aside a specific amount or rate of funds into a restricted reserve.

Statements on Auditing Standards (SAS). SAS provide guidance to external auditors on generally accepted auditing standards in regards to auditing a non-public company entity and issuing a report.

Statistical sampling. Statistical sampling involves the random selection of a number of items for inspection where each item has a calculable chance of being selected. It is used for the purpose of making inferences to the whole population.

Stratified random sampling. Stratified sampling consists of dividing the population into homogenous groups and sampling each group. This method reduces sample variability, thereby improving the sampling reliability.

Subcontractor. One who performs for and takes from the prime contractor a specific part of the original requirements of the prime contract.

Subrogation. The right to recover benefit expenses paid by an insurance company when the subscriber has the right to recover for the same expenses from the party causing the injury or need for care.

Subscriber. A federal employee or annuitant enrolled in the FEHB program.

Subsequent events. Events that occur after the period covered by the financial statements and affect estimates in the financial statements or impact upon the future financial operations of the organization.

Substantive tests. The detailed examination of records made to test the validity and propriety of specific transactions or account balances, and thus provide the evidence required by the third standard of field work.

Sufficiency. The presence of enough factual and convincing evidence to support the auditors' findings, conclusions and recommendations.

Survey. The process used to gather background information about an entity's organization, programs, activities and functions. A survey is performed as part of the planning phase of the audit.

Survivor annuitant. The spouse, former spouse, or child of a deceased federal employee or annuitant who is entitled to participate in the health benefit and retirement programs.

System edits. In computer or application programs, the automated validation of data entered for a given field to ensure the data meets specific criteria.

System programmer. A computer programmer who plans, maintains, and controls the use of an operating system.

T TeamMate. TeamMate is an audit management system developed and supported by Wolters Kluwer. TeamMate enables the auditor to use a paperless audit environment and bring efficiencies to the audit planning, fieldwork, review, and archival processes. TeamMate provides a common platform for documenting, reviewing and sharing work during and after the audit.

Technical proposal. That part of a proposed contract which describes the contractor's method and ability to accomplish the work for which the proposal was made.

Time-and-materials contract. This contract provides for acquiring supplies or services on the basis of the actual time worked at specified fixed rates that include wages, overhead, general and administrative expenses, and profit. Materials are priced separately.

Traditional Community-Rating (TCR) Standard. TCR - Standard is a community-rating methodology that uses the cost of providing benefits to the entire community to develop a standard set of rates. These standard rates, based on benefit levels, are charged to all groups purchasing that benefit level without consideration of any group specific adjustment.

Traditional Community-Rating (TCR) Variable. TCR – Variable is a community-rating methodology that uses the cost of providing benefits to the entire community to develop a standard per-member-per-month (or capitation) rate. These standard capitation rates, based on benefit levels, are used as the starting point in the rate development. The standard capitations are adjusted by conversion factors which are determined based on the specific demographics of a group (i.e., contract mix and average family size).

Training Management Assistance (TMA). A contract and consultant program administered by OPM and used by federal agencies to develop training courses.

Treasury Financial Manual (TFM). The Department of the Treasury's official publication of policies, procedures, and instructions concerning financial management in the Federal Government.

Trust Funds (TF). Funds maintained by OPM for the retirement, life insurance and health insurance programs.

U Unallowable cost. A cost which may be allocable but which, under the provisions of any pertinent law, regulation, contract, or agreement cannot be included in prices, cost-reimbursements, or settlements.

Uniform plan. A health insurance plan administered by the Aetna Life Insurance Company which covers federal employees who retired before the effective date of the FEHB program.

United States Code (USC). The codification of Public Laws of the United States.

Universe. The total population or group of items.

Unqualified opinion. An audit opinion which states that the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with generally accepted accounting principles.

Unsupported cost. A cost questioned by the OIG because this cost is not supported by adequate documentation.

User ID. User Identification - A string of characters that uniquely identifies a user to a computer system.

Usual, customary, and reasonable (UCR). In reference to charges for medical services, "usual" is the fee most frequently charged by a provider for a particular service; "customary" is the range of fees usually charged by providers of similar training, experience, and location; and "reasonable" is the fee determined to be fair when a "usual" and "customary" fee has not been established for a given medical service.

V Variability. A term expressing the spread of items around a sample average; usually measured as a standard deviation.

Variables sampling. The sampling process used to measure characteristics in a population in terms of their individual magnitudes or values. This method measures "how much" (for example, the total dollar value of inventory or the total value of a certain type of recurring error). The variable may be dollars, length of time, weight, age, or any quantitatively measurable value.

Vulnerability assessment. A review of the susceptibility of a program to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion.

W Walk-through. Tracing one or more transactions through a system to gain an understanding of the internal control structure and operating procedures.

Webinar. A presentation, lecture, or workshop that is transmitted over the Web.

Working paper summaries. These work sheets, in numerical or narrative form, are used to consolidate the results of various audit steps, to control and administer the audit, and to analyze and interpret the audit results.

Working papers. The compilation of evidence obtained by the auditors during the audit, which supports the auditors' findings, opinions, conclusions and judgments.

World Wide Web (WWW). WWW is a collection of resources that a computer user is able to access by using a browser client program such as Internet Explorer.

Y Yellow Book. The Comptroller General's "Yellow Book" presents generally accepted Governmental auditing standards (GAGAS) for use by government auditors and nongovernment auditors doing government work. The "Yellow Book" outlines the standards pertaining to the auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports.

2-3. ACRONYMS.

A	ACA:	Affordable Care Act
	AGA:	Association of Government Accountants
	AICPA:	American Institute of Certified Public Accountants
	ASB:	Auditing Standards Board
	ASBCA:	Armed Services Board of Contract Appeals
	ASPA:	American Society for Public Administration
	AR:	Audit Resolution
B	BCBS:	BlueCross BlueShield Association
	BENEFEDS:	FEDVIP Enrollment Portal
C	CAAT:	Computer Assisted Audit Techniques
	CAS:	Cost Accounting Standards
	CASB:	Cost Accounting Standards Board
	CBIS:	Consolidated Business Information System
	CEO:	Chief Executive Officer
	CFC:	Combined Federal Campaign
	CFE:	Certified Fraud Examiner
	CFO:	Chief Financial Officer
	CFR:	Code of Federal Regulations
	CIA:	Certified Internal Auditor
	CIGIE:	The Council of Inspectors General on Integrity and Efficiency
	CIO:	Chief Information Officer

	CISA:	Certified Information Systems Auditor
	CLA:	Congressional, Legislative & Intergovernmental Affairs Office
	CMP:	Comprehensive medical plan
	COB:	Coordination of benefits; close of business
	COBIT:	Control Objectives for Information and Related Technology
	COSO:	Committee of Sponsoring Organizations
	COTS:	Commercial Off-The-Shelf software
	CPA:	Certified Public Accountant
	CPDF:	Central Personnel Data File
	CPT:	Current Procedural Terminology
	CPU:	Central processing unit
	CSRS:	Civil Service Retirement System
E	EOB:	Explanation of benefits
	EOP:	Explanation of payments
	ES:	Employee Services
F	FAR:	Federal Acquisition Regulation
	FASB:	Financial Accounting Standards Board
	FEDVIP:	Federal Employees Dental and Vision Program
	FEGLI:	Federal Employees Group Life Insurance
	FEHB:	Federal Employees Health Benefits
	FEHBAR:	Federal Employees Health Benefits Acquisition Regulation
	FEHBP:	Federal Employees Health Benefits Program

	FEI:	Federal Executive Institute
	FEP:	Federal Employee Program
	FERS:	Federal Employees Retirement System
	FIS:	Federal Investigative Services
	FISCAM:	Federal Information Systems Controls Audit Manual
	FISMA:	Federal Information Security Management Act
	FLTCIP:	Federal Long Term Care Insurance Program
	FMFIA:	Federal Managers Financial Integrity Act
	FPDS:	Federal Procurement Data System
	FPR:	Federal Procurement Regulations
	FSAFeds:	Flexible Spending Account Program for Federal Employees
G	GAAP:	Generally accepted accounting principles
	GAAS:	Generally accepted auditing standards
	GAGAS:	Generally accepted government auditing standards
	GAO:	Government Accountability Office
	GAS:	Government Auditing Standards
	GASB:	Government Accounting Standards Board
	GOALS:	Government On-Line Accounting Link System
	GPRA:	Government Performance and Results Act
H	HI:	Healthcare & Insurance
	HMO:	Health maintenance organization

	HRS:	Human Resources Solutions
I	ICD:	International Classification of Diseases
	IIA:	Institute of Internal Auditors
	IOC:	Internal Oversight & Compliance
	IPAC:	On-Line Payment and Collection System
	ISACA:	Information Systems Audit and Control Association
	IT:	Information Technology
J	JFMIP:	Joint Financial Management Improvement Program
L	LOC:	Letter of credit
M	MDC:	Management Development Centers
	MER:	Master Employee Record
	MLR:	Medical Loss Ratio
	MOU:	Memorandum of Understanding
	MSP:	Multi-State Plan
	MSPP:	Multi-State Plan Program
N	NAI:	Notice of Audit Inquiry
	NHCAA:	National Health Care Anti-Fraud Association
O	OA	Office of Audits
	OAD:	Overage dependent loading
	ODL:	Open Document Listings
	OGC:	Office of the General Counsel
	OIG:	Office of Inspector General

	OMB:	Office of Management and Budget
	OPM:	Office of Personnel Management
	OS:	Operating system
P	PBM:	Pharmacy Benefit Manager
	PC:	Personal computer
	PL:	Public Law
	PMPM:	Per member per month
	PPA:	Planning & Policy Analysis
R	R&C:	Reasonable and customary
	RF:	Revolving Funds
	RFEHBP:	Retired Federal Employees Health Benefits Program
	RFI:	Request for Information
	RFP:	Request for Proposal
	RFQ:	Request for Quote
	RS:	Retirement Services
S	S&E:	Salary and Expenses Appropriation
	SAS:	Statements on Auditing Standards
	SSSG:	Similarly Sized Subscriber Groups
T	TF:	Trust Funds
	TFM:	Treasury Financial Manual
	TMA:	Training Management Assistance
U	UCR:	Usual, customary, and reasonable

USC: United States Code

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2020

**Development of Audit Universe and
Agenda**

CHAPTER 2020 - DEVELOPMENT OF AUDIT UNIVERSE AND AGENDA

CONTENTS

	<u>Page</u>
 SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Background.....	1
1-3. Definitions.....	1
1-4. Policy.....	2
1-5. Annual Planning Cycle.....	4
 SECTION 2. AUDIT UNIVERSE	
2-1. General.....	5
2-2. Developing the Audit Universe.....	5
2-3. Profiles of Audit Areas.....	5
2-4. Vulnerability Assessments.....	7
2-5. Audit Priorities.....	7
2-6. Annual Update of the Audit Universe.....	7
 SECTION 3. ANNUAL AUDIT AGENDA	
3-1. General.....	9
3-2. Process.....	9
3-3. Management Input.....	9
3-4. Determination of Available Resources.....	9
3-5. Agenda Selection.....	10
3-6. Format.....	10
3-7. Approval Process.....	11
3-8. Revisions to the Annual Audit Agenda.....	11
 EXHIBITS	
A. Annual Audit Agenda - Available Resources	
B. Annual Audit Agenda - Application of Resources	
C. Annual Audit Agenda - Audit Project Proposal	

CHAPTER 2020 - DEVELOPMENT OF AUDIT UNIVERSE AND AGENDASECTION 1. GENERAL

- 1-1. **PURPOSE.** This chapter establishes policies and procedures for the development and maintenance of an audit universe and for both a two-year and annual audit plan. The planning policies and procedures outlined in this chapter are designed to provide an effective audit planning framework for the OIG and meet the planning requirements previously outlined in Office of Management and Budget (OMB) Circular A-73, Audit of Federal Operations and Programs (OMB Circular A-73 was rescinded May 22, 1995 as unnecessary because the audit practices in the circular had become common throughout the government. However, we continue to use the framework provided by this Circular).
- 1-2. **BACKGROUND.** OMB Circular A-73, Audit of Federal Operations and Programs, required that each government audit organization develop an audit universe and maintain records of its universe which identify the programs, activities, and functions of the organization subject to audit. Each audit organization was also required to periodically review its audit universe to determine the coverage, frequency, and priority of audit required for each identified component. OMB Circular A-73 also required that each federal agency prepare an audit plan at least annually which considers audit priorities, cross servicing arrangements, and reliance on non-federal audits. At a minimum, such plans will identify the programs and operations selected for audit and define for each:
- a. Specific reason for selection;
 - b. overall audit objective and scope;
 - c. audit organization that will perform the audit;
 - d. location to be audited;
 - e. staff days and other resources needed to perform the audit; and
 - f. anticipated benefits to be obtained from the audit.
- 1-3. **DEFINITIONS.** The audit universe should be structured according to organizations, programs, activities, and functions for which the OIG has direct audit responsibility. Audit profiles should contain detailed information about each organization, program, activity, and function within the audit universe.

- a. Organizations are defined as functional structures such as the units or elements that make up an agency. Major organizations may usually be identified through a review of the organization chart.
 - b. Programs are defined as efforts which are legislatively mandated or have been identified as essential in meeting the mission and purpose of an organization. As such, programs should only change as a result of new or revised mission goals.
 - c. Activities are defined as subordinate to programs and are supportive of program objectives. Moreover, activities are identifiable efforts directly related to specific objectives. Similar to programs, activities are also primarily generic in nature and should not change except for major mission or program restructuring.
 - d. Functions are defined as specific duties or efforts that are conducted in support of activities. Unlike programs and activities, functions are more susceptible to short-term changes and are the primary areas for review when updating the audit universe.
- 1-4. POLICY. The Office of Audits will update its audit universe at least annually and maintain current audit profiles for all OPM organizational elements. The research work required to update the audit universe and maintain audit profiles will be the primary responsibility of Group Chiefs/designees and their staffs. In carrying out this responsibility, Group Chiefs or designees will review various laws, regulations, and directives that pertain to their areas of responsibility, and they must be alert for program or organizational changes that could result in new or revised audit opportunities.

The Office of Audits policy is to target its audit efforts and staff resources into programs and functions where OPM's vulnerability to fraud, waste, and mismanagement is most evident. This policy is reflected throughout the audit planning process when audits are being identified, developed, rated, ranked, and selected for including in audit plans. The criteria for implementing this policy includes the priority factors prescribed by OMB Circular A-73, and they reflect a commitment to address the special concerns of the President, the Congress, OMB, the Council of Inspectors General on Integrity and Efficiency (CIGIE), and OPM management. These priority factors are grouped into three categories to facilitate the rating process, as follows:

- a. Materiality.
 - 1. Dollar magnitude.
 - 2. Extent of federal participation in terms of resources of regulatory authority.

- b. Vulnerability.
 - 1. Susceptibility to occurrences of fraud, embezzlement, program abuse, or other types of irregularities.
 - 2. Prior audit experience.
 - 3. Adequacy of financial management systems and controls.
 - 4. Results of other evaluations, e.g., inspections, program reviews, etc.
 - 5. Timeliness, reliability, and scope of audits performed by others, such as state and local government auditors and independent public accountants.
 - 6. Newness, changed conditions, or sensitivity of the organization, program, activity, or function.
 - 7. Adequacy of internal control systems as indicated by vulnerability assessments and internal control reviews required by OMB Circular A-123 “Internal Control Systems.”

- c. Additional Considerations and Special Concerns.
 - 1. Legislative requirements and congressional concerns.
 - 2. Emphasis by the President, OMB, CIGIE or OPM top management.
 - 3. Management needs need to be met, as developed in consultation with the responsible program officials.
 - 4. Availability of audit resources.

- 1-5. ANNUAL PLANNING CYCLE. Maintenance of the audit universe and audit planning is a continuous process. However, deadlines for certain events have been established in order to facilitate the annual planning process. Deadlines are as follows:
- a. June 1 - A request to OPM management officials soliciting input will be initiated (See Section 3-3).
 - b. August 31 - Group Chiefs or designees will submit their updated audit universe to the Deputy Assistant Inspector General for Audits (DAIGA) and Assistant Inspector General for Audits (AIGA) for approval (See Section 3-7).
 - c. September 30 - The AIGA will submit the annual audit agenda to the Deputy Inspector General/Inspector General for approval (See Section 3-7).

SECTION 2. AUDIT UNIVERSE

- 2-1. GENERAL. The Assistant Inspector General for Audits is the senior official within the Office of Audits and has overall responsibility for audit planning. Group Chiefs/designees and their staffs are responsible for developing the audit universe for their area of audit responsibility and for **updating** it on an **annual** basis.
- 2-2. DEVELOPING THE AUDIT UNIVERSE. The audit universe shall consist of a listing of each organization, program, activity, or function subject to audit. These should be maintained by organizational element, to the extent possible, and should include:
- a. Title of organizations, programs, activities, or functions;
 - b. a narrative description of each organization, program, activity, or function (See Section 2-3);
 - c. if applicable, the vulnerability or risk assessment rating established by OPM management; i.e., "H" for high, "M" for moderate, and "L" for low;
 - d. vulnerability or risk assessment rating assigned by the Group Chief/designee; e.g., "H" for high, "M" for moderate, and "L" for low (See Section 2-4);
 - e. prior audit report titles and identification numbers, where applicable;
 - f. status information on all known GAO and OIG recommendations which are still pending management action, where applicable;
 - g. audit priority (See Section 2-5);
 - h. staff days required to perform the audit considering the audit cycle identified in item "i" below; and
 - i. the desired frequency of audit; i.e., the audit cycle.
- 2-3. PROFILES OF AUDIT AREAS. Group Chiefs or designees are responsible for maintaining up-to-date audit profiles for each organization, program, activity, and function for which they have cognizance. Based upon research and liaison activities, these profiles may include the following information:

- a. An organization chart identifying the management structure responsible for each organization, program, activity, and function which includes the name of the individual in each management position identified.
- b. The specific goals and objectives for each program, activity, and function. This should include goals and objectives identified in component planning documents, expressed by top management officials, or implied by legal or regulatory requirements. The source of this information should be specifically identified.
- c. The identification of long-range planning objectives which may impact upon the future operation or management of the organization, program, activity, or function.
- d. The identification of significant systems development efforts which may impact upon the future operation or management of the organization, program, activity, or function.
- e. The identification of any pending legislation which may impact upon the future operation or management of the program, activity, or function.
- f. An assessment of the issues and sensitivities which characterize the political environment in which the organization, program, activity, or function operates, as well as an assessment of its overall visibility.
- g. A list of all relevant audit reports and other written assessments of the organization, program, activity, or function which have been issued during, at minimum, the last three years. This list should include the following information: source of report, type of report, report title, report date, report number (if any), primary subject, and other subject(s) or issue areas(s).
- h. Budget information, including assessment of potential impact of changes in budget authority on operations.
- i. Information on known control weaknesses and the basis or source of such information.
- j. An inventory of ADP and accounting/financial systems in place, under development, and planned. This inventory should identify the organization(s), program(s), activity(ies), and function(s) supported by each system.

- 2-4. VULNERABILITY ASSESSMENTS. Group Chiefs or designees should make an annual review to determine the vulnerability assessment rating assigned for each program, activity, or function. At a minimum, the annual review should focus on the following:
- a. Vulnerability to waste, fraud, or abuse;
 - b. statutory and regulatory requirements;
 - c. adequacy of internal control systems as indicated by vulnerability or risk assessments and management control reviews required by OMB Circular A-123, Internal Control Systems;
 - d. newness, changed conditions, or sensitivity of the program, activity or function;
 - e. current and potential dollar magnitude;
 - f. prior audit experience;
 - g. timeliness, reliability, effectiveness, and scope of audits performed by others, such as GAO and independent public accountants; and
 - h. results of other evaluations (e.g., inspections or program reviews).

These annual reviews are designed to be used to develop audit plans which focus on programs or operations most in need of audit coverage.

- 2-5. AUDIT PRIORITIES. The data included in the audit universe narratives and schedules, vulnerability assessment ratings, as well as other related information contained in audit profiles, should be used in identifying audit priorities. There are a variety of ways that the information can be assessed. The method used to combine and weight the various characteristics will depend on the characteristics of the audit universe being assessed. Whatever method is used, the end result should be translated into high, medium, and low priority classifications. Audit priorities should be established without consideration for the availability of audit resources. The results of this process will form the basis for developing the audit agenda.
- 2-6. ANNUAL UPDATE OF THE AUDIT UNIVERSE. Group Chiefs or designees shall make necessary revisions, on an annual basis, of their respective parts of the audit

universe and related audit profiles. They have primary responsibility for maintenance of documents pertaining to the audit universe. Annual review and revision of profiles is intended to ensure that they contain the most current data about each organization and their programs, activities, and functions. This process also provides the opportunity for consolidating programs, activities, or functions where they may be too extensive, or for expanding the number of programs, activities, or functions where they may be too few and/or very general.

All revisions to the audit universe should be completed no later than 30 days prior to the annual audit agenda.

SECTION 3. ANNUAL AUDIT AGENDA

- 3-1. GENERAL. The OIG's annual audit agenda identifies specific audits planned for the coming year. Because it also lists ongoing audits as of the beginning of the fiscal year, it is a summary of where planned OIG audit activities stand as of the beginning of each fiscal year. The primary purpose of the annual audit agenda is to establish the action plan through which long-range audit objectives will be met. In addition, the published plan is a fundamental tool for communicating OIG planning to top OPM managers, members and committees of the Congress, and other appropriate external parties.
- 3-2. PROCESS. An annual audit agenda will be prepared each year. The agenda should be challenging, but realistic, and flexible enough to provide for audit coverage of unforeseen priorities. Factors to be considered in developing the plan and determining priorities are those identified in Section 2-4, Vulnerability Assessments; and
- a. Management, OMB, and congressional needs to be met;
 - b. extent of federal participation in terms of resources or regulatory authority;
 - c. availability of audit resources; and
 - d. reviews planned by other groups or components.
- 3-3. MANAGEMENT INPUT. In order to ensure that management has an opportunity to express their needs, a request should be made to key management officials of major groups and offices for input into the annual audit agenda. This request should be made by June 1 of each year.
- 3-4. DETERMINATION OF AVAILABLE RESOURCES. Group Chiefs/designees and Senior Team Leaders will be provided an allocation of staff positions for the next fiscal year prior to preparing the annual audit agenda. The schedule in Exhibit A should be used to calculate and document "net available days" of staff time for audit planning purposes.

Column 1 of the schedule requires you to identify each auditor by name. Include vacant positions which you anticipate filling during the fiscal year by title and grade.

Column 2 is base days which should be computed at 251 (365 – 104 (weekends) – 10 (holidays)) for a full year. Prorate, as required, based on your knowledge of when vacancies will be filled.

Column 3 adjusts base days to net working days by eliminating annual leave (13, 20, or 26 days), sick leave (estimated at 7 days), and training (estimated at 5 days). Determine the appropriate adjustment for each staff member and calculate the net working days. Prorate time if appropriate.

Column 4 allows for an experience factor, such as 1.0 for a GS 12 and above, 0.9 for a GS 11, 0.75 for a GS 9, and 0.6 for a GS 5/7. This factor accounts for the fact that a less experienced auditor is less productive than a more experienced auditor. Consequently, an assignment staffed with less experienced auditors will require more time to complete than an assignment staffed with experienced auditors. Judgment may be exercised in applying these factors to specific individuals.

Column 5 represents the net available days for scheduling audit assignments. This column is computed by multiplying net work days (column 3) by the experience factor (column 4).

- 3-5. AGENDA SELECTION. Extensive use should be made of audit priorities assigned in preparing the audit universe when preparing the annual audit agenda. Normally, those audits assigned a high priority will be scheduled ahead of audits assigned a low priority. Some deviations may be necessary due to scheduling problems, staff expertise, travel funds, etc.
- 3-6. FORMAT. Each Group Chief or designee will be responsible for preparing his/her proposed audit agenda using the Application of Resources form provided in Exhibit B. The proposed agenda should include all planned audit work plus all prior year work which will still be in process at the beginning of the planning year, regardless of how much or how little time will be required to complete the work and issue the final report. In addition, estimated time should be factored into the schedule for nonaudit professional services (i.e., technical and consulting type activities that are not directly related to a specific ongoing audit such as oversight work, responding to requests for advice, reviewing proposed regulations or guidance, preparing responses to requests for information, preparing agency/OIG policy and procedures, etc.) and administrative

activities (i.e., performing tasks such as preparing travel vouchers and maintaining T & A records).

The resources for the proposed audit agenda should not exceed the available resources calculated in Exhibit A. Each audit described in Exhibit B should be supported by an audit project proposal. The audit project proposal should be prepared on the form described in Exhibit C. As required by OMB Circular A-73, an audit project proposal will include at a minimum:

- a. The organization that will conduct the audit;
 - b. the staff days and other resources needed to perform the audit;
 - c. the specific reasons for the selection; e.g., highly vulnerable because..., request from OPM management, etc.
 - d. the overall audit objectives and scope;
 - e. the locations to be audited; and
 - f. the anticipated benefits to be obtained from the audit.
- 3-7. APPROVAL PROCESS. Group Chiefs or designees will forward the annual audit agenda proposal through the DAIGA to the AIGA for review, input, and approval. These must be forwarded no later than 30 days prior to the end of the fiscal year (August 31) in order to allow time for them to be reviewed and presented to the Deputy Inspector General and Inspector General by September 30 for their approval. Following approval, the annual audit agenda will be summarized and presented in an Agenda Memorandum to the Director of OPM. The memorandum will include brief descriptions of the agenda items including any unusual reasons for selecting the agenda item. This should be done during the first month of the new fiscal year.
- 3-8. REVISIONS TO THE ANNUAL AUDIT AGENDA. Group Chiefs/designees and other team leaders should periodically assess the implementation of the annual audit agenda. Circumstances may arise that require changes to the annual audit agenda after it has been approved. Efforts should be made to follow the plan and audits should be dropped or added only with the approval of the AIGA. Before Group Chiefs or designees undertake an unplanned audit, they should forward a written justification to the DAIGA and AIGA for approval. The justification should include an explanation of the expected impact of

the new audit on other work and should in addition contain the information on Exhibit C.

Exhibit A

Office of Inspector General
Office of Audits

(Group)
Annual Audit Agenda - Available Resources, FY _____

Col 1 Name	Col 2 Base Days	Col 3 Net Days	Col 4 Experience Factor	Col 5 Net Available Days
Name of auditor. Include vacant positions which will be filled during fiscal year.	Gross calendar days available (Full yr. = 251 days). Prorate as required.	Net work days = Gross days less: A/L-13,20, or 26 days; S/L-7 days; trng-5 days. Adjust or Prorate as required.	GS 12/13= 1 GS 11 = .9 GS 9 = .75 GS 5/7 = .6 Judgment may be exercised in applying these factors to specific individuals	Column 3 times column 4
SAMPLE				
TOTAL				

Exhibit B

Office of Inspector General
Office of Audits

(Group)

Annual Audit Agenda -Application of Resources, FY _____

Activity	Planned Time
Description of audit activity. Include in process work carried over from previous fiscal year.	Direct time planned for activity (Pre, field, report writing, workpaper completion, supervisory review, and independent referencing)
SAMPLE	
TOTAL DIRECT TIME SCHEDULED	
TOTAL NONAUDIT PROFESSIONAL SERVICES	
TOTAL ADMINISTRATIVE TIME	
TOTAL DIRECT AND INDIRECT TIME	
TOTAL BASE DAYS AVAILABLE (Exhibit A, Col 2)	
UNAPPLIED RESOURCES	

Exhibit C

Office of the Inspector General
Office of Audits

(Group)
Annual Audit Agenda -Audit Project Proposal

Title of Audit:		
Organization:		
Audit Site:		
Type Audit: Financial <input type="checkbox"/> Performance <input type="checkbox"/> Effic. & Effect. <input type="checkbox"/> Prog. Results <input type="checkbox"/>		
Group Chief:	Estimated Staff Days	
Est. Start Date:		
Est. Completion Date:	Preaudit	
Est. Travel Costs:	On-site	
Special Resources Needed:	Post Audit	
	Total Days	
Reason for Selection:		
Audit Objectives and Scope:		
Anticipated Benefits:		

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2100

Government Auditing Standards

CHAPTER 2100 - GOVERNMENT AUDITING STANDARDS

CONTENTS

Page

SECTION 1. GENERAL

1-1.	Purpose.....	1
1-2.	Policy.....	1
1-3.	Responsibilities.....	1

CHAPTER 2100 - GOVERNMENT AUDITING STANDARDSSECTION 1. GENERAL

1-1. PURPOSE. This Chapter provides information concerning the applicable standards for performing audits and other services.

1-2. POLICY. The Government Auditing Standards (GAS) issued by the Comptroller General of the United States must be followed by the OIG Office of Audits when conducting audits. The IG Act requires that OIGs comply with standards established by the Comptroller General of the United States for audits of Federal organizations, programs, functions, and activities. These standards are referred to as GAS, commonly known as the “Yellow Book,” and can be found at <http://www.gao.gov/yellowbook>.

The December 2011 GAS are effective for financial audits and attestation engagements for periods beginning on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011.

1-3. RESPONSIBILITIES. All staff who work on audits are expected to know GAS and apply the applicable standards when performing audits, evaluations, and other services.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2120

Using the Work of a Specialist

CHAPTER 2120 - USING THE WORK OF A SPECIALIST

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Definition.....	1
1-3. Policy.....	1
SECTION 2. TYPES OF SPECIALISTS	
2-1. General.....	2
2-2. Internal Specialists.....	6
2-3. External Specialists.....	7

CHAPTER 2120 - USING THE WORK OF A SPECIALISTSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides guidance to the auditor-in-charge (AIC) and the auditors who use the work of a specialist in performing audits and attestation engagements.
- 1-2. DEFINITION. A specialist is a person (or a member of a specialty group or firm) possessing special skill or knowledge in a particular field other than accounting or auditing. Examples of specialists include, but are not limited to, actuaries, appraisers, attorneys, benefit specialists, computer specialists, engineers, medical analysts, and statisticians.
- 1-3. POLICY.
- a. The OIG Office of Audits will utilize specialists during audits and attestation engagements in accordance with:
 - (1) Government Auditing Standards (GAS) issued by the Comptroller General of the United States;
 - (2) American Institute of Certified Public Accountants (AICPA) Statements on Auditing Standards; and
 - (3) OIG policies and procedures.

SECTION 2. TYPES OF SPECIALISTS

- 2-1. GENERAL. When the audit team does not have the skills necessary to meet the objectives of an assigned audit, the team will consider using a specialist. The use of a specialist will ensure that the audit staff possesses the professional proficiency necessary to meet audit objectives. When using the work of a specialist, auditors need to consider the specialist as a team member and, accordingly assess the specialist's ability to perform the work and report results impartially.

If planning to use the work of a specialist, auditors should document the nature and scope of the work to be performed by the specialist, including:

- a. the objectives and scope of the specialist's work;
- b. the intended use of the specialist's work to support the audit objectives;
- c. the specialist's procedures and findings so they can be evaluated and related to other planned audit procedures, and;
- d. the assumptions and methods used by the specialist.

Auditors who use the work of specialists should document that the specialists are qualified in their areas of specialization.

In general, all specialists must understand, possess, and practice the preceding standards and guidelines (1-3a) to ensure quality audit work:

- a. Government Audit Standards and Guidelines. GAS, issued by the Comptroller General of the United States, describes the types of audits and attestation engagements and prescribes the general standards, field work standards and reporting standards. The AICPA has also issued auditing and attestation standards that apply to financial audits. These standards are to be observed by all OIG Office of Audits staff members, including specialists, when performing work to support a specific audit. In accordance with AICPA requirements, all work performed by specialists will be supervised and reviewed in the same manner as the work conducted by other staff auditors.
- b. These standards apply to all specialists in conducting OIG audits:
 - (1) Planning. Specialists should assist in the planning of audit steps necessary

to achieve the audit objectives. In the planning stages, specialists should:

- a) Determine what is to be accomplished in the audit.
- b) Obtain an understanding of the program to be audited.
- c) Design a methodology that provides sufficient, competent, and relevant evidence to accomplish the audit objectives.
- d) Consider any applicable legal and regulatory requirements and contract provisions which affect the audit.
- e) Obtain an understanding of internal controls as it relates to the specific objectives and scope of the audit.
- f) Identify potential sources of data that could be used as audit evidence.
- g) Identify all criteria needed to evaluate audit subject matters.
- h) Consider the results of previous audits that could affect the current audit objectives.

All planning should be documented and include a written audit plan or approach to the audit assignment(s).

- (2) Competence. Specialists assigned to OIG audits or attestation engagements should possess adequate professional skills, knowledge and experience for the tasks required. The specialist's skills should also be appropriate for the work being performed.

Evaluating the professional qualifications of the specialist involves the following:

- 1) the professional certification, license or other recognition of the specialist in her or his field, as appropriate;
- 2) the reputation and standing of the specialist in the views of peers and others familiar with the specialist's capability or performance;

- 3) the specialist's experience and previous work in the subject matter; and
- 4) the OA's prior experience in using the specialist's work. Specialists should maintain professional proficiency in their areas of expertise. **The GAS CPE requirements become effective for internal specialists when an audit organization first assigns an internal specialist to an audit. Because internal specialists apply specialized knowledge in government audits, training in their areas of specialization qualify under the requirement for 24 hours of CPE that directly relates to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. Internal specialists consulting on a GAS audit who are not involved in directing the audit, performing audit procedures, or reporting on a GAS audit are not required to meet the GAS CPE requirements.**

- (3) Independence. When auditors use the work of a specialist, auditors should assess the specialist's ability to perform the work and report results impartially as it relates to their relationship with the program or entity under audit. Specialists are also responsible for maintaining independence in all matters relating to their work on an audit or engagement. Specialists need to observe the three general classes of impairments to independence: personal, external and organizational. If one or more of these impairments affects a specialist's ability to work and report findings impartially, the specialist should immediately report any impairments to their supervisor and the supervisor should determine whether the impairments affect the performance of the specialist's assignment. If the impairment cannot be eliminated, the audit organization should remove the specialist from the audit engagement and if necessary replace with another independent specialist. In addition, if at any time the specialist's independence is impaired, the auditors should not use the work of that specialist. Also, a specialist for audit organizations should not provide nonaudit services that involve performing routine program office functions, management functions or making management decisions.

Compliance with supplemental safeguards will not overcome independence impairments in this category. By their nature, certain nonaudit services directly support the entity's operations and impair the audit organization's ability to meet either or both of the overarching

independence principles. Examples of the types of services under this category include the following:

- a. maintaining or preparing the audited entity's basic accounting records or maintaining or taking responsibility for basic financial or other records that the audit organization will audit;
- b. posting transactions (whether coded or not coded) to the entity's financial records or to other records that subsequently provide input to the entity's financial records;
- c. determining account balances or determining capitalization criteria;
- d. designing, developing, installing, or operating the entity's accounting system or other information systems that are material or significant to the subject matter of the audit;
- e. providing payroll services that (1) are material to the subject matter of the audit or the audit objectives, and/or (2) involve making management decisions;
- f. providing appraisal or valuation services;
- g. recommending a single individual for a specific position that is key to the entity or program under audit, otherwise ranking or influencing management's selection of the candidate, or conducting an executive search or a recruiting program for the audited entity;
- h. developing an entity's performance measurement system when that system is material or significant to the subject matter of the audit;
- i. developing an entity's policies, procedures, and internal controls;
- j. performing management's assessment of internal controls when those controls are significant to the subject matter of the audit;
- k. providing services that are intended to be used as management's primary basis for making decisions that are significant to the subject matter under audit;

- l. carrying out internal audit functions; and,
- m. serving as voting members of an entity's management committee or board of directors, making policy decisions that affect future direction and operation of an entity's programs, supervising entity employees, developing programmatic policy, authorizing an entity's transactions, or maintaining custody of an entity's assets.

The specialist should not audit their own work or provide nonaudit services in situations where the nonaudit services are significant/material to the subject matter of audits.

- (4) Professional Judgment. Specialists are required to use professional judgment when planning and performing audits or attestation engagements and in reporting the results. Professional judgment requires specialists to exercise professional skepticism, which is an attitude that includes a questioning mind and a critical assessment of evidence. Specialists are responsible for determining and observing the standards that apply to the work to be conducted. In consultation with the AIC/Team Leader, the specialist should recommend the methodology, tests, and procedures to achieve the audit objectives with regard to their assigned segment of the audit or attestation work.
- (5) Supervision. Specialists are to receive guidance and supervision in the same manner as other staff members. Supervision involves directing the efforts of auditors and others, including specialists, who are involved in the audit or attestation engagement, to ensure that audit standards are followed and the audit objectives are being accomplished. The AIC/Team Leader is primarily responsible for the conduct of the audit and for providing daily supervision. This includes instructing all staff members, including specialists; being aware of significant problems encountered by specialists; and reviewing the work performed by the specialists. Supervisors should satisfy themselves that the specialist clearly understands what work to perform, why the work is to be conducted, and what the work is expected to accomplish. The specialists' work should be retained in the form of audit documentation. This documentation should reflect evidence of timely supervisory review.

The OIG Office of Audits utilizes two types of specialists: internal specialists and external specialists.

- 2-2. **INTERNAL SPECIALISTS.** Internal specialists are staff who are employed by the OIG. Staff specialists employed by the OIG include attorneys, information technology specialists, and human resource specialists. For additional information concerning attorneys, see Chapter 2915 (Requesting Legal Opinions and Interpretations).

The work of staff specialists may be vital to the accomplishment of the audit engagement. The responsibility of the AIC/Team Leader is to ensure that professional standards and audit objectives are met by the staff specialists. Internal specialists who are part of the audit organization and perform as a member of the team should comply with GAGAS, including the continuing professional education (CPE) requirements. The responsibility of staff specialists is to complete all assigned duties and provide the results to the AIC/Team Leader. They will also develop audit findings and prepare working papers documenting work performed. In addition, the staff specialist may be asked to prepare pertinent sections of the audit report.

- 2-3. **EXTERNAL SPECIALISTS.** External specialists are individuals who are not members of OPM's OIG and who have skills in a profession other than auditing.
- a. **Decision to Use an External Specialist.** Particular auditing situations may require the OIG Office of Audits to use an external specialist. An external specialist may be needed when in-house expertise is not sufficient to meet audit objectives.
- The decision to use the work of an external specialist is normally determined during the initial planning of the audit. The extent to which reliance can be placed upon the work of others depends on the adequacy and extent of the work performed.
- b. **Selecting an External Specialist.** Once the decision is made to use an external specialist, the selection process should consider the specialist's:
- (1) Professional qualifications, such as their certification, license, or other designation as an expert to perform specialized service or other recognition of the competence of the specialist. **External specialists assisting in performing a GAGAS assignment should be qualified and maintain professional competence in their areas of specialization but are not required to meet the GAGAS CPE requirement. However, OA staff that plan to use the work of external specialists should assess the professional qualifications of such specialists and document their findings and conclusions.**

- (2) Reputation and standing in the views of peers and others familiar with the specialist's capability or performance.
- (3) Relationship, if any, to the audited entity. It should be determined whether the specialist is independent of the audited entity. Ordinarily, the auditor should attempt to obtain a specialist who is unrelated to the audited entity. However, when circumstances so warrant, the work of a specialist who has a relationship with the audited entity may be acceptable. **When specialists are employees of the audited entity, this fact should be prominently stated in the audit report.**

If the specialist is related to the audited entity, the auditor should perform additional procedures with respect to all or some of the related specialist's assumptions, methods, or findings to determine that the findings are reasonable. If the auditor cannot evaluate the work of the specialist, then the services of an unrelated specialist should be used. Overall, a specialist unrelated to the audited entity will usually provide the auditor with greater assurance of reliability because of the absence of a relationship that might impair objectivity.

- c. Work Performed by the External Specialist. After the external specialist has been selected, the auditor, the audited entity (if appropriate), and the specialist should meet and establish an understanding as to the nature of work to be performed by the specialist. This understanding should be discussed and documented, detailing:
 - (1) The objectives and scope of the specialist's work.
 - (2) The specialist's representation of the relationship to the audited entity.
 - (3) The methods or assumptions to be used by the specialist.
 - (4) A comparison of the assumptions or methods to be used with those used in the preceding audit engagement.
 - (5) A description of how the auditor will use the specialist's work to support assertions made in the audit report.
 - (6) A description of the format and content of the specialist's report.

- d. Using the Evidence (or Findings) of the External Specialist. Once the external specialist has completed the audit work and developed the findings, the auditor will review the findings or report to determine if they will be presented in the audit report. In addition, the auditor can determine the sufficiency, relevance, and competence of the specialist's work by making supplemental tests of the work conducted and by reviewing the supporting evidence. When reviewing the specialist's findings and/or report, the auditor should:
- (1) Obtain an understanding of the methods or assumptions used by the specialist to determine whether the findings are suitable for corroborating the representations¹ in the financial data or documentation.²
 - (2) Consider whether the specialist's findings support the related representations in the financial data or documentation.
 - (3) Perform appropriate tests of the data provided by the audited entity to the specialist.
 - (4) Use the work of the specialist unless audit procedures lead the auditor to believe that the findings are unreasonable.
 - (5) Review the specialist's work program and the audit documentation.

When the auditor determines that the external specialist's findings support the related representations in the audited documentation, it may be reasonably concluded that the auditor has obtained sufficient competent evidence. When specialists are employees of the audited entity, this fact should be prominently stated in the audit report.

- e. Reporting the External Specialist's Work in Federal Financial Statement Audit Reports. (Note: If we are the auditor, and use a specialist, this section provides guidance for preparing the report. If we have contracted the audit to an IPA and are overseeing their work, we should use this section to review their report before signing off on it.) Auditors are required to express an opinion on financial statements audited, or if circumstances require, disclaim an opinion on the data audited. The auditor's conclusions with regard to the specialist's findings may

¹Representations are defined as completeness, existence or occurrence, valuation and allocation, rights and obligations, presentations and disclosure.

²The appropriateness and reasonableness of methods or assumptions used and their application are the responsibility of the specialist.

affect the opinion and may require a limitation on the scope of the audit.

- (1) When the auditor concludes that the specialist's findings support the particular assertions in the financial statements, an unqualified opinion, without reference to the work or findings of the specialist, can be issued.
- (2) If the auditor concludes that there is a material difference between the specialist's findings and the representations in the financial statements or if the determinations made by the specialist are unreasonable, additional audit procedures should be applied. If after applying additional audit procedures the matter is still unresolved, the auditor should obtain the services of another specialist. If an additional specialist cannot resolve the problem and the matter goes unresolved, a scope limitation exists. The auditor will ordinarily conclude that a qualified opinion or a disclaimer of opinion must be expressed. If it clarifies the opinion, the auditor may refer to the work of the specialist in the report.
- (3) When the auditor concludes that the specialist's findings demonstrate that the financial statements are not in accordance with generally accepted accounting principles, a qualified opinion or an adverse opinion may be issued. In this event, the auditor may refer to the work of the specialist if such a reference further clarifies the reason for the opinion.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2205

Quality Control and Quality Assurance

CHAPTER 2205 - QUALITY CONTROL AND QUALITY ASSURANCECONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Definitions.....	1
1-3. Background.....	1
1-4. Policy.....	2
1-5. Addressing a System of Quality Control Policies and Procedures.....	2
SECTION 2. INTERNAL QUALITY CONTROL SYSTEM	
2-1. General.....	5
2-2. Policies and Procedures.....	5
2-3. Personnel Administration.....	5
2-4. Supervision and Audit Project Control.....	10
2-5. Pre-Release Report Reviews.....	14
SECTION 3. AUDIT QUALITY ASSURANCE REVIEW	
3-1. General.....	20
3-2. Purpose.....	20
3-3. Process Overview.....	20
3-4. The Quality Assurance Review.....	21
3-5. QA Report Processing and Records Management.....	26
3-6. Other QA Reviews.....	28
SECTION 4. EXTERNAL PEER REVIEW	
4-1. Background.....	29
4-2. Memorandum of Understanding.....	29
4-3. Staffing Requirements.....	30
4-4. Review Objectives.....	31
4-5. Review Scope.....	31
4-6. Review Methodology.....	32

CHAPTER 2205 - QUALITY CONTROL AND QUALITY ASSURANCECONTENTSPage

SECTION 4. EXTERNAL PEER REVIEW (continued)

4-7.	Audit Documentation.....	33
4-8.	Reporting.....	33
4-9.	Follow-up.....	35
4-10.	Report Distribution.....	35

EXHIBITS

- A. Final Audit Report Review Checklist
- B. Resolution of Comments
- C. OIG Report Clearance and Review Sheet
- D. Audit Documentation Review Checklist
- E. OIG's Office of Policy, Resources Management, and Oversight (PRMO) Training Memorandum, dated May 27, 1992, titled "OIG Training and Employee Development Policies and Procedures"
- F. OIG's Office of Audits Memorandum, dated January 25, 1995, titled "Office of Audits Policy on Administrative Leave for Professional Exams".
- G. OIG Training Request and CPE Tracking System User's Guide, dated January 27, 2005.
- H. Audit Documentation Review Checklist for the Oversight of Consolidated Financial Statement Audit Work
- I. Draft and Final Audit Report Review and Distribution Work Flow

CHAPTER 2205 - QUALITY CONTROL AND QUALITY ASSURANCESECTION 1. GENERAL

- 1-1. PURPOSE. This chapter defines the OIG Office of Audits' (OA) quality control system and quality assurance review processes. Furthermore, it establishes an ongoing, periodic assessment of work completed on audit assignments designed to provide management of the audit organization with reasonable assurance that the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of (1) adherence to professional standards and legal and regulatory requirements, (2) whether the quality control system has been appropriately designed, and (3) whether quality control policies and procedures are operating effectively and complied with in practice. The audit organization should perform monitoring procedures that enable it to assess compliance with applicable professional standards and quality control policies and procedures for GAGAS audits. Individuals performing monitoring should collectively have sufficient expertise and authority for this role.
- 1-2. DEFINITIONS.
- a. Quality control is the inherent responsibility of managers to ensure that their staff is performing quality work that meets professional standards and OIG policies.
 - b. Quality assurance is an evaluative effort to independently determine that the work meets professional standards and the requirements of the OIG.
- 1-3. BACKGROUND.
- a. The generally accepted government auditing standards (GAGAS) established by the Comptroller General of the United States require that organizations conducting government audits have an internal quality control system. The general standard related to quality control and assurance specifically states:

"Each audit organization performing audits in accordance with GAGAS must:

a. establish and maintain a system of quality control that is designed to provide the audit organization with reasonable assurance that the

organization and its personnel comply with professional standards and applicable legal and regulatory requirements, and

b. have an external peer review performed by reviewers independent of the audit organization being reviewed at least once every 3 years."

- b. The standard also provides guidance on internal quality control systems:

"An audit organization's system of quality control encompasses the audit organization's leadership, emphasis on performing high quality work, and the organization's policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements. The nature, extent, and formality of an audit organization's quality control system will vary based on the organization's circumstances, such as the audit organization's size, number of offices and geographic dispersion, the knowledge and experience of its personnel, the nature and complexity of its audit work, and cost-benefit considerations."

1-4. POLICY.

- a. OA will maintain an internal quality control system to ensure that work performed by its audit groups complies with Government Auditing Standards (GAS) and assures that audit work conforms to professional standards and procedures and OIG policy and procedures, and OA performs efficiently and produces useful, high quality reports.
- b. OA considers quality control as a continuous process involving every aspect of the administration, organization, and production of the audit work.
- c. All levels of personnel in OA will be responsible for implementing proper internal/management controls and quality control.
- d. OA's internal quality control system will include internal/management controls, internal quality assurance reviews, and external quality control reviews.

1-5. ADDRESSING A SYSTEM OF QUALITY CONTROL POLICIES AND PROCEDURES.

- a. As required by GAS, the OPM-OIG audit manual includes quality control policies

and procedures that collectively address:

1. Leadership Responsibilities for Quality within the Audit Organization are discussed in section 2-4 of this chapter. It establishes the policies and procedures that designate responsibility for quality of audits performed under GAGAS. The Quality Assurance Group (QAG) is responsible for maintaining the OPM-OIG Audit Manual. The audit manual is located

(b)
(7)
(E)
)

The auditors have “read only” access.

New or revised quality control policies and procedures are communicated to the OIG audit staff through memoranda (for major revisions) or emails (for minor revisions). All changes are approved by the Assistant IG for Audits (AIGA) or the Deputy Assistant IG for Audits (DAIGA). The correspondence highlighting the change will state what was revised and why, as well as the effective date. Each auditor is then required to confirm that they have received and reviewed the audit manual revisions. QAG will maintain a list of each audit manual change and the date each staff member confirmed receipt of the audit manual revisions.

2. Independence, Legal, and Ethical Requirements are covered in section 2 of this chapter and Chapter 2210, section 2, Audit Planning. These chapters establish the policies and procedures designed to provide reasonable assurance that the Office of Audits maintains its independence. In addition, Chapter 2915, Requesting Legal Opinions and Interpretations, establishes the policies and procedures to ensure that the Office of Audits complies with legal requirements. Chapter 2330, Ethical Principles in Government Auditing, establishes the policies and procedures to ensure that the Office of Audits complies with ethical requirements. Finally, Chapter 2335, Independence in Government Auditing, establishes the policies and procedures to ensure that the Office of Audits complies with independence requirements.
3. Initiation, Acceptance and Continuance of Audit and Attestation Engagements are discussed in Chapter 2210, section 2, Audit Planning; Chapter 2215, Managing the Audit; Chapter 2400, Audit Report Preparation and Standards; and Chapter 2410, Report Organization and

Processing. These chapters establish the policies and procedures designed to provide reasonable assurance that the audit organization will undertake audit engagements only if it can comply with professional standards and ethical principles and is acting within the legal mandate or authority of the audit organization.

4. Human Resources are covered in section 2-3 of this chapter; Chapter 2210, Audit Planning; and Chapter 2215, Managing the Audit. These chapters establish policies and procedures designed to provide the audit organization with reasonable assurance that it has personnel with the capabilities and competence to perform its audits in accordance with professional standards, as well as legal and regulatory requirements.
5. Performance of Audit and Attestation Engagements is discussed in Chapters 2005 through 2930. They establish policies and procedures designed to provide the audit organization with reasonable assurance that audit engagements are performed and reports are issued in accordance with professional standards and legal and regulatory requirements.

SECTION 2. INTERNAL QUALITY CONTROL SYSTEM

- 2-1. GENERAL. OA's internal quality controls will include: OIG policies and procedures, personnel administration, supervision, and audit project control. In addition, audits will be subjected to quality assurance reviews described below in Section 3.
- 2-2. POLICIES AND PROCEDURES. Written policies and procedures provide the foundation upon which internal quality controls are built. In order to provide direction, promote adherence to audit standards, and promote uniformity and consistency in the conduct of audit work and administrative practices, the OIG has developed, issued, and maintains a series of manuals covering administration, audit, and investigation policies and procedures. OA is responsible for the OPM OIG Audit Manual. This manual covers such topics as audit standards, field work methods, audit documentation preparation, audit report writing, and supervision.
- 2-3. PERSONNEL ADMINISTRATION. Personnel administration should be designed to promote the selection of qualified, well trained and motivated personnel as required by the general standard related to competence. This standard states, "The staff assigned to perform the audit must collectively possess adequate professional competence needed to address the audit objectives and perform the work in accordance with GAGAS."
- a. Staff proficiency.
1. Personnel recruited and selected for OA positions within the OIG will meet the minimum requirements established by OPM for the occupation series for which they are hired: (a) For entrance level auditor positions, recruiting will focus on students who have a bachelor's degree with at least 24 credit hours of accounting. In addition, professional certification goals, motivation, maturity, leadership, and work ethic should be considered to complement high academic achievement; and (b) all candidates should be willing to travel at least occasionally, and frequently if assigned to perform insurance and information systems audits: High priority should be given to well-qualified candidates.
 2. With the assistance of the OIG administrative staff, OA will recruit, interview, and select its audit staff. At least two members of the OA should interview each candidate.
 3. In addition to recruiting and retaining auditors with an accounting background, OA has a need for computer specialists on a full-time basis to

ensure the staff possesses the complementary professional proficiency necessary to audit OPM programs. Other skills will be acquired on an as-needed basis.

4. Office files should show that the auditors assigned to an audit collectively possess adequate professional proficiency.

b. Training.

1. OA will provide for three types of training to ensure new personnel learn their job responsibilities and experienced personnel maintain their technical competence. The three training opportunities include: (1) new employee orientation; (2) on-the-job training; and (3) continuing education.

(a) New Employee Orientation. All new employees should receive an orientation acquainting them with the Office of the Inspector General and their job responsibilities. The orientation should include: meeting with audit management personnel; reading the OIG policy and audit procedures manual and other background material; and touring appropriate offices. In addition, new employees should be given an overview of the programs they will be responsible for auditing and should be provided with copies of the laws and regulations pertaining to the audit area to which they are assigned.

(b) On-the-Job Training.

- (1) On-the-job training refers to the informal, daily interaction between two or more staff members in the normal course of audit work. It is particularly important for new or less experienced employees because it enables them to learn their job responsibilities and to develop professionally. On-the-job training is also an effective method for quickly identifying performance weaknesses, providing appropriate feedback and allowing supervisors to determine the need for additional training opportunities to strengthen skills.
- (2) During on-the-job training, entry level employees must be given carefully constructed assignments. They must have a clear understanding of the objective of the assignment and the steps that they must perform to complete the assignment. The work

of inexperienced employees should be carefully monitored, and their work reviewed immediately after completion so that timely feedback can be provided.

- (3) It is vital to the auditors' training and future professional development that they acquire the habit of performing audit work in accordance with acceptable auditing standards. The importance of implementing proper quality controls and adhering to the standards should be stressed by supervisory and other personnel when introducing new employees to the audit techniques involved in proper audit documentation preparation, i.e., headings, purpose, source, scope, conclusion, cross-referencing, etc.; proper development of an audit finding, i.e., condition, criteria, cause, effect, and recommendation; rules of evidence; the concepts of materiality; professional judgment; the importance of audit programs; etc.

(c) Continuing Education.

- (1) In order to meet GAS requirements and to enhance the quality of audit work, OA staff must participate in continuing education to maintain and improve technical competence and professional proficiency.
- (2) As required by GAS, all OA individuals responsible for planning, directing, performing field work, or reporting on government audits must complete at least 80 hours of continuing education and training every two years, with a minimum of 20 hours completed in any one year. GAS further requires that at least 24 of the 80 hours be in subjects directly related to government auditing, the government environment, or the specific or unique environment in which the audited entity operates. Also, internal specialists who are part of the audit organization and part of the team should comply with GAGAS, including the CPE requirements. Auditors involved in the planning, directing, or reporting on GAGAS assignments and all auditors who are not involved in those activities but charge 20 percent or more of their time annually to GAGAS requirements, should also obtain at least an additional 56 hours of CPE (for a total of 80 hours of CPE in every 2-year period)

that enhances the auditors' professional proficiency to conduct audits.

The required training hours for new hires are prorated based on the number of full 6-month intervals remaining in the CPE period. (For example, if the CPE period runs from January 1, 2007 through December 31, 2008 and the new staff member was hired on May 8, 2008, then he/she would need 20 hours [$\frac{1}{4} \times 80$ hours]). The starting period for the present 2-year period is: January 1, 2015. The ending period for the present 2-year period is: December 31, 2016. (For future 2-year periods, OA supervisors and auditors will need to earn at least 80 hours of CPE credits at the end of the following 2-year periods: December 31, 2018, 2020, 2022, etc.)

Any supervisors or auditors that have not met the GAGAS's CPE requirements will have 2 months (January and February) following the 2-year period to make up any training deficiency. Supervisors and auditors who still have not met the 80 hours CPE training requirement after the 2-month grace period should not participate in audits or attestation engagements performed in accordance with GAGAS until the training requirements are met. Any CPE training hours earned toward a deficiency in one period should be documented in the employee's CPE training folder and may not be counted toward the requirements for the next 2-year period.¹

- (3) Each person is responsible for providing their group chief with evidence to support CPE training received and the accuracy of their training file. All groups will utilize our paperless, web-based tracking application that will allow group staff members to enter information about CPE courses taken and completed. The group staff members will submit (scanned) copies of their CPE certificates of completion to their respective group chiefs, through the automated CPE system. See Exhibit G for more details. Training obtained will be maintained in a data base

¹ The entire set of training requirements established by GAO's Government Auditing Standards entitled, "Guidance on GAGAS Requirements for Continuing Professional Education", dated April 2005, can be found at GAO's web site <http://www.gao.gov/govaud/ybcpe2005.pdf>.

from which reports and queries can be generated. Staff members should keep their own paper copy of the certificate of completion. Supervisors, auditors, and the OIG training officer are jointly responsible for ensuring that auditors receive appropriate training in sufficient quantities to meet GAS continuing education requirements. See PRMO Memorandum dated May 27, 1992, titled "OIG Training and Employee Development Policies and Procedures," Exhibit E.

- (4) OA will provide or pay for the continuing education for staff members, including a portion of the cost of a review course to prepare for a professional certification exam. Individual staff members also have responsibility for their own professional development. Therefore, OA expects that staff members will, on their own, pursue individual development goals such as obtaining additional college credits, obtaining a professional certification, participating in professional organizations, and reading professional journals. Also, OA will grant administrative leave for staff taking professional examinations. See Exhibit F for more details.
- c. Career Development Plan. The Career Development Plan (CDP) is the auditor's plan for professional development. The purpose of the CDP is to identify and assist the auditor in the attainment of career goals and objectives. The CDP is designed by the auditor and is based on his/her individual development needs as defined by the auditor and his/her supervisor. See Chapter 2920 (Career Enhancement) for more details.
 - d. Employee Performance Evaluations. The OA shall participate in the employee evaluation system required by OPM's Office of Human Resources. This system involves employee performance standards and interim and fiscal year performance appraisals which provide important feedback on the quality of work performed. This process helps to assure that employees obtain high standards of performance or identifies areas in which assistance is needed to correct performance weaknesses. Supervisors and staff members are encouraged to provide frequent feedback concerning employee performance. This helps to ensure that employees have an ongoing understanding of their expected performance level.
 - e. Staff Independence. To provide evidence that audit work is free from personal

and external impairments, all audit team members who prepared, worked on or reviewed an audit report or set of work papers (this includes the Group Chief, Senior Team Leader, Team Leader/AIC, audit staff, and the independent referencer) must complete the "Audit Staff Declaration of Personal and Financial Independence" statement for each audit in which they are involved. This statement is retained with the audit documentation and should be properly signed and dated by all staff involved with the audit. In addition, each auditor should immediately notify his/her immediate supervisor when something occurs that may impair their independence. Also, OA staff that are GS-12's or above must complete and file a financial disclosure statement annually with the Assistant IG for Legal Affairs.

If the staff has a threat to their independence, for example a financial or other interest that will inappropriately influence the auditor's judgment or behavior, this should be reported to their supervisors. If an impairment to independence is identified after the audit report is issued, the OA should assess the impact on the audit. Once the assessment is done, the audit organization should make sure it is noted in writing to the auditee and individuals known to use the audit report. See Chapter 2335 (Independence in Government Auditing) for more details.

2-4. SUPERVISION AND AUDIT PROJECT CONTROL.

- a. Supervision is the most important step in the internal quality control system and should be exercised at each level of the organization and for each level of responsibility. During an audit, supervisors² at all levels should establish methods that ensure that audit assignments are planned, controlled, and directed properly. The level of supervision required on each audit assignment may vary depending on the complexity and sensitivity of the audit assignment and staff experience. GAGAS requirements for the quality control system are consistent with the AICPA proposed statement on Quality Control Standards, except that the GAGAS requirements state that work and report reviews that are performed as part of supervision are not monitoring controls when used alone.
- b. Audit assignments may be divided into three major phases: (1) planning; (2) field work; and (3) reporting. The key methods of supervision and quality control are highlighted for each of these phases:

² As used here, the term "supervisor" refers to the chain of responsibility for a given audit assignment. Thus the term "supervisor" means any individual, irrespective of grade level or title, that has responsibility for a given audit assignment.

1. Planning.

- (a) The principal method of planning an audit is the preparation of a written audit program which is the primary management tool to: (1) ensure audit objectives will be met; (2) keep the audit staff on track during the audit process; (3) provide a systematic basis for the assignment of work; and (4) provide a record of the work performed. Audit planning should include the preparation of a time-phased audit plan to ensure the most efficient use of audit resources. See Chapter 2210 (Audit Planning) for information on preparing the time-phased audit plan.
- (b) Under the supervision of the AIC, a written audit program will be prepared for all audit assignments. The Auditor-in-Charge's (AIC)/Team Leader's immediate supervisor will review and approve (initial and date) each audit program. See Chapter 2210 (Audit Planning) for audit program preparation guidelines.
- (c) Changes to the written audit program will be annotated and initialed on the program itself by the AIC's/Team Leader's supervisor. Alternatively, the AIC/Team Leader may annotate and initial any deviations in the audit program due to field work conditions or issues. The AIC/Team Leader will discuss these deviations with his/her immediate supervisor and will annotate the audit documentation accordingly. See Chapter 2210 (Audit Planning).

2. Field Work.

- (a) The term field work describes the detailed part of the audit in which the steps of the audit program are completed. It encompasses the process of collecting, analyzing, interpreting, and documenting data and information. The term reflects the type of work being performed rather than the location of the work. See Chapter 2215 (Managing the Audit).
- (b) Field work should be continuously supervised to ensure that the audit objectives are achieved and the work adheres to the auditing standards and OIG policies. This supervision usually begins with the AIC/Team Leader (first line supervisor), who has the primary

responsibility for the conduct of the audit. The second line supervisor should monitor the field work using the following methods:

- (1) Time Reporting. The audit documentation for each audit assignment shall contain an Auditor Time Log which records the time spent by each auditor on the audit assignment. See Exhibit F in Chapter 2220 (Audit Documentation and Files). Alternatively, reports from the OIG "Audits Time Reporting System" or any equivalent system may be used. Periodically, the time expended on each audit shall be reported to management.
- (2) Staff Meetings. During audits the AIC's/Team Leader's supervisor should review the progress of the audit with the audit team. The purpose of these meetings/discussions is to give the audit team an opportunity to: raise questions or surface problems they are unable to cover in progress reports; assist in project management; and provide other feedback. Site visits are encouraged. During site visits, audit documentation should also be reviewed and written comments should be left with the AIC/Team Leader, when appropriate.
- (3) Audit Documentation Review.
 - (a) The AIC should review audit documentation as soon as possible after completion of the field work to ensure: (1) the audit program was followed; (2) there is adequate evidence of the work performed; (3) there is sufficient, competent and reliable evidence to support the audit findings; and (4) OIG's policies on audit methods and audit documentation were followed. When complex issues arise or inexperienced auditors are assigned to an audit, the AIC is also encouraged to review documentation as they are prepared. Reviewed documentation should be initialed. See Chapter 2220 (Audit Documentation and Files).
 - (b) Any problems with the audit documentation should be resolved early in the audit process, preferably before the auditors leave the audit site. Comments

or concerns arising from the review of the audit team's automated documentation must be documented in TeamMate's "coaching notes". The supervisor or an experienced auditor will provide the auditor(s) with coaching notes for any review comments concerning any automated document. The auditor(s) will address the comments and electronically sign off on the coaching note. The supervisor or an experienced auditor will review the response and sign off on the coaching note or send another coaching note if the response is insufficient. The supervisor or an experienced auditor will document acceptance of the audit documentation after all deficiencies and questions are resolved by placing his/her initials and date (with the month, day, and year of his or her review) in TeamMate's Signoff and Edit History tab (located in each document). In addition, any items reviewed on the documentation should be tick marked by the supervisor or an experienced auditor as evidence of verification.

- (c) Other supervisory levels may also review the audit documentation to ensure the audit work has been completed in accordance with GAS and other applicable standards. When done, the reviewed documentation shall be initialed by the reviewer and any comments should be noted in the documentation.
3. Reporting Requirements. OA's internal quality control system shall include supervisory and editorial reviews and independent referencing of all audit reports. These procedures should aim to produce complete, clear and concise reports with no errors of fact, logic, or reasoning which would cast doubt on the entire reports' validity or divert attention from its substance.
- (a) Supervisory Report Reviews. The audit reports should be reviewed by designated supervisors to ensure high quality reports and conformance with OIG policies and standards. These reviews shall be documented by initialing and dating any edited versions of the audit

reports, responding to quality assurance review checklists (see Exhibits A and D), and completing an OIG report clearance and review sheet (see Exhibit C).

(b) Independent Referencing of Audit Reports.

- (1) Before submitting audit reports to higher level supervisors, the AIC/Team Leader should ensure the audit reports are indexed (cross-referenced) and the audit documentation has been completed. (See Chapter 2415, Indexing and Independent Referencing, for specific guidance on independent referencing). The AIC/Team Leader will generally be responsible for ensuring that all revisions resulting from higher level review are made.
 - (2) After all significant changes have been made to the audit report, an experienced audit staff member, independent from the team submitting the audit report, should verify or "reference" the audit reports. The Independent Referencer will trace the accuracy of the audit reports' numbers, significant facts, and statements to the audit documentation. (The draft report must be indexed [cross-referenced] before issuance. However, the signer of a draft audit report has the option of having the report independently referenced before issuance. All final audit reports will be indexed and independently referenced to the supporting audit documents before issuance.)
- (c) The appropriate supervisor will ensure that the audit documentation and audit report referencing have been completed. The supervisor will also review the audit report to assure that all review objectives have been met.
- (d) The Group Chief or designee will verify that the audit documentation is complete, that the Referencer and supervisor have concluded their reviews, and that all referencing comments have been cleared. The audit report will then be processed for issuance.

2-5. PRE-RELEASE REPORT REVIEWS.

- a. Most final audit reports will receive a pre-release quality assurance review by the Quality Assurance Group (QA). Reports that are time sensitive, such as the

financial statement audit opinions, pre-award audits, rate reconciliation audits, or other reports as determined by the DAIGA or AIGA, will not receive a pre-release quality assurance review. However, those reports which do not receive a pre-release quality assurance review will be subject to a quality assurance review in accordance with the guidelines set forth in section 3 of this chapter.

When the internal quality control review is completed at the group level, the Group Chief will put the audit report, transmittal memo, independent reference check list, and blue sheet in the group's respective folder and in the sub-file identified by the audit report number, (b) (7)(E) for QAG to review. The Group Chief will email QAG stating the final audit report is ready for review.

The reviews performed by QA do not replace the independent referencing process at the group level. Independent referencing and the QA review are not synonymous. As discussed in more detail in this chapter and Chapter 2415, Indexing and Independent Referencing, although complementary, are designed to achieve different objectives.

- b. QA will perform a quality assurance review of appropriate final audit reports. In addition, QA will review a sample of work paper documents related to the final audit reports to ensure compliance with the audit manual and related audit standards. The QA reviewer shall be independent of the group being reviewed and shall not have had any audit responsibility or involvement with the audit being reviewed. These reviews will be completed before the audit reports are presented to the DAIGA and the AIGA for signature.

In addition to ensuring compliance with GAS and OIG policies and procedures, QA's review and comments ensure consistency among the audit groups in complying with the requirements and minimize peer review issues. QA has the final word on determining if GAS and OIG policies and procedures have been met. Each group is expected to take the steps that QA outlines to correct identified instances of non-compliance. All comments raised by QA must be resolved to QA's satisfaction before the final report is forwarded to the AIGA for review. Audit groups must resolve QA comments as soon as possible.

In unusual or rare instances, the audit group may ask the DAIGA or AIGA to make a determination as to the resolution of an issue identified through the QA review. This should only occur when the issue involved is clouded (not black and white) and the group believes that a course of action different from QA's will

satisfactorily resolve the problem. In these cases, the following steps will be taken.

1. The audit group will state in writing the issue in question, the action QA determines is necessary to resolve it, and the group's position on what needs to be done to correct it.
 2. The audit group will forward its comments/position paper to QA.
 3. QA will add its comments to the group's position paper.
 4. The position paper, along with the final report, will then be forwarded to the AIGA for review. The AIGA will make the final decision on what action is to be taken on this issue and annotate it on the position paper. The position paper will be routed back to the group, through QA, for appropriate action.
 5. The group will complete the required action as soon as possible, sign the position paper when the work is complete, and forward it to QA as verification.
- c. QA will review audit reports to ensure that they include the following items:
1. Communication to Appropriate Level. There should be a properly prepared transmittal letter and/or memorandum accompanying the report;
 2. Clearly Stated Executive Summary. The report should contain an executive summary that is brief and sufficient to understand the overall conclusions of the audit report, the nature of each audit finding, and recommendations.
 3. Objectives. The report should describe the audit objectives in clear, distinct and concise statements. The objectives should explain why the OA undertook the assignment and state what the report is to accomplish and why the subject matter is important. The audit objectives must provide perspective as to what is reported, provide a clear understanding as to any significant limitations, and avoid any unstated assumptions. The reported objectives should be measurable and feasible and not stated in a broad or general manner. When the audit objectives are limited and broader objectives can be inferred, the objectives not pursued should be stated. The body of the report should address each objective stated.

4. Scope. The scope section of the report should describe the depth and parameters of audit coverage to meet the audit objectives. The scope section should state the type of audit conducted. The scope section should explain the relationship between the population of items sampled and what was audited (identify universe to be audited); identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence or documents; and explain any problems with the evidence. Any scope limitation or constraints (time, resources, data, access to certain records or individuals or other) should be identified. The scope section should report the auditor's testing of the audited entity's internal control system.
5. Methodology. The methodology section of the report should clearly explain how the audit objectives were accomplished. The section should explain evidence gathering and analytical techniques used in conducting the audit, including any assumptions made in performing the audit; comparative techniques applied; measures and criteria used to assess performance. When sampling significantly supports the findings, describe the sample design and state why it was chosen, including whether the results can be projected to the intended population. If extensive or multiple sources of information are used, the report may include a description of the procedures performed as part of the assessment of the sufficiency and appropriateness of information used as audit evidence.
6. Findings. The report should present audit findings in a convincing and fair manner. The findings should include:
 - (a) Criteria that establish the standards, measures, or expectations used in evaluating audit results;
 - (b) conditions that present factual evidence;
 - (c) causes showing the underlying reason for the condition (where it can be determined);
 - (d) effects demonstrating the risk or exposure the audited entity or the government faces; and
 - (e) recommendations for corrective actions which are responsive to audit findings cited.

Whether all the elements of a finding (condition, criteria, cause, and effect) are needed depends on the stated audit objectives. A finding or set of findings is complete when the audit objectives have been satisfied and the report clearly relates the objectives to the elements of a finding (See Objectives above).

7. Internal Controls. If applicable, the scope section of the report should include a comment on the scope of work conducted on internal controls. The audit report should also include any significant³ deficiencies found in internal controls during the audit. If internal control findings are insignificant, they should be communicated to the audited entity in a separate letter unless the deficiencies are clearly inconsequential considering both qualitative and quantitative factors. The audit report should discuss the results of an internal controls review if the sole objective is to audit the internal controls.
8. Legal Compliance. The scope section of the report should include a comment on the work conducted on the compliance with applicable laws and regulations.
9. Responsible Views. The final report should include the pertinent views of the audited entity concerning the audit findings and recommendations. The views should be reflected in the body of the report with verbatim comments attached as a separate addendum or appendix. Also, the report should include an evaluation of the comments, as appropriate. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report if they find the comments to be valid and supported with sufficient evidence. If the audited entity refuses to provide comments or is unable to comment, the auditor may issue the report without receiving the comments from the audited entity. This should be noted in the report.
10. Follow-Up Issues. The report should contain a statement on audit follow-up on significant findings and recommendations from previous audits that could have an effect on the current audit objectives or scope.

³ Significant deficiencies are those matters coming to the auditor's attention that, in the auditor's judgment, affect the results of the auditors' work and the auditors' conclusions and recommendations about those results.

11. Accomplishments. The report should include any noteworthy accomplishments pertaining to the audit and any issues needing further study by the auditors.
 12. Significant Waste or Significant Abuse Identified. The report, if applicable, should contain a statement on whether acts of significant waste or abuse, or indications of such acts, have occurred that could affect the audit or audited entity.
 13. Fraud, Illegal Acts, and Significant Violations of Provisions of Contracts or Grant Agreements Identified. The report handles fraud, illegal acts and significant violations of provisions of contracts or grant agreements consistent with OIG Audit Manual Chapter 2325 (Fraud and Illegal Acts).
- d. Exhibit A is the Final Report Review checklist used by QA staff to conduct an editorial review of all final audit reports in accordance with GAS and OIG policies and procedures.
 - e. The QA reviewer of each report will document his/her review by dating the Final Report Review checklist and initialing and dating the corresponding OIG report clearance and review sheet (See Exhibit C), which is located in the appropriate (b) (7)(E) folder for the audit.
 - f. The review process of the report will follow the Draft and Final Audit Report Review and Distribution Work Flow Guidelines found in Exhibit I of this chapter. The Group Chief will also review the QA Final Report Review checklist and if necessary, address any QA comments and/or the Group's position paper.
 - g. Upon completion of the QA review process, the QA reviewer will individually list on the Resolution of Comments sheet (See Exhibit B) under two separate headings, each item for which 1) there is agreement that requirements were not followed; and 2) there is a disagreement as to whether requirements were followed. For those items in which there is a disagreement, the AIGA's decision reached on the disposition from the process used in Section 2-5 b. will be recorded on the Resolution of Comments sheet. The QA reviewer will sign-off and date the Resolution of Comments sheet.

SECTION 3. AUDIT QUALITY ASSURANCE REVIEW

- 3-1. GENERAL. On a post-audit basis, quality assurance (QA) will perform selected internal quality assurance reviews of audit documentation and other audit operations to monitor the overall quality of Office of Audits (OA) work products. The QA reviewer shall be independent of the group being reviewed, shall not have had any audit responsibility or involvement with the audit being reviewed, and shall be at least a senior auditor (GS-13).
- 3-2. PURPOSE. The purpose of these quality assurance reviews will be to determine whether the Office of Audits is in substantial compliance with GAS as a whole; and if not in compliance, to identify the specific areas requiring improvement. QA reviews are also designed to ensure favorable peer review results.
- 3-3. PROCESS OVERVIEW. QA will conduct a quality assurance review of a judgmental sample of supporting documentation on "an after-the-fact basis" (i.e., after issuance of the report) to determine whether the audit met all GAS and OIG policies. Each review will assess the audit's compliance with the individual government auditing standards. No overall opinion regarding an individual audit's compliance with GAS shall be made.

However, through quality assurance biannual evaluations (written report with findings and recommendations) of individual QA reviews, an assessment will be made to determine whether overall Office of Audits operations are in substantial compliance with auditing standards and OIG policies and procedures.

In performing an individual QA review of the audit report or documentation, the QA reviewer shall adhere to the following general guidelines:

- a. All QA review comments should be supported by specific references to the appropriate audit documentation or report section at issue in order to facilitate comment resolution.
- b. Duplicate comments should be avoided. Instead, the original comment should be referenced.
- c. To facilitate the process, the QA reviewer is encouraged to discuss and clarify with the group chief or designee or other appropriate staff, the applicability of specific standards in highly technical areas before drafting the QA review comments.

- 3-4. THE QUALITY ASSURANCE REVIEW. Audit documentation will be selected for review on a judgmental basis designed to ensure that all audit organizations within the OA are subjected to review. The corresponding final reports will also be included in the review if they were not subjected to a pre-release review. QA will coordinate its reviews with the groups and will be given access to all staff members, audit documentation, audit reports, and documents in order to properly conduct the internal quality assurance reviews. QA will concentrate its review of audit documentation on the following items:
- a. Audit Program. The quality assurance review will verify that the audit program was prepared and completed following the OIG Audit Manual's specific guidance. The review will verify that the audit program contains the following elements:
 1. Introduction. The basic introduction may include the type and name of the review and location; and the authority to conduct the review. It can also include the pertinent laws and regulations.
 2. Background. The program should provide information about the audited entity. Examples of background data are:
 - (a) Description of program or contract;
 - (b) previous audit experience;
 - (c) known deficiencies or problems; and
 - (d) types of transactions.
 3. Objectives. The program should clearly state the audit objectives.
 4. Scope. The program should clearly describe the scope.
 5. Methodology. The program should state the methods to be used to obtain audit evidence.
 6. Steps. The program should identify those specific tests and procedures which permit the auditor to develop an audit opinion or conclusion. Each series of audit steps should be prefaced with the specific audit objectives. Audit steps required in the audit program are:

- (a) A time-phased audit plan should be prepared to show budgeted versus actual audit completion for at least each major audit section. In addition, any material variances identified should be noted and explained;
- (b) exit and entrance conferences should be held and the meeting results summarized and documented;
- (c) statistical sampling and other sampling techniques, if applicable, should be identified. See Chapter 2505 (Statistical Sampling Techniques);
- (d) prior audit report comments should be reviewed and recommendations followed up for implementation. In addition, the prior report comments should be assessed for the impact on audit scope and objectives;
- (e) a comment on the scope of work conducted on internal controls; if appropriate and an audit objective, an understanding of internal controls should be obtained and control risk should be assessed (financial audits). See Chapter 2315 (Review of Internal Controls);
- (f) if appropriate, a comment on the information systems controls for the purpose of assessing audit risk and planning the audit. This would consist of internal controls that are dependent on information systems processing; include general and application controls; are significant to the audit objectives; and if significant, auditors should evaluate the design and operating effectiveness of such controls by performing audit procedures;
- (g) if appropriate, procedures should be conducted to provide reasonable assurance of detecting significant irregularities, illegal acts, fraud, waste, abuse, and significant violations of provisions of contracts or grant agreements that could have an effect on the audit objectives. See Chapter 2325 (Fraud, Illegal Acts, and Abuse);
- (h) a review of computer data should be conducted to ensure that computer generated data used can be relied upon. See Chapter 2230 (Auditing Information Systems Controls);

- (i) a review should be conducted to ensure the audited entity's compliance with applicable laws and regulations; and
 - (j) for audits involving contracts, a review should be performed to ensure:
 - (1) compliance with the Anti-Lobbying Act and FAR; and
 - (2) the contract requirements are met.
- b. Overall Quality of Audit Documentation. QA will verify that audit documentation is indexed (hyperlinked) and cross-referenced and complies with OIG policies and procedures and GAS. The review will cover the following elements contained on the "Audit Documentation Review Checklist," (Exhibit D):
1. Purpose. The procedure summaries in TeamMate should describe why the procedure was performed; i.e., the procedure objectives.
 2. Source. The procedure summaries should specifically identify the records, files, and person(s) (including name, title, and area located) from which the evidence was obtained. The source information must be sufficiently detailed to enable others to evaluate the competence or reliability of information and to locate the original documents.
 3. Scope. The procedure summaries should describe the universe being examined in terms of:
 - (a) Time and quantity;
 - (b) how evidence was obtained;
 - (c) the basis of selection of items examined;
 - (d) the work performed; and
 - (e) the techniques employed.
 4. Conclusion. The procedure summaries should describe the results drawn from the auditors' test, analysis, and other evidence. The conclusion should relate to the purpose and objectives of the procedure.

5. Preparer's initials and date. The audit documentation should contain the preparer's initials and date (month/day/year) in the TeamMate signoff and edit history box evidencing the document's completion.
6. Supervisor's initials and date. The audit documentation should contain the supervisor's initials and date (month/day/year) in the TeamMate signoff and edit history box.
7. Supervisory review. The audit documentation should show evidence of supervisory reviews.
 - (a) The supporting documentation should document the supervisor's participation in the audit. Evidence of the supervisor's participation may be reflected in the audit time logs, staff meetings, on-site meetings, including attendance at the entrance and exit conferences, telephone discussions, and audit documentation checklists.
 - (b) The audit documentation should have TeamMate coaching notes. See Chapter 2215 (Managing Audit Field Work).
 - (c) The audit documentation should show that the review was timely. See Chapter 2215 (Managing Audit Field Work).
8. Documented audit communication. The audit documentation must:
 - (a) Be complete and accurate; provide proper support for findings, opinions, and conclusions; and document the nature and scope of the auditors' examination;
 - (b) be sufficiently detailed to enable a reviewer to ascertain the conclusions reached and the work done to support those conclusions. They should not ordinarily require supplementary oral explanations;
 - (c) be legible and neat; and
 - (d) contain information relating to matters that are materially important and relevant to the audit objectives.
9. Working paper indexing. TeamMate will automatically assign an index to

an audit document.

10. Cross referencing. Appropriate cross referencing should be made to the audit documentation in the:
 - (a) Audit program;
 - (b) TeamMate's procedure summaries;
 - (c) draft and final audit report; and
 - (d) audit inquiries, if applicable.
- c. Overall Quality of Audit Documentation for the Oversight of Consolidated Financial Statement Audit Work. QA will verify that audit documentation is indexed (hyperlinked) and cross-referenced and complies with OIG policies and procedures and GAS. The review will cover the following elements contained on the "Audit Documentation Review Checklist for the Oversight of Consolidated Financial Statement Audit Work," (Exhibit H):
 1. Contracting Process. This review will verify that the OIG determined that the independent public accountant (IPA) engaged to perform the financial statement audit is a licensed certified public accounting firm, is independent, has proper qualifications, and has a system of quality control. This review will also verify that the OIG reviewed the IPA's latest peer review report, references, audit scope and objectives, milestones, and deliverables.
 2. Planning and Monitoring the Work of the Independent Public Accountant (IPA). This review will verify the degree of responsibility the OIG accepted with respect to using the work of the IPA. This review will also verify that the OIG developed a plan to monitor and accept the IPA's work and carried out this plan in a reasonable manner.
 3. Concluding on the Adequacy of the IPA Monitoring. This review will verify that the OIG perform adequate procedures to ensure that the work of the IPA adhered to GAS.
- d. Supervisory Oversight. The review will verify that all levels of supervisory review have been completed and that all supervisory comments or coaching notes have been resolved.
- e. Independent Referencing. The review will verify the quality and accuracy of

independent referencing of the report's assertions. Independent referencing is expected to accurately verify all statements, names, numbers, etc. in the issued report. The draft report must be indexed before issuance. However, the signer of the draft report has the option of having it independently referenced before issuance. All final reports will be indexed and independently referenced to the supporting audit documentation before issuance.

- f. Audit Evidence. The QA review will examine the quality, adequacy, and presentation of audit evidence in support of audit findings. In this regard, QA will consider whether audit evidence is sufficient, appropriate, and significant (same as material) to support the audit findings.
- g. Other GAS Field Work and Reporting Standards. The QA review will also assess compliance with other applicable GAS field work and reporting standards for financial and performance audits as well as compliance with the OIG Audit Manual Chapter 2220 (Audit Documentation and Files).

3-5. QA REPORT PROCESSING AND RECORDS MANAGEMENT.

- a. Upon the completion of each QA audit documentation review, a copy of the audit documentation review comments will be provided to the appropriate group chief or designee. The audit documentation review comments will identify individual deviations from audit standards or office policy. No overall opinion will be rendered.
- b. Each group is expected to take the steps QA states are necessary to comply with the standards and OIG policies and procedures. The group chief or designee is responsible for ensuring that the QA's audit documentation comments are properly addressed. The disposition of each item should be recorded on the audit documentation review comment sheet. After the audit documentation comments are addressed, the group chief or designee will return the review comments to QA for analysis.
- c. QA will evaluate the group's response to QA's comments to determine if the appropriate action was taken to resolve the identified problem(s). **For any identified problem that may have become moot or immaterial or appropriately addressed by the group, the QA reviewer will initial and date it as resolved.** For comments on which the QA reviewer finds that a problem has not been satisfactorily resolved, the QA reviewer will notify the group of the action needed to clear the issue. The group will take the action recommended by the QA

reviewer as soon as possible. In rare instances, the group may ask the DAIGA to make a final decision on what action needs to be taken to resolve a problem identified by the QA reviewer. In such cases, the steps presented in section 2-5 b. will be followed.

- d. Upon completion of the QA review process, the QA reviewer will individually list on the Resolution of Comments sheet (See Exhibit B) under two separate headings, each item for which 1) there is agreement that requirements were not followed; and 2) there is a disagreement as to whether requirements were followed. For those items in which there is a disagreement, the DAIGA's decision reached on the disposition from the process used in Section 2-5 b. will be recorded on the Resolution of Comments sheet. The Resolution of Comments sheet will be signed and dated by the QA reviewer.
- e. At this point, all issues raised by QA and the DAIGA should be resolved. The QA reviewer will sign-off and date the audit documentation review sheets, the Resolution of Comments sheet, a copy of the group's position paper (if applicable), and file it in QA's audit documentation papers for peer review purposes. All QA reviews will be maintained in QA's audit documentation papers separate from the auditor's audit documentation papers. QA's review comments of the group's audit documentation can be photocopied by the group for their information. This photocopy should not be filed with the audit documents.
- f. At six month intervals or every semiannual report period, QA shall evaluate all the individual QA audit documentation reviews made during the period. **QA will provide the AIGA with a final memorandum and overall opinion regarding compliance with GAS and office policy. Any systemic issues needing improvement along with actions taken to address these issues will be included in this semiannual memorandum.**
- g. **QA will follow-up on issues identified in the final memorandum on subsequent QA reviews.**
- h. QA will prepare audit documentation papers according to GAS and the OIG audit manual and policies and procedures. Audit documentation will demonstrate how QA's conclusions were reached and provide the basis for determining whether the conclusions are reasonable and correct. Audit documentation must be complete and accurate, provide proper evidence to support the audit findings, comments, and conclusions and document the nature and scope of QA's examination. QA's

audit documentation should be bound, labeled, properly indexed and cross-referenced. Each individual document will contain the proper headings; the preparer information and evidence of supervisory review; a purpose, source, scope, and conclusion. See Chapter 2220 (Audit Documentation and Files).

All audit documentation must be reviewed to ensure that the QA audit work complies with GAS and OIG policies and procedures. Supervisory reviews of QA audit documents should ensure that audit standards have been met; adequate support exists for QA's conclusions and recommendations; and the audit work was conducted with professional judgment. See Chapter 2220, Section 4 (Audit Documentation Reviews).

- 3-6. OTHER QA REVIEWS. QA may periodically conduct more detailed assessments of selected audits (quality assurance, peer reviews, Federal Managers' Financial Integrity Act review, etc.), organizational functions, or internal processes within the audit organization (recruiting) as part of the internal quality assurance process.

SECTION 4. EXTERNAL PEER REVIEW

- 4-1. BACKGROUND. GAS requires that the OA participate and fully cooperate in an external peer review once every three years⁴. To ensure that independence is maintained both in appearance and in fact, reciprocal organization reviews within two consecutive three year cycles are not permitted.
- a. The review will be conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) “Guide For Conducting External Peer Reviews of The Audit Organizations of Federal Offices of Inspector General” and the CIGIE's “Audit Committee Policy Statement on Systems of Quality Control and the External Peer Review Program.” The goal of the CIGIE external review program is to foster quality audits by OIG's through an independent assessment of their quality control policies and procedures.
 - b. OA will both provide staff to serve as members of a review team and will also be subject to review.
 - c. The AIGA/DAIGA is responsible for coordinating the review and establishing the liaison with the review team. The AIGA/DAIGA shall also ensure that the review team is given access to all OIG staff members, audit documents, audit reports, the OIG Audit Manual, and other documents required to conduct the review.
- 4-2. MEMORANDUM OF UNDERSTANDING. The OPM Inspector General will sign a Memorandum of Understanding (MOU) with the participating agencies' Inspector General defining the terms of the review. The MOU should be prepared to ensure that there is a mutual understanding regarding the fundamental aspects of the review. Important provisions that should be included in the MOU are:
- a. Scope of the review;
 - b. staffing and timing;
 - c. description and listing of nonaudit services provided and all reports which did not conform with GAS in the prior 3 years;

⁴ Audit organizations should have an external peer review conducted within 3 years from the date they start (that is, start of field work) their first assignment in accordance with GAS. Subsequent external peer reviews should be conducted every 3 years. Extensions of these time frames beyond 3 months to meet the external peer review requirements can only be granted by GAO and should only be requested for extraordinary circumstances.

- d. The need for timely interim discussion of preliminary findings;
- e. added consideration for reaching agreement on each potential issue at the earliest point in the review process;
- f. provision for the draft report and letter of comments;
- g. holding of an exit or close out conference;
- h. designating a period of time for a response to the draft report;
- i. issuing the final report and letter of comments;
- j. report review procedures; and
- k. who is going to sign the report.

4-3. STAFFING REQUIREMENTS. A review team should exercise professional judgment in all matters relating to planning, performing, and reporting the results of the external peer review.

- a. The staff assigned to the review team is dependent on a number of factors including, but not limited to, the size and geographic dispersion of the OIG being reviewed, the nature and extent of its audit universe, and the scope of the review. The review should be adequately staffed to complete the review in a timely manner. Generally, the review team will include a full-time leader and the equivalent of at least three other full-time members.
 - 1. The team leader should be a senior manager with appropriate audit background and experience;
 - 2. the remaining team members should be at least senior team leaders or team leaders (GS 13 grade level or above) and collectively possess the necessary skills to perform the review;
 - 3. each team member should have current knowledge of GAS, the government environment relative to the work being reviewed, and knowledge of how to perform a peer review;
 - 4. team members should be selected based on the types and complexity of

audits to be reviewed and any specialized skills that may be needed. Also, when OIG's document their work by using electronic audit work papers, team members should be capable of reviewing such audit documents.

- b. The reviewing organization and review team members should be independent (as defined by GAS's independence criteria) with respect to the organization being reviewed. Team members should be independent of the OIG being reviewed, its staff, and its auditees whose audits are selected for review. Employees separated from the reviewed agency within the past 3 years should not participate in the external peer review of their former agency. To ensure independence, the reviewing OIG cannot review the OIG that conducted its most recent review. Also, an audit organization should not review an audit organization if that OIG's investigation unit was reviewed by the proposed reviewing OIG.

4-4. REVIEW OBJECTIVES. The review can address any objectives agreed to by the review team and the organization being reviewed. However, the primary objectives of the external peer review are to determine whether:

- a. The organization's internal quality control system is adequate, in place, and operating effectively; and
- b. established policies, procedures, and applicable auditing standards are being followed in its audit work.

4-5. REVIEW SCOPE. At a minimum, the scope of the external peer review should cover the audits that the OIG performs (or for which it directly contracts) and those elements of the organization's quality control/assurance system that are designed to ensure that these audits are carried out in accordance with GAS and established policies and procedures. The scope of the review can be expanded to other areas of the audit operations if mutually agreed upon.

- a. The period under review should cover the year comprised of the two most recent semiannual reports to Congress, unless there is some compelling reason to cover a different period.
- b. The scope should also include an agreement on the time to be allotted to provide for a thorough and efficient review. The reviewing organization should maintain administrative records on the staff days and length of time it takes to do the review as well as the travel and other costs incurred.

- 4-6. REVIEW METHODOLOGY. The peer review team will apply a “no advance notice” policy in advising the OIG of the specific individual audits selected for review. The peer review team should advise the OIG of the specific audits selected for examination only when it is ready to initiate the review of audit reports. If the OIG cannot provide the requested documentation within 2 working days, the OIG should complete the “Certification of Working Papers” certification document (see the CIGIE’s “Guide For Conducting External Peer Reviews of The Audit Organizations of Federal Offices of Inspector General”) for completeness of the audit documentation upon its delivery of documents to the peer review team.

The selection of individual audits to review involves the exercise of considerable professional judgment. While there is no set criterion, a sufficient number of audits that are representative of the audit organization should be methodically selected. Factors to consider include:

- a. Number, size, and geographical dispersion of the audit organization;
- b. number, type, importance, and a reasonable cross section of audit reports issued or a reasonable cross section subject to the OIG’s internal quality control program;
- c. number, type, and importance of nonaudit services provided with the prior 3 years;
- d. number, type, and importance of audit reports issued that did not conform to GAS;
- e. degree of centralized control over audit groups and offices;
- f. coverage and results of internal quality assurance reports;
- g. the need to verify the results of internal quality assurance reports;
- h. the need to select and review one financial statement audit;
- i. scope and results of prior external peer reviews; and
- j. changes in audit structure and leadership.

- 4-7. AUDIT DOCUMENTATION. Audit documentation should be prepared in accordance with GAS to document the work performed and the conclusions reached during the course of the peer review. They should be subject to the same custody and physical safeguard policies that the reviewing OIG applies to its audit documentation. Therefore, at a minimum, these policies should include safeguards against unauthorized use or access to the documentation, particularly any documentation that contains confidential information. The documentation should be retained by the reviewing OIG at least until the subsequent external peer review is completed on the reviewed OIG.
- 4-8. REPORTING. A final written report, and if appropriate, a letter of comments, should be prepared and addressed to the Inspector General of the reviewed organization. Any decisions concerning implementation of any recommendations in the report rest solely with the reviewed Inspector General. The report should contain the following information.
- a. Statement on review standards and guidelines. The peer review report should state the professional standards to which the reviewed OIG organization is being held. The report should state that the elements of quality control are described in the “generally accepted Government Auditing Standards (GAGAS) promulgated by the Comptroller General of the United States.” The report should also include a statement that the review was done in accordance with the guidelines established by CIGIE.
 - b. Review objectives. The report should include a description of the objectives and characteristics of an internal quality control system.
 - c. Review of scope and methodology. The statement of scope and methodology should describe the depth and coverage of the work conducted and the use of evidence-gathering techniques. The report should include any limitations as well as a description of any expansion, if applicable, identify where work was conducted, the time period covered, what was reviewed to identify the OIG’s internal quality control system, the steps performed to verify its operating effectiveness, how many individual audits were selected and reviewed, the review of the OIG’s financial statement audit and monitoring activities of the contractor performing the financial statement audit, and a list of audit reports reviewed and the OIG offices visited.
 - d. Findings, conclusions, and recommendations. The report should identify all significant deficiencies in the OIG’s quality control system and all significant instances of noncompliance with GAS and OIG policies. The report’s findings

should include the elements of condition, criteria, cause, and effect. The findings should also be supported by sufficient, competent, and relevant evidence and be complete, fair, and conveyed in a positive and constructive manner. The report should also include recommendations for corrective actions. Recommendations should be constructive, action oriented, specific, achievable, and cost effective. The decision to implement any recommendations in the report rests solely with the reviewed OIG; for those recommendations implemented, the reviewed OIG is responsible for the resolution and follow-up of corrective actions.

Any deficiencies found that are not considered to be significant are not required to be included in the letter of comments but are required to be documented in the audit documentation and communicated to the reviewed OIG organization.

- e. Opinion. The report should contain an opinion on whether the OIG's internal quality control system was designed and was complied with during the period under review to provide reasonable assurance of compliance with GAS in the conduct its audits. An OIG's noncompliance with the peer review requirements will result in a modified GAS compliance statement.
- f. Letter of Comments. The report should reference to a letter of comments, if warranted. Matters reported in the letter of comments should consist of findings and recommendations where improvements in an organization's internal quality control system are needed. The letter of comments should indicate that the comments discussed did not affect the overall opinion.
- g. Noteworthy accomplishments. The peer review team should report any best practices found during the review such as particularly creative, efficient and effective audit approaches.
- h. Views of the appropriate responsible officials. The report should obtain comments from the reviewed OIG organization to ensure the objectiveness, accuracy, and completeness of the report's findings. The peer review team should discuss deficiencies with senior audit management and staff or the designated responsible official. All preliminary findings must be presented to the designated official to avoid misunderstandings and assure all the facts are correct before the draft is prepared. This may be conveyed informally but should be in writing. An exit conference should be held, and then a formal draft report is issued with a request for written comments. The written reply should be included as an attachment to the final report. The peer review team must review the responding OIG's comments to the draft report. The final report should be revised, or the

response rebutted as necessary, throughout the report.

- 4-9. FOLLOW-UP. Subsequent external peer reviews should look at areas where problems were found in the past to determine if the same problems exist during the subsequent period. Any repeat occurrences should be reported in the peer review report and/or the letter of comments. The OPM OIG will review the peer review issues and take corrective actions to address and correct all peer review findings.
- 4-10. REPORT DISTRIBUTION. The reviewed OIG organization should provide copies of the final peer review report and letter of comments (if appropriate), to the head of its agency, the Chair and Vice Chair of the CIGIE, the Chair of the CIGIE's Audit Committee, and appropriate congressional oversight bodies⁵. Upon request, the peer review report and the letter of comments should be made available to other members of Congress, the Government Accountability Office, and the public in a timely manner. The peer review report (excluding the letter of comments) can be posted on an external website or to a publicly available file designed for public transparency of peer review results. Internal audit organizations that report internally to management should provide a copy of the external peer review report to those charged with governance.

Information in external peer review reports and letters of comment may be relevant to decisions on procuring audit or attestation engagements. Therefore, audit organizations seeking to enter into a contract to perform an audit or attestation engagement in accordance with GAS should provide the following to the party contracting for such services:

- a. the audit organization's most recent peer review report and any letter of comment, and
- b. any subsequent peer review reports and letters of comment received during the period of the contract.

Auditors who are using another audit organization's work should request a copy of the audit organization's latest peer review report and any letter of comment. The audit organization should provide these documents when requested.

⁵ The Vice Chair, CIGIE will prepare a schedule of completed peer reviews, and advise the appropriate congressional committees that the opinion reports are available on request from the reviewed OIGs.

U.S. OFFICE OF PERSONNEL MANAGEMENT
 OFFICE OF THE INSPECTOR GENERAL
 OFFICE OF AUDITS
 QUALITY ASSURANCE (QA)

FINAL AUDIT REPORT REVIEW CHECKLIST

AUDIT OF:
 REPORT NUMBER:
 REVIEWED BY:

TYPE OF AUDIT:
 GROUP CHIEF:
 DATE:

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL/ DATE	QA APPROVAL (DATE/ INITIAL)
THE QUALITY ASSURANCE PERFORMS AN EDITORIAL REVIEW OF ALL FINAL AUDIT REPORTS IN ACCORDANCE WITH THE OIG POLICIES AND PROCEDURES AND GENERALLY ACCEPTED GOVERNMENT AUDITING STANDARDS.							
1. GENERAL PRESENTATIONS							
	DID ALL PARTICIPANTS INCLUDING THE INDEPENDENT REFERENCER REVIEWER SIGN THE INDEPENDENCE STATEMENT?	X					
	WAS AN ASSESSMENT OF FRAUD DOCUMENTED IN THE WORK PAPERS?	X					
	WAS AN ASSESSMENT OF RISK DOCUMENTED IN THE WORK PAPERS?	X					
	WERE APPROPRIATE MANAGEMENT CHECKLISTS DOCUMENTED AND PROPERLY COMPLETED?	X					
	WERE TIME LOGS PROPERLY DOCUMENTED AND COMPLETED?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
WAS A TIME PHASED AUDIT PLAN PROPERLY DOCUMENTED AND COMPLETED WITH COMPARISONS BETWEEN BUDGETED AND ACTUAL FOR MAJOR PHASES OF THE AUDIT AND EXPLANATIONS FOR MATERIAL OVERAGES.	X					
AUDIT PROGRAM AND AUDIT PLANNING DOCUMENT PROPERLY DOCUMENTED AND COMPLETED WITH EVIDENCE OF PREPERATION AND REVIEW PRIOR TO THE START OF FIELD WORK.	X					
WERE ALL THE WORKPAPERS PREPARED AND REVIEWED (EXCEPT FOR THE FINAL REPORT AND ASSOCIATED WORKPAPERS THAT ARE FINALIZED UPON ITS ISSUANCE)	X					
WAS EACH SERIES OF AUDIT STEPS PREFACED WITH THE SPECIFIC AUDIT OBJECTIVES WHICH THOSE STEPS ARE DESIGNED TO ACHIEVE?	X					
IS THE FINAL REPORT PREPARED IN ACCORDANCE WITH GOVERNMENT/OIG STYLE FORMAT REQUIREMENTS?	X					
a. ARE APPROPRIATE TRANSMITTAL LETTERS/MEMOS PRESENT?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

b. DOES THE TRANSMITTAL MEMO ADDRESSED TO THE OPM FOLLOW-UP OFFICIAL REQUEST THEIR AGREEMENT OR DISAGREEMENT WITH THE AUDIT FINDINGS, AS WELL AS THE FACT THAT A MANAGEMENT DECISION MUST BE MADE ON ALL AUDIT RECOMMENDATIONS WITHIN SIX MONTHS OF ISSUANCE OF THE REPORT?	X					
c. IS THE TABLE OF CONTENTS CONSISTENT WITH THE REPORT'S HEADINGS AND CAPTIONS?	X					
d. ARE THE REPORT'S PAGE MARGINS, CAPTIONS, AND OUTLINE CONSISTENT?	X					
e. ARE THE STARTING AND ENDING DATES OF THE AUDIT'S SCOPE CONSISTENT THROUGHOUT THE REPORT AND MEMOS?	X					
f. ARE THE FORMAT OF THE ATTACHMENTS, EXHIBITS, AND APPENDICES CORRECT?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
2.		X				
<p>WAS THE REPORT PREPARED IN ACCORDANCE WITH THE OIG TIMELINESS STANDARDS?</p> <p>PLAN'S REPLY DATED 00/00/00 FINAL TO QA 00/00/00</p> <p>ELAPSED TIME 0 DAYS</p> <p>REQUIRED TIME 0 DAYS</p> <p>VARIANCE 0 DAYS</p>						
<p><u>GAGAS COMPLIANCE</u></p> <p>QUALITY ASSURANCE PERFORMS A COMPLIANCE REVIEW OF ALL FINAL AUDIT REPORTS IN ACCORDANCE WITH OIG POLICIES AND PROCEDURES AND GENERALLY ACCEPTED GOVERNMENT AUDITING STANDARDS PRIOR TO ISSUANCE.</p>						
<p><u>-REPORT CONTENTS-</u> <u>INTRODUCTION AND BACKGROUND SECTION-</u> THESE SECTIONS SHOULD PROVIDE BASIC INFORMATION ON THE AUDIT AND THE NATURE OF THE PROGRAM UNDER REVIEW.</p>						
3.		X				
4.		X				

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
5.	DOES THE REPORT DESCRIBE THE PROGRAM UNDER REVIEW AND THE AUDITEE'S OPERATIONS?	X					
6.	DOES THE REPORT COMMENT ON ISSUES RAISED IN PRIOR AUDITS, INCLUDING RECOMMENDATIONS AND FOLLOW-UP ACTIVITIES?	X					
<u>OBJECTIVE SECTION</u> – THIS SECTION SHOULD EXPLAIN WHY THE AUDIT WAS CONDUCTED AND STATE WHAT THE AUDIT WAS TO ACCOMPLISH.							
7.	ARE THE OBJECTIVE(S) OF THE AUDIT STATED?	X					
	a. IS EVERY OBJECTIVE, REQUIRING A CONCLUSION ADDRESSED IN THE FINAL REPORT?	X					
<u>SCOPE SECTION</u> – SHOULD DESCRIBE THE DEPTH AND COVERAGE OF WORK CONDUCTED TO ACCOMPLISH THE AUDIT'S OBJECTIVES.							
8.	DOES THE SCOPE SECTION STATE THAT THE AUDIT WAS CONDUCTED IN ACCORDANCE WITH "GENERALLY ACCEPTED GOVERNMENT AUDITING STANDARDS?"	X					
9.	DOES THE REPORT EXPLAIN THE SCOPE INCLUDING:	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

	a. THE WORK ACTUALLY CONDUCTED TO ACCOMPLISH THE OBJECTIVES?	X				
	b. THE PERIOD/TIME COVERED BY THE AUDIT, WHERE APPLICABLE?	X				
	c. THE PLACE(S)/LOCATION(S) WHERE THE AUDIT WAS CONDUCTED?	X				
	d. ANY SCOPE LIMITATIONS?		X			
	e. RELATIONSHIP OF POPULATION TO WHAT WAS AUDITED?	X				
	f. QUALIFYING OR LIMITING REMARKS TO CALL ATTENTION TO DEPARTURES FROM STANDARDS OR OMISSION OF REGULAR AUDITING PROCEDURES, INCLUDING DEMANDS OF ACCESS TO RECORDS OR INDIVIDUALS?		X			
	g. RELIANCE ON THE WORK OF OTHERS WHEN APPROPRIATE?	N / A				
10.	DOES THE SCOPE SECTION CONTAIN APPROPRIATE COMMENTS ON THE AUDITOR'S RELIANCE ON INTERNAL CONTROLS IN PLANNING THE AUDIT?	X				

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

METHODOLOGY SECTION – SHOULD CLEARLY EXPLAIN THE EVIDENCE GATHERING AND ANALYSIS TECHNIQUES USED.						
11.	DOES THIS SECTION PROVIDE A METHODOLOGY APPLICABLE IN ACCOMPLISHING EACH STATED OBJECTIVE?	X				
	a. THE KINDS AND SOURCES OF EVIDENCE USED?	X				
	b. TECHNIQUES USED TO VERIFY EVIDENCE AND WHY UNVERIFIED DATA WAS USED, IF APPROPRIATE?	X				
12.	IS THE TYPE OF CRITERIA USED STATED IN THIS SECTION?	X				
13.	WHEN SAMPLING IS USED DOES THIS SECTION DESCRIBE THE SAMPLE DESIGN, INCLUDING WHETHER THE RESULTS CAN BE PROJECTED TO THE POPULATION?	X				
	a. HOW DID YOU JUDGMENTALLY, RANDOMLY OR STATISTICALLY SELECT THE SAMPLE?	X				
	b. WAS EVERY “nth” ITEM SELECTED? WERE THE SAMPLE ITEMS STRATIFIED? BY ITEM? BY DOLLAR AMOUNT?	X				
	c. WHAT WAS THE TOTAL UNIVERSE OF ITEMS? WHAT WAS THE NUMBER OF ITEMS OUT OF HOW MANY ITEMS?	X				

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

	d. WAS SAS USED FOR THE SAMPLING METHOD? DID SAS GENERATE THE NUMBER OF ITEMS TO REVIEW?	X				
<u>AUDIT RESULTS</u> – SIGNIFICANT AUDIT FINDINGS AND CONCLUSIONS SHOULD BE REPORTED.						
14.	ARE SPECIFIC CONCLUSIONS PROVIDED FOR EACH AUDIT OBJECTIVE THAT WAS STATED IN THE AUDIT OBJECTIVE SECTION?	X				
15.	WHEN APPROPRIATE, DOES EACH AUDIT FINDING DESCRIBE THE:					
	a. <u>CRITERIA</u> – WHICH ESTABLISHED THE STANDARDS, MEASURES, OR EXPECTATIONS AGAINST WHICH A PROGRAM OR CIRCUMSTANCE IS EVALUATED?	X				
	b. <u>CONDITION</u> – WHICH PRESENTS A SITUATION WHICH VARIES FROM THE ESTABLISHED CRITERIA?	X				
	c. <u>CAUSE</u> – WHICH SHOWS THE UNDERLYING REASON FOR THE CONDITION WHEN KNOWN?	X				
	d. <u>EFFECT</u> – WHICH DEMONSTRATES THE RISK, EXPOSURE, OR CONSEQUENCE MANAGEMENT FACES?	X				

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
16.	ARE THE FINDINGS PRESENTED IN PROPER PERSPECTIVE BY RELATING THE EXTENT OF NONCOMPLIANCE TO THE NUMBER OF CASES EXAMINED OR THE POPULATION?	X					
17.	DOES THE REPORT PRESENT RECOMMENDATIONS WHICH ADDRESS THE CAUSE OF THE CONDITION?	X					
18.	DOES THE REPORT CONTAIN A COMMENT ON THE SCOPE OF WORK CONDUCTED ON INTERNAL CONTROLS?	X					
	DOES THE AUDIT REPORT INCLUDE THEREIN: a. THE SCOPE OF AUDIT WORK PERFORMED IN UNDERSTANDING THE ENTITY'S INTERNAL CONTROLS AND ASSESSING CONTROL RISK.	X					
19.	DOES THE REPORT CONTAIN A COMMENT ON THE SCOPE OF WORK CONDUCTED ON COMPLIANCE WITH LAWS AND REGULATIONS?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

20.	IF ONE OR MORE APPLICABLE STANDARDS WERE NOT FOLLOWED, DOES THE REPORT DISCLOSE THIS FACT, THE REASONS THEREFORE, AND THE KNOWN EFFECT OF NOT FOLLOWING THE STANDARD(S)?	X				
21.	IF THE AUDITEES RESPONSE TO THE DRAFT REPORT IS NOT INCLUDED IN ITS ENTIRETY AS AN APPENDIX, DOES THE FINAL REPORT ACCURATELY PARAPHRASE THE AUDITEE'S RESPONSE?	X				
22.	DOES THE AUDITOR'S REPLY TO THE AUDITEE'S REPNSE ADDRESS THE ISSUES RAISED?	X				
23.	IS THE SUPERVISORY REVIEW OF THE AUDIT REPORT DOCUMENTED?	X				
24.	ARE THERE OTHER NOTED DEVIATIONS FROM GAGAS OR OIG POLICY AND PROCEDURES?		X			

EXHIBIT B

**INTERNAL QUALITY ASSURANCE REVIEWS OF THE AUDIT OPERATIONS
OF THE OFFICE OF AUDITS (OA)
QUALITY ASSURANCE (QA)
FINAL AUDIT REPORT REVIEW
WASHINGTON, D.C.**

AUDIT TITLE: (NAME OF AUDIT)

REPORT NUMBER: XX-XX-XX-XX-XXX

RESOLUTION OF COMMENTS

ALL COMMENTS HAVE BEEN RESOLVED:

YES NO

AGREEMENT BETWEEN QA AND THE OA THAT AUDIT REPORTING REQUIREMENTS WERE NOT FOLLOWED:	DISAGREEMENT BETWEEN QA AND THE OA THAT AUDIT REPORTING REQUIREMENTS WERE NOT FOLLOWED:
NONE	NONE

QA REVIEWER: _____

**OFFICE OF THE INSPECTOR GENERAL
OIG REPORT CLEARANCE AND REVIEW SHEET**

EXHIBIT C

	Initials/Date	Initials/Date	Initials/Date	Initials/Date
IG				
DIG				
SPECIAL COUNSEL				
AIGI				
AIGA				
DAIGA				
GROUP CHIEF				
QUALITY ASSURANCE				
INDEPENDENT REFERENCER				
SENIOR TEAM LEADER				
AIC/TEAM LEADER				
AUDITOR				

Subject:

Comments:

Comments:

File Information

Author: _____

Typist: _____

Disk/Directory ID/Document Name: _____

Subject File: _____

Cross-Reference File(s): _____

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS
QUALITY ASSURANCE GROUP (QAG)**

AUDIT DOCUMENTATION REVIEW CHECKLIST

AUDIT OF:
REPORT NUMBER:
REVIEWED BY:

TYPE OF AUDIT:
GROUP CHIEF:
DATE:

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL/ DATE	QA APPROVAL (DATE/ INITIAL)
<u>INDEPENDENCE AND PROFESSIONAL JUDGMENT</u>							
1.	WAS THE "AUDIT STAFF DECLARATION OF PERSONAL AND FINANCIAL INDEPENDENCE" FORM COMPLETED BY THE AUDITOR(S)?	X					
2.	IF IMPAIRMENTS TO INDEPENDENCE WERE FOUND TO HAVE EXISTED (i.e. NONAUDIT SERVICES), WERE THEY REPORTED IN THE SCOPE SECTION OF THE AUDIT REPORT?	X					
3.	DID THE AUDITORS FOLLOW PROPER PROCEDURES WHEN DETERMINING THAT AN APPLICABLE STANDARD WAS NOT TO BE FOLLOWED?	X					
4.	DID THE AUDITORS DOCUMENT THE DETERMINATION THAT CERTAIN STANDARDS DID NOT APPLY?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

COMPETENCE

5.	DID THE STAFF ASSIGNED TO THE AUDIT COLLECTIVELY HAVE ADEQUATE PROFESSIONAL COMPETENCE TO ADDRESS THE AUDIT OBJECTIVES AND PERFORM THE WORK?	X					
6.	DID THE AUDIT STAFF AND INTERNAL SPECIALISTS WHO PLANNED AND PERFORMED THE AUDIT AND REPORTED ON THE RESULTS OF THE AUDIT MEET GAGAS REQUIREMENTS FOR CONTINUING PROFESSIONAL EDUCATION?	X					
7.	FOR EXTERNAL SPECIALISTS WHO ASSISTED IN PERFORMING THE AUDIT OR INTERNAL SPECIALISTS WHO PROVIDED CONSULTATION ON THE AUDIT, DID THE AUDITORS DETERMINE THAT THE SPECIALIST WAS QUALIFIED AND COMPETENT IN THEIR AREA OF SPECIALIZATION?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

AUDIT PLANNING

PROPER AUDIT PLANNING HELPS TO ENSURE THAT AUDIT OBJECTIVES ARE MET ON TIME; ADHERENCE TO PROFESSIONAL STANDARDS IN CONDUCTING AUDIT FIELD WORK; AND CLEAR, CONCISE, CONVINCING REPORTING OF AUDIT RESULTS. ALSO, PLANNING HELPS TO ENSURE PROPER STAFF DEVELOPMENT THROUGH THE MATCHING OF AUDITOR SKILLS TO SPECIFIC AUDIT OBJECTIVES.

AUDIT PLANNING

8.	IF APPLICABLE, DID THE AUDIT DOCUMENTATION CONTAIN AN "AUDIT PLANNING DOCUMENT" THAT WAS PREPARED PRIOR TO FINALIZING THE AUDIT PROGRAM SERVING AS THE FOUNDATION FOR PREPARING OR FOCUSING THE AUDIT PROGRAM?	X					
9.	DID THE "INTRODUCTION" SECTION STATE THE FOLLOWING:	- - -					
	a. THE TYPE OF EXAMINATION (i.e. AUDIT, REVIEW, INSPECTION, EVALUATION, AGREED UPON PROCEDURES, ETC.)	X					
	b. AUTHORITY TO CONDUCT THE EXAMINATION (i.e., INSPECTOR GENERAL ACT, SPECIFIC STATUTORY REQUIREMENT, ETC.)	X					
10.	DID THE "OBJECTIVES" SECTION CLEARLY STATE:	- -					
	a. OBJECTIVES IN DISTINCT AND CONCISE STATEMENTS?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
11.	DID THE "BACKGROUND" SECTION PROVIDE INFORMATION ON:	-					
	a. THE AUDITEE'S HISTORY AND OBJECTIVES?	X					
	b. LEGAL AUTHORITY FOR THE AUDITED ACTIVITY?	X					
	c. PREVIOUS AUDIT EXPERIENCE?	X					
	d. FOLLOW-UP ON PRIOR AUDIT FINDINGS?	X					
	e. OPM PROGRAM OR CONTRACTS?	X					
	f. KNOWN DEFICIENCIES OR PROBLEMS?	X					
	g. SYSTEMS USED TO DEVELOP, ALLOCATE, AND CONTROL COSTS?	X					
	h. TYPES AND FLOW OF TRANSACTIONS?	X					
	i. LOCATIONS TO BE REVIEWED?	X					
	j. GENERAL TIME FRAME FOR THE REVIEW?	X					
12.	DID THE "SCOPE" SECTION STATE THE FOLLOWING:	-					
	a. THE TYPE OF AUDIT (i.e. PERFORMANCE, FINANCIAL, ETC.)?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

	b. AN IDENTIFICATION OF WHAT IS TO BE AUDITED?	X					
	c. THE TIME PERIOD COVERED BY THE AUDIT?	X					
	d. ANY LIMITATIONS PLACED ON THE AUDIT BY DATA OR SCOPE?	X					
	e. DEVIATIONS FROM AUDITING STANDARDS, INCLUDING DEMANDS OF ACCESS TO RECORDS OR INDIVIDUALS?		X				
	f. IDENTIFICATION OF THE ORGANIZATION AND GEOGRAPHIC LOCATION FOR CONDUCTING THE AUDIT?	X					
	g. DATES THE FIELD WORK WILL BE PERFORMED AT EACH LOCATION?	X					
13.	DID THE "METHODOLOGY" SECTION PROVIDE THE FOLLOWING:	-					
	a. SUMMARY OF THE OVERALL APPROACH TO BE TAKEN?	X					
	b. THE USE OF SAMPLING TECHNIQUES AND IF APPROPRIATE, WHETHER THE RESULTS CAN BE PROJECTED TO THE POPULATION?	X					
	c. THE USE OF COMPUTER ASSISTED TECHNIQUES?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

	d. THE KINDS AND SOURCES OF EVIDENCE USED?	X					
	e. OTHER AUDIT TECHNIQUES REQUIRED TO VERIFY EVIDENCE AND WHY UNVERIFIED DATA WAS USED, IF APPROPRIATE?	X					
	f. DESCRIPTION OF ANY MEASURES OR CRITERIA USED TO ASSESS PERFORMANCE OR COMPLIANCE?	X					
14.	WAS EACH SERIES OF AUDIT STEPS PREFACED WITH THE SPECIFIC AUDIT OBJECTIVES WHICH THOSE STEPS ARE DESIGNED TO ACHIEVE?	X					
15.	WAS EACH STEP IN THE PROGRAM INDEXED TO THE AUDIT DOCUMENTS, OR INITIALED AS NOT PERFORMED?	X					
16.	DID THE AUDITOR(S) INITIAL AND DATE EACH AUDIT STEP?	X					
17.	WAS THE AUDIT PROGRAM FOLLOWED?	X					
18.	WERE EXPLANATIONS PROVIDED IN THE AUDIT DOCUMENTS WHEN WORK IN THE AUDIT PROGRAM WAS NOT COMPLETED?	X					
19.	WAS THE "AUDITOR(S)" TIME LOG COMPLETED?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL)
20.	DID THE AUDITORS GAIN AN UNDERSTANDING OF THE NATURE AND PROFILE OF THE PROGRAM AND THE NEEDS OF POTENTIAL USERS OF THE AUDIT REPORT AND ASSESS AUDIT RISK AND ITS SIGNIFICANCE WITHIN THE CONTEXT OF THE AUDIT OBJECTIVES?						
21.	DID THE AUDITORS EVALUATE WHETHER TO USE THE WORK OF OTHER AUDITORS AND SPECIALISTS TO ADDRESS SOME OF THE AUDIT OBJECTIVES AND DETERMINING WHETHER OTHER AUDITORS HAVE CONDUCTED OR ARE CONDUCTING WORK IN THE SAME PROGRAM? (GAS, 6.12C, 6.40- 6.42)						
DID THE <u>AUDIT PROGRAM</u> CONTAIN STEPS FOR THE FOLLOWING PROCEDURES:							
22.	WERE THERE STEPS FOR A TIME PHASED AUDIT PLAN INCLUDING:	-	-				
	a. BUDGETED VERSUS ACTUAL FOR AT LEAST EACH MAJOR AUDIT SECTION?	X					
	b. IDENTIFICATION AND EXPLANATION OF ANY MATERIAL VARIANCES FOR EACH MAJOR AUDIT SECTION?	X					
23.	REVIEW OF PRIOR OIG AUDIT REPORTS AND REPORTS ISSUED BY OTHERS FOR POSSIBLE PREVIOUS COVERAGE OR AUDIT FOLLOW-UP?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
24.	ENTRANCE/EXIT CONFERENCES?	X					
25.	SAMPLING TECHNIQUES USED (i.e. STATISTICAL, RANDOM, OR JUDGEMENTAL) AND IF APPROPRIATE, WHETHER THE RESULTS CAN BE PROJECTED TO THE POPULATION?	X					
26.	COMMENT ON THE REVIEW FOR COMPLIANCE WITH LAWS, REGULATIONS, CONTRACT, AND ETC.?	X					
27.	COMMENT ON THE SCOPE OF WORK CONDUCTED ON INTERNAL CONTROLS ASSESSMENT?	X					
28.	DETECTION FOR SIGNIFICANT INSTANCES OF FRAUD, WASTE, ABUSE, ILLEGAL ACTS, AND SIGNIFICANT VIOLATIONS OF PROVISIONS OF CONTRACT OR GRANT AGREEMENTS?	X					
29.	REVIEW OF COMPUTER GENERATED DATA, IF APPROPRIATE?	X					
30.	FINAL AUDIT REPORT REVIEW COMPLETED BY THE QA?	X					
31.	CROSS-REFERENCING TO THE:	-					
	a. DRAFT AND FINAL REPORT?	X					
	b. AUDIT PROGRAM?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

	c. AUDIT DOCUMENTATION OR TEAMMATE'S PROCEDURE SUMMARIES?	X					
--	---	---	--	--	--	--	--

SUPERVISION

32.	WAS THE AUDIT PROGRAM APPROVED BY (INCLUDING SIGNATURE AND DATE) THE: a. AIC'S/TEAM LEADER'S SUPERVISOR?	X					
33.	DID DEVIATIONS FROM PRESCRIBED AUDIT PROGRAM PROCEDURES HAVE SUPERVISORY APPROVAL?	X					
34.	DID THE AUDIT DOCUMENTS SHOW EVIDENCE OF SUPERVISORY REVIEWS (AUDITOR-IN-CHARGE, TEAM LEADERS.SENIOR TEAM LEADERS, GROUP CHIEFS, ETC.) OF THE WORK PERFORMED?	X					
35.	DID AUDIT DOCUMENTS SHOW THAT THE SUPERVISOR MONITORED ADHERENCE TO THE AUDIT PLAN AND AUDIT OBJECTIVES?	X					
36.	WHEN COMMENTS/COACHING NOTES WERE RAISED BY THE SUPERVISOR(S) DURING THE AUDIT DOCUMENTATION REVIEWS, DID THE AUDITOR ADDRESS THE ISSUE(S) AND WERE THEY SUBSEQUENTLY CLEARED BY THE SUPERVISOR?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

37.	WERE MOST SUPERVISORY REVIEWS TIMELY, INCLUDING REVIEWS OF THE DRAFT AND FINAL AUDIT REPORTS?	X					
38.	WERE THE RESPECTIVE SUPERVISOR "AUDIT DOCUMENTATION CHECKLISTS" COMPLETED?	X					
39.	DID THE AUDIT DOCUMENTS SHOW THAT THE "TIME PHASED AUDIT PLAN" WAS MONITORED FOR VARIANCES BETWEEN BUDGETED AND ACTUAL TIME?	X					

INTERNAL CONTROLS

40.	DID THE AUDITORS IDENTIFY THE INTERNAL CONTROL SYSTEMS PERTINENT TO THE AUDIT? THIS QUESTION IS APPLICABLE TO EVERY FINANCIAL STATEMENT AUDIT AND IF APPROPRIATE, EVERY PERFORMANCE AUDIT WHEN A REVIEW OF CONTROLS IS ONE OF THE AUDIT OBJECTIVE(S).	X					
-----	---	---	--	--	--	--	--

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
41.	FOR A FINANCIAL STATEMENT AUDIT, AND IF APPROPRIATE, FOR A PERFORMANCE AUDIT, DID THE AUDITORS OBTAIN A SUFFICIENT UNDERSTANDING OF INTERNAL CONTROLS TO PLAN THE AUDIT AND DETERMINE THE NATURE, TIMING, AND EXTENT OF TESTS TO BE PERFORMED? WAS CONTROL RISK ASSESSED?	X					
42.	WHEN INFORMATION SYSTEMS CONTROLS ARE USED EXTENSIVELY IN THE PROGRAMS UNDER AUDIT OR IN BUSINESS PROCESSES INCLUDED IN THE AUDIT OBJECTIVES, DID THE AUDITORS I) OBTAIN AN UNDERSTANDING OF THESE CONTROLS; II) EVALUATE THE CONTROLS DESIGN AND OPERATING EFFECTIVENESS; AND III) DETERMINE WHICH PROCEDURES RELATED TO THE CONTROLS ARE NEEDED?						
43.	IF THE OIG AUDITORS RELIED ON OTHER AUDITORS' WORK ON INTERNAL CONTROLS: a. DID THE AUDIT DOCUMENTS DOCUMENT THE AUDITOR'S CONCLUSIONS REGARDING THE OTHER AUDITOR'S REPUTATION, INDEPENDENCE AND QUALITY OF WORK?	X					
	b. IF NECESSARY, DID THE OIG AUDITOR UPDATE THE WORK PERFORMED BY THE OTHER AUDITOR?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

<u>AUDIT EVIDENCE AND AUDIT DOCUMENTATION</u>							
44.	WAS A COPY OF THE INDEPENDENTLY REFERENCED DRAFT AND/OR FINAL REPORT FILED IN THE AUTOMATED AUDIT DOCUMENTS?	X					
45.	WAS THE INDEPENDENT REFERENCED DRAFT AND/OR FINAL REPORTS THE FINAL VERSION?	X					
46.	DID THE AUDIT DOCUMENTS CONTAIN DOCUMENTATION OF THE WORK PERFORMED TO SUPPORT SIGNIFICANT CONCLUSIONS AND JUDGEMENTS (INCLUDING DESCRIPTIONS OF TRANSACTIONS AND RECORDS EXAMINED THAT WOULD ENABLE AN EXPERIENCED AUDITOR TO EXAMINE THE SAME TRANSACTIONS AND RECORDS)?	X					
47.	WERE THE AUDIT DOCUMENTS COMPLETED?	X					
48.	IF THE AUDIT RELIED ON ADP-GENERATED DATA, DID THE AUDITOR DETERMINE THE RELIABILITY OF THE DATA BY EITHER (A) CONDUCTING A REVIEW OF THE GENERAL AND APPLICATION CONTROLS IN THE COMPUTER BASED SYSTEMS OR (B) CONDUCTING OTHER TESTS?	N / A					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
49.	DID THE AUDIT DOCUMENTS CONTAIN:						
	a. FOR EACH DOCUMENT OR GROUP OF DOCUMENTS EXCEPT THE ADMINISTRATIVE DOCUMENTS, A PURPOSE, SOURCE, SCOPE, AND CONCLUSION?	X					
	b. SUMMARIES OR PROCEDURE SUMMARIES PREPARED FOR EACH AUDIT SEGMENT AND FINDING. AUDIT STEPS TO ENSURE "CONCLUSIONS" ARE APPROPRIATELY SUMMARIZED.	X					
	c. THE IDENTIFICATION OF SAMPLING USED, AND IF APPROPRIATE, WHETHER THE RESULTS CAN BE PROJECTED TO THE POPULATION.	X					
	1. HOW DID YOU JUDGMENTALLY, RANDOMLY OR STATISTICALLY SELECT THE SAMPLE?	X					
	2. WAS EVERY "nth" ITEM SELECTED? WERE THE SAMPLE ITEMS STRATIFIED? BY ITEM? BY DOLLAR AMOUNT?	X					
	3. WHAT WAS THE TOTAL UNIVERSE? WHAT WAS THE NUMBER OF ITEMS OUT OF THE TOTAL UNIVERSE?	X					
	4. WAS SAS USED FOR THE SAMPLING METHOD? DID SAS GENERATE THE NUMBER OF ITEMS TO REVIEW?	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

50.	DID THE AUDITORS IDENTIFY WHICH LAWS AND REGULATIONS ARE APPLICABLE TO THE AUDIT?	X					
-----	---	---	--	--	--	--	--

51.	DID THE AUDITORS TEST FOR ADHERENCE TO PERTINENT LAWS AND REGULATIONS?	X					
-----	--	---	--	--	--	--	--

52.	IF THERE WERE INDICATIONS OF FRAUD, ABUSE, IRREGULARITIES, OR ILLEGAL ACTS AND SIGNIFICANT VIOLATIONS OF PROVISIONS OF CONTRACT OR GRANT AGREEMENTS, DID THE AUDITORS: a. CONSIDER THE IMPACT OF THESE ACTS ON THE AUDIT RESULTS?	N / A					
-----	--	-------------	--	--	--	--	--

	b. EXERCISE PROFESSIONAL JUDGEMENT IN THE PURSUIT OF ILLEGAL ACTS TO ENSURE THAT POTENTIAL INVESTIGATIONS AND/OR LEGAL PROCEEDINGS ARE NOT COMPROMISED (1) BY CONSULTING WITH APPROPRIATE INVESTIGATORY STAFF AND/OR LEGAL COUNSEL BEFORE PROCEEDINGS OR (2) BY OTHER MEANS?	N / A					
--	--	-------------	--	--	--	--	--

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
	c. IF THE ABUSIVE ACTS COULD HAVE A MATERIAL OR SIGNIFICANT EFFECT ON THE AUDIT RESULTS AND THE AUDITOR WAS NOT ASKED BY INVESTIGATORS TO DEFER ADDITIONAL AUDIT WORK, WERE AUDIT PROCEDURES EXTENDED TO DETERMINE WHETHER THE ACTS OCCURRED, AND TO WHAT EXTENT?	N / A					
53.	IF NOTEWORTHY ACCOMPLISHMENTS WERE NOTED IN THE AUDIT DOCUMENTS, WERE THEY NOTED IN THE AUDIT REPORT?	X					
54.	IF SIGNIFICANT ISSUES REQUIRING FURTHER STUDY WERE NOTED IN THE AUDIT DOCUMENTS, WERE THEY NOTED IN THE AUDIT REPORT?	X					
55.	DID THE AUDIT REPORT PROPERLY ADDRESS PRIVILEGED OR CONFIDENTIAL INFORMATION?	N / A					
56.	IF THE AUDIT DOCUMENTS NOTED ANY OTHER EXCEPTIONS OR SUGGESTIONS FOR IMPROVEMENTS, WERE THEY ADDRESSED IN THE AUDIT REPORT OR MANAGEMENT LETTER?	X					
57.	ARE THERE OTHER NOTED DEVIATIONS FROM GAGAS OR OIG POLICIES AND PROCEDURES?		X				

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
58.	ARE THERE ANY THREATS TO INDEPENDENCE NOTED AFTER THE AUDIT REPORT WAS ISSUED? IF SO, DID AUDITORS ASSESS THE IMPACT ON THE AUDIT AND NOTIFY MANAGEMENT AND OTHER INTERESTED PARTIES OF THE IMPACT?						
59.	WHEN AN AUDIT IS TERMINATED BEFORE COMPLETION, DID THE AUDITORS DOCUMENT THE RESULTS OF THE WORK UP TO THIS DATE AND THE REASON FOR THE TERMINATION?						
<p>A JUDGMENTAL SAMPLE OF AUDIT FINDINGS WILL BE REVIEWED TO DETERMINE THE SUFFICIENCY, RELEVANCE, AND COMPETENCE OF THE EVIDENCE USED TO SUPPORT THE AUDIT FINDINGS' OPINIONS, CONCLUSIONS, AND RECOMMENDATIONS. AUDIT EVIDENCE SHOULD PROVIDE A FACTUAL BASIS FOR AUDIT OPINIONS, CONCLUSIONS, AND RECOMMENDATIONS. ALL AUDIT EVIDENCE SHOULD STAND THE TESTS OF SUFFICIENCY, COMPETENCY, AND RELEVANCY. WHENEVER EVIDENCE DOES NOT MEET THE STANDARDS OF SUFFICIENCY, COMPETENCY, AND RELEVANCY, THE AUDITOR'S WORK REMAINS UNFINISHED. WHEN THE AUDITOR EXPRESSES AN OPINION, IT MUST BE BASED ON INCONTROVERTIBLE EVIDENCE.</p>							
AUDIT FINDING(S): (NAME OF FINDINGS)							
	<p>WAS THERE SUFFICIENT EVIDENCE TO SUPPORT THE AUDITOR'S FINDINGS?</p> <p>(Sufficiency is the presence of enough factual and convincing evidence to support the auditors' findings, conclusions, and recommendations. Evidence is sufficient if it is so factual, adequate, and convincing that it would lead a prudent person to the same conclusion as the auditor. This, of course, would be a matter of judgment; but the judgment should be objective.)</p>	X					

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
	<p>WAS THE EVIDENCE RELEVANT TO ITS USE?</p> <p>(The information used to prove or disprove an issue is relevant if it has a logical relationship to that issue. Information that has no logical relationship to the issue is irrelevant and, therefore, should not be included as evidence.)</p>	X					
	<p>WAS THE EVIDENCE COMPETENT?</p> <p>(Competence means that the evidence must be valid and reliable. It should be the best that is reasonably obtainable. In evaluating the competence of evidence, the auditors must carefully consider whether reasons exist to doubt its validity or completeness. If there is a reason for doubt, the auditors should obtain additional evidence or reflect the situation in the audit report.)</p>	X					

Exhibit E



UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, D.C. 20415-0001

May 27, 1992

MEMORANDUM FOR HARVEY THORP
ASSISTANT INSPECTOR GENERAL
FOR AUDITS

JIMMY ANDREWS
ASSISTANT INSPECTOR GENERAL
FOR INVESTIGATIONS

KENNETH HUFFMAN
ASSISTANT INSPECTOR GENERAL FOR
POLICY, RESOURCES MANAGEMENT AND OVERSIGHT

FROM: JOSEPH R. WILLEVER
DEPUTY INSPECTOR GENERAL

SUBJECT: OIG Training and Employee Development
Policies and Procedures

Attached is OIG's Training and Employee Development Policies and Procedures. Sections 1-6 address general training policy and procedures affecting all OIG employees. Section 7 exclusively addresses training for employees engaged in government auditing activities and Section 8 is reserved to address training for criminal investigators. Please ensure that your staff receives a copy of the attached information.

This issuance incorporates OIG policy statements, precedent decisions and memoranda regarding training, as well as recent changes in training regulations. Appendix A contains procedures for completing the SF-182. All forms should be completed in compliance with these instructions.

Appendix A contains new procedures for requesting approval to attend training. When no funds will be expended, SF-182 (5 part) is to be completed to receive credit for attendance at in-house training or outside activities. The SF-182 (10 part) is to be used to request attendance at OPM and out-of-agency training and development activities, i.e., Federal, State, and local or other professional conferences and job-related courses when funds will be expended.

Also outlined in Appendix A are new procedures to document attendance and completion of training. Copy 9 of the SF-182 (10 Part) form entitled "Evaluation," or Copy 4, "Evaluation," of SF-182 (5 Part) form will be returned by Management Resources and

Administration Branch to the employee and should be filled out after completion of a specific course. The immediate supervisor must sign the copy to certify completion of the course and return the copy to Management Resources and Administration Branch. The completed and signed copy must be submitted to receive credit for attendance at a training function.

For all employees subject to GAO's CPE requirements, please review Section 7, "Crediting Training for CPE Purposes." Section 7-7, "Measuring Compliance of the 80-hour Requirement," establishes new policy for measuring the 80-hour requirement. OIG will review the 80-hour requirement on a two-year fixed period. The two-year fixed period began on January 1, 1991, and will end on December 31, 1992.

Employees should also take note of Section 5-2, "Training Through Non-Government Facilities." OIG will require employees to complete the "Employee's Agreement to Continue in Service" prior to attending a course provided by a non-Government facility. The reverse of copy one of the SF 182 is used to document the employee's agreement to continue to work for OIG for a specified length of time, or to reimburse the Government for the costs incurred if the specified time of continued employment is not completed. This requirement will be waived in the following instances: 1) the training does not exceed 80 hours, 2) correspondence courses, or 3) the employee transfers to another government agency.

If you have any questions, please contact (b) (6) Management, Resources and Administration Branch on 606-1185.

Attachment

cc: Executive Assistant
Special Counsel

**OIG TRAINING AND EMPLOYEE DEVELOPMENT
INTERIM POLICIES AND PROCEDURES**

TABLE OF CONTENTS

SECTION 1	-	GENERAL
1-1		PURPOSE
1-2		POLICY
1-3		AUTHORITY
1-4		REFERENCES
SECTION 2	-	TRAINING PROGRAM
2-1		RESPONSIBILITIES
2-2		TRAINING OPTIONS
SECTION 3	-	DOCUMENTATION
3-1		INTERNAL TRAINING
3-2		EXTERNAL OR FORMAL TRAINING
3-3		RECORDS RETENTION
SECTION 4	-	ALLOWABLE TRAINING COSTS
4-1		TRAINING EXPENSES
4-2		LIMITATIONS
SECTION 5	-	SELECTING TRAINING SOURCES
5-1		SELECTING TRAINING
5-2		TRAINING THROUGH NON-GOVERNMENT FACILITIES
SECTION 6	-	SELECTION AND ASSIGNMENT OF EMPLOYEES FOR TRAINING
6-1		GENERAL
6-2		LIMITATIONS
SECTION 7	-	CREDITING TRAINING FOR CPE PURPOSES
7-1		INTRODUCTION
7-2		APPLICABILITY OF REQUIREMENTS
7-3		QUALIFYING PROGRAMS
7-4		UNACCEPTABLE PROGRAMS AND SUBJECTS
7-5		MEASURING HOURS
7-6		CPE CREDIT DETERMINATION
7-7		MEASURING COMPLIANCE OF THE 80-HOUR REQUIREMENT
SECTION 8	-	TRAINING PROGRAM FOR CRIMINAL INVESTIGATORS
8-1		CONDITIONS OF EMPLOYMENT
8-2		EXTERNAL TRAINING
APPENDIX A	-	THE SF-182 (10 PART) AND (5 PART)

SECTION 1. TRAINING AND DEVELOPMENT

- 1-1 PURPOSE. This issuance establishes the policies and procedures for the training and development of OIG personnel. Section 7 addresses training for employees engaged in government audit activities. Section 8 is reserved to address training for criminal investigators.
- 1-2 POLICY. The overall goal of OIG's training policy is to develop and improve employees' knowledge, skills and abilities in the performance of official duties. Management retains the right to approve or disapprove training requests based on the availability of training funds, workload of the office, and the relevancy of the course to the official mission of the office.
- 1-3 AUTHORITY. The following OIG officials are authorized to approve training:

AUTHORIZED OFFICIAL: Inspector General
Deputy Inspector General
Assistant Inspectors General
Division Chiefs
Special Counsel

SCOPE OF AUTHORITY: The Inspector General and Deputy Inspector General have office-wide authority. The Assistant Inspectors General, Division Chiefs and Special Counsel have authority for all employees supervised.

- 1-4 REFERENCES. This issuance is in accordance with Title 5, Chapter 41, Chapter 410 of the Federal Personnel Manual, Chapter 410 of the OPM Administrative Manual, and the Government Auditing Standards.

SECTION 2. TRAINING PROGRAM

- 2-1 RESPONSIBILITIES. Direct responsibility for employee development is vested in OIG supervisors. Individual supervisors are responsible for assessing and evaluating the developmental needs of their employees and taking appropriate actions to meet development objectives.

The Office of Policy, Resources Management and Oversight (PRMO), Management Resources and Administration Branch (MRAB), is responsible for maintaining individual training files, tracking the number of training hours for each

employee and periodically providing reports to OIG management regarding training. PRMO also provides guidance and assistance to management in planning, establishing and promoting the OIG training program.

2-2 TRAINING OPTIONS.

- a. Formal Training - Classroom instruction at Government or non-Government facilities which provide job related training and skills to employees.
- b. Special projects/assignments - This is a form of on-the-job-training for which the duties are not part of the regular job but can be assigned to develop employees in special areas.
- c. Self-study - This may take the form of a mentor who can outline a program of reading assignments or programmed self-instructional packages.
- d. Details/rotational assignments - The use of details is not always available, however when available, details do enable employees to gain new skills and experience.
- e. Correspondence Courses - Various vendors, such as OPM and USDA, offer training through correspondence courses.
- f. Attendance at conferences, seminars, etc. - These are excellent sources for updating and enhancing professional knowledge and skills.
- g. Internal Training - Periodically, the OIG will develop and/or present customized courses, seminars, and briefings designed to develop specific skills. This internal training will help bridge the gap between formal education and experience.

Participation in professional societies and serving as an outside speaker are also highly encouraged as a means not only for individual development but also for OIG representation with the professional community.

SECTION 3. DOCUMENTATION

- 3-1 INTERNAL TRAINING. PRMO maintains a file for each training course, seminar, etc. Internal training is to be documented on the SF-182 (5 part) form. (See Appendix A) Documentation for internal training may also include the presentation's agenda or outline which indicates the name(s) and qualifications of the instructor(s); the topic(s) covered; the program's learning objectives; a description of any materials used; the location where the program was given; and the date(s) and length of the program. Employees

subject to the CPE requirements must submit the above information to receive CPE credits. The file also contains a certification of attendance and the number of hours earned by each participant.

3-2 EXTERNAL OR FORMAL TRAINING. All training provided by Government or non-Government facilities in which there are expenses should be documented on the SF-182 (10 part). The following steps should be taken to ensure proper registration:

a. Training Request. Employees are responsible for ensuring that an SF-182 (10 part) form is submitted to PRMO along with other descriptive materials which contain course-specific information including a course description, the date(s) of training, hours of training and tuition.

b. Review and Clearance. The SF-182 is reviewed and signed by the employee's immediate supervisor and is submitted to the second-line supervisor, if appropriate. The SF-182 must be approved by the appropriate authorizing official. See Appendix A for instruction in completing the SF-182.

The signed SF-182 is returned to PRMO for approval of expenditure of training funds and to ensure that copies of the form are distributed to the appropriate parties.

c. Proof of Attendance. At the completion of training, the employee is responsible for providing PRMO copy 9 of the SF-182 "Evaluation." If appropriate, the information regarding course attendance may also be submitted, i.e., a notice of the grade received from a university or college; a certificate of completion from the program sponsor; a notice of the number of CPE hours earned; or an outline of the course demonstrating attendance or participation as an instructor or discussion leader.

3-3 RECORDS RETENTION. All training records maintained by PRMO will be maintained for a four year period. A copy of certificates, grades, etc. and the SF-182 will also be permanently maintained in the employee's Official Personnel Folder maintained by OPM Personnel.

SECTION 4. ALLOWABLE TRAINING COSTS

4-1. TRAINING EXPENSES. Only the actual cost of training and those expenses incurred as a direct result of training will be paid. These expenses include regular salary; the cost of tuition and books; any associated travel and subsistence in accordance with policies and procedures.

4-2 LIMITATIONS.

a. All training must be in fields which are or will be directly related to the performance of official duties by the employee trained and for the purpose of increasing that employee's knowledge and skills in the performance of official duties.

b. Training at colleges or universities or attendance at a review course generally must be accomplished during nonduty hours.

The OIG values professional achievements such as, obtaining pertinent certifications, or obtaining related advanced degrees. While professional development is supported by the OIG with monetary aid and time off, the amounts of each can vary. Due to training budget limitations, OIG will authorize payment of up to 75 percent of the cost for attendance at a review course. Depending on the availability of funds, OIG may pay 75 percent of the cost of college or university courses providing the courses directly relate to the performance of official duties.

c. Travel cost in addition to training costs for out-of-the area training in Government facilities should be held to the minimum by using the closest Government facility that meets training needs. For example, when using OPM Executive Training Centers, select the Center that offers the needed training and is closest to Washington, D.C., unless the differences in travel expenses are insignificant.

d. No employee having less than one year of current, continuous civilian service is eligible for training in non-Government facilities unless the Inspector or Deputy Inspector General determine that postponement of the training would be contrary to the mission of the office.

SECTION 5. SELECTING TRAINING SOURCES

5-1 SELECTING TRAINING. It is OIG policy to select training resources designed to achieve clear and relevant training and development objectives with minimum expenditure of time and resources. Wherever feasible the following OIG guidelines should be followed:

a. Generally, Government training facilities will be used to train OIG employees. OIG will not use private training vendors if comparable training can be provided by Government facilities. This not only demonstrates our support for Federal training establishments, but also provides training at a reasonable cost. When private training vendors are used, they must, if at all possible, be within the local commuting area in order to minimize travel expenses.

b. To the extent that training and travel funds are available, OIG will pay for employees who are members of professional organizations to attend conferences providing the subject matter will further the interests of the employee and the office.

Employees who are not members (either individually or through OIG-group memberships) of an organization will not be permitted to attend conferences except in unusual circumstances, i.e., last minute substitution for members who cannot attend or when the office has a critical need to have an employee(s) trained in an area that is being offered as part of the conference.

5-2 TRAINING THROUGH NON-GOVERNMENT FACILITIES. All OIG employees will be required to complete the "Employee's Agreement to Continue in Service," prior to attending a course provided by a non-Government facility. The reverse of copy one of the SF-182 is used to document the employee's agreement to continue to work for OIG for a specified length of time, or to reimburse the Government for the costs incurred if the specified time of continued employment is not completed. The Inspector General may waive this requirement for the following reasons:

- a. Training that does not exceed 80 hours,
- b. Correspondence courses, or
- c. The employee transfers to another government agency.

SECTION 6. SELECTION AND ASSIGNMENT OF EMPLOYEES FOR TRAINING

6-1 GENERAL. It is the policy of this office to ensure fair and equitable treatment in the selection and assignment of employees for training.

6-2 LIMITATIONS. Whenever the number of employees nominated for training or the number of attendees at a professional conference must be limited, the following factors will be considered in determining who will attend:

- a. the current status of the employee's workload;
- b. the employee's individual membership in the organization;
- c. the time elapsed since the last class or conference the employee attended; and/or
- d. the benefit that one employee would receive from the conference or the course in comparison to another employee, based on the actual duties and experience of the employees involved.

SECTION 7. CREDITING TRAINING FOR CPE PURPOSES

7-1 **INTRODUCTION.** The qualifications standard in Government Auditing Standards, 1988 Revision, places responsibility on the audit organization to ensure that audits are conducted by staff who collectively have the knowledge and skills necessary for the audits being conducted. In order to meet the qualifications standard, auditors should complete the following CPE (continuing professional education) requirements:

- a. Auditors responsible for planning, directing, conducting or reporting on a government audit should complete, every two years, at least 80 hours of CPE which contribute to the auditor's professional proficiency.
- b. At least 20 hours should be completed in any one year of the two year period.
- c. Individuals responsible for planning, directing, conducting a substantial portion of the field work, or reporting on a government audit should complete at least 24 of the 80 hours of CPE in subjects directly related to the government environment and to government auditing. If the audited entity operates in a specific or unique environment, auditors should receive training that is related to that environment.

The individual auditor is responsible, as well as the audit organization, for seeking opportunities for CPE, for successful completion of CPE programs, and for providing documentation of the CPE hours completed. In addition, individual auditors are responsible for monitoring their own progress toward meeting the CPE requirement.

7-2 **APPLICABILITY OF REQUIREMENTS.** The 80-hour CPE requirement applies to all OIG auditors or employees who are responsible for planning, directing, conducting or reporting on yellow book audits.

While the following individuals should be qualified to perform their assigned tasks, they are not usually subject to CPE requirements.

- a. Internal experts and specialists, such as, actuaries, attorneys, and statisticians;
- b. Auditors performing nonaudit activities within the OIG, such as individuals assigned to staff positions in budgeting, policy, personnel, or training;

- d. Education and development programs presented at conferences, conventions, meetings, seminars, and workshops of professional organizations; and
- e. Training programs presented by other audit organizations, educational organizations, government agencies, foundations, and associations.

The criteria for assessing individual study programs are:

- a. Participants are required to register for the program, and
- b. The program sponsor provides evidence of satisfactory completion.

Examples of individual study programs that could qualify for CPE hours:

- a. Correspondence courses, and
- b. Courses given through audio cassette tapes, video tapes, and computers.

For all individual study programs, the supervisor must verify completion of the program for purposes of CPE credit prior to the submission of the "Evaluation" to PRMO.

Other professional activities that may qualify include serving as a speaker, instructor, or discussion leader at group programs that qualify for CPE hours and publishing articles on subjects or topics related to the auditor's expertise and/or work that contributes to their professional proficiency.

7-4 UNACCEPTABLE PROGRAMS AND SUBJECTS. Examples of programs or subjects and topics that do not qualify as acceptable for CPE purposes include, but are not limited to:

- a. On-the-job training;
- b. Basic/elementary courses in subjects and topics in which the auditor already has the necessary knowledge and skills;
- c. Programs that are not designed to maintain and/or enhance professional proficiency, such as information on subjects and topics for the general public (e.g., resume writing, improving parent-child relations, personal development, retirement planning);
- d. Sales-oriented programs to demonstrate office equipment, such as computers or communications systems;

- e. Programs covering the OIG's administrative operations; and
- f. Business sessions at professional organizations, conferences, conventions, and meetings.

7-5 MEASURING HOURS. A CPE hour is granted for each 50 minutes of participation in programs and activities that qualify. A number of sponsoring organizations, such as the U.S. Department of Agriculture Graduate School and the Institute of Internal Auditors, certify hours of attendance on this basis.

CPE hours are granted in whole hours only. For example, a CPE activity lasting 90 minutes will count as one CPE hour while an activity lasting 40 minutes will not count. A one day program consisting of eight hours of training will count as eight CPE hours. At conferences and conventions where individual presentations are less than 50 minutes, the sum of the presentations is considered as one total program. For example, five 40 minute presentations equals 200 minutes or four CPE hours.

Participants receive CPE hours only for the actual time they attend the program.

For university or college credit courses, each semester hour credit equals 15 CPE hours and each quarter hour credit equals 10 CPE hours. For noncredit short courses each classroom hour equals one CPE hour.

Participants in correspondence or individual study programs are granted CPE hours in an amount equal to one-half of the average completion time when that figure is known. For example, a correspondence course that takes an average of 600 minutes to complete would be granted 300 CPE minutes, or 6 CPE hours. If the program has not been pretested and the average completion time is not known, the participant is granted CPE hours in an amount equal to one-half of the time he or she actually spent on the program.

Speakers, instructors and discussion leaders at programs that qualify for CPE receive CPE hours for preparation and presentation time to the extent the subject matter contributes directly to their professional proficiency. One CPE hour is granted for each 50 minutes of presentation time, and up to two additional hours of CPE may be granted for advance preparation for each 50 minutes of their presentation.

An individual should not receive CPE hours for either preparation or presentation time for repetitious presentations that they make, unless the subject matter involved was changed significantly. The maximum number of

CPE hours that may be granted to an individual speaker, instructor, or discussion leader cannot exceed 40 hours for any two-year period.

Published writings by auditors on subjects or topics related to their expertise and/or work that contribute directly to the auditor's professional proficiency qualify for CPE hours in the year they are published. One hour of CPE is granted for each hour devoted to writing an article or book that is published. However, CPE hours for published writings cannot exceed 20 hours for any two-year period.

7-6 CPE CREDIT DETERMINATION. Upon receipt of proof of attendance at an external training program or activity, PRMO determines whether the program or activity qualifies for CPE credit in accordance with GAO standards and calculates the creditable hours. For internal training programs and activities, employee's CPE records will be updated when PRMO receives the record of attendance and the number of CPE hours earned by each participant.

7-7 MEASURING COMPLIANCE OF THE 80-HOUR REQUIREMENT. The yellow book states that all of the CPE requirements should be met within 2 years from the yellow book's effective date, January 1, 1989. Therefore, the first 2 year period ended on December 31, 1990. To simplify the administration of the CPE program, OIG's policy is that the 80-hour requirement will be reviewed on a fixed 2 year period. The second period began on January 1, 1991 and will continue to December 31, 1992.

For entry-level employees or for other auditors hired or assigned to OIG after the beginning of the 2 year period, a pro rata number of hours will be determined. Entry-level auditors with less than one year of service in OIG will, at a minimum, be provided with training that provides a sound understanding of the requirements and expectations of government auditing and the needed skills and tools to effectively meet these requirements.

SECTION 8 - TRAINING FOR CRIMINAL INVESTIGATORS

8-1 CONDITIONS OF EMPLOYMENT. Newly hired criminal investigators must successfully complete the basic Criminal Investigator Course held at the Federal Law Enforcement Training Center (FLETC). The only exception to this requirement is for agents who have completed comparable special agent or law enforcement training.

8-2 EXTERNAL TRAINING. Generally, external training for criminal investigators will not be provided until the employee has successfully completed the basic Criminal

Investigator Course at FLETC. Requests for external training must also be consistent with other OIG policies as stated throughout this document, specifically in Section 4.2 regarding limitations.

APPENDIX A: THE SF-182 (10 PART) and (5 PART)

The SF-182 (10 part) is appropriately used to request attendance at a variety of OPM and out-of-agency training and development activities, i.e., Federal, State, and local or other professional conferences and job-related courses needed to keep job skills up-to-date or to improve job performance. The SF-182 (5 part) is to be completed when no funds will be expended for the training. The SF-182 is used Government-wide and serves the following major functions:

TO REQUEST TRAINING

An employee who wishes to attend either OPM training, or out of agency training usually initiates the SF-182. By completing the SF-182 in the appropriate manner, the employee will provide the required work-related biographical information, course-related information, benefits to be derived by the Government and fiscal information.

Once completed, the SF-182 should be submitted to your immediate supervisor at least three weeks prior to the registration deadline for the program. Copy 2 of the SF-182 will be returned to the employee and serve as a notification of approval or disapproval to attend the course.

AS AN AUTHORIZATION FOR TRAINING AND TRAVEL

The SF-182 signed by the Authorizing Official is an official authorization to expend funds for travel to attend training, but must be supplemented with a travel order, OPM Form 2769B. A copy of the approved SF-182 should always be submitted with the employee's travel voucher.

CANCELLATION OF A REQUEST FOR TRAINING

The employee is responsible for notifying the Training Officer at the earliest possible date in cases of non-attendance. Every effort should be made to avoid penalties or payment for non-attendance. When an employee cannot attend a training course for which he/she has been approved, and another student is going to substitute, the employee or the supervisor must notify the Training Officer at the earliest possible date.

TO DOCUMENT COMPLETION OF TRAINING

Copy 9 "Evaluation" of the 10 part form (Copy 4 of the 5 part) will be returned to the employee and is to be filled out after completion of the course. The immediate supervisor must sign Copy 9 to certify completion of the course and return the form to MRAB. This copy must be submitted to receive credit for attending a course.

A copy of the SF-182 is filed in the employee's Official Personnel File (OPF) along with appropriate grade records and certificates. In addition, a copy of the SF-182 is kept by the Training Officer in Management Resources and Administration Branch.

INSTRUCTIONS FOR COMPLETION OF THE SF-182

As you read through these instructions, reference the sample SF-182 attached. All 10 copies of this form must be clear and correct.

Item A - [Agency, code agency...]

Enter OM-00-1000

Item B - [OFFICE USE ONLY]

Leave Blank

Item C - [Request Status]

Check appropriate block

Section A - TRAINEE INFORMATION

Item 1 - [Applicant's Name]

Insert your name, last name first. Then, enter the first five letters of your last name in the shaded box in capital letters.

Item 2 - [Social Security Number]

Enter your nine digit Social Security number, but do not hyphenate.

Item 3 - [Date of Birth]

Completion optional

Item 4 - [Home Address]

Completion optional

Item 5 - [Home Telephone Number]

Completion optional

Item 6 - [Position Level]

Check appropriate box

Item 7 - [Organization Mailing Address]

OPM - Office of the Inspector General
1900 E Street, Room 6400
Washington, DC 20415

Item 8 - [Office Telephone Number]

Enter your ten digit office telephone number.

Item 9 - [Continuous Civilian Service]

Enter the number of years and months of continuous non-military Government service, as of the starting date of the training being requested.

Item 10 - [Number of prior non-Government training days]

Enter number of days of agency-paid or reimbursed training attended at a non-Government program (such as a college course) during the same fiscal year as the training being requested. Required item to comply with 5 U.S.C., Chapter 41.

Item 11a [Position title/function]

Enter your official title or position as it appears on personnel forms (e.g. Auditor, Secretary, Criminal Investigator, etc.)

Item 11b [Applicant handicapped or disabled]

If special equipment or arrangements are required because of a disability or handicap, check the box and provide a description of the requested accommodation as an attachment.

Item 12 - [Pay plan/series/grade/step]

Enter your official pay plan, series, grade, and step as it appears on personnel forms (e.g. GS-511-12/2)

Item 13 - [Type of appointment]

Enter abbreviation of your type of appointment (e.g. Career Conditional - CC, Career - C, Temporary - T, etc.)

Item 14 - [Education level]

Enter the number of years of education normally associated with formal U.S. education (e.g. H.S. = 12).

Section B - TRAINING COURSE DATA

Item 15A [Name and Address of Training Vendor]

Enter the complete mailing address of the training vendor.

Item 15b [Location of training site]

If the training site is different from the vendor's mailing address, type the complete location of the site.

Item 16 - [Course title and training objectives]

Enter the official title of the course, seminar, conference, etc. Also, concisely state the objective(s) of the program and the relationship to the applicant's job which justify expenditure of funds.

Item 17 - [Catalog/Course No.]

If the vendor uses a code to denote the course, enter it here. Many vendors require this entry to facilitate processing of the application.

Item 18 - [Training period]

Enter the year, month, and day the course begins and ends.

Item 19 - [No. of course hours]

The number of course hours is the number of hours to be attended. This is entered in 4 digits.

Item 20 - [Training codes]

Please see the instructions printed on the back of the SF-182. Select an appropriate code for each item.

Section C - ESTIMATED COSTS AND BILLING INFORMATION

Item 21 - [Direct costs and appropriation/fund chargeable]

and

Item 22 - [Indirect costs and appropriation/fund chargeable]

It is not necessary to include travel costs on the SF-182, unless it is integral to registration, i.e., hotel bill is included in registration but itemized separate from the cost of the course. The total is to be entered in 4 digits. Be sure to enter the totals in 21d and 22d, even if the total is 0000.

Do not fill in anything in the "Appropriation/fund" box.

Item 23 - [Document/Purchase Order/Requisition No]

Do not fill in this item.

Item 24 - [8 digit station symbol]

Do not fill in this item.

Item 25 - [Billing Instructions]

U.S. Office of Personnel Management
Budget and Finance, Room 2326
1900 E Street, NW
Washington, DC 20415

Section D - APPROVALS

Item 26a [Immediate supervisor - Name and Title]

Enter the name, title and telephone number of your immediate supervisor.

Item 27 - [Second-line supervisor - Name and title]

Enter the name, title and telephone number of the Division Chief, Deputy AIG, AIG or Deputy IG.

Item 28 - [Training Officer - Name and title]

Enter MRAB Training Officer, Angela P. Cole.

Section E - APPROVAL/CONCURRENCE

Item 29a [Authorizing Official]

Enter the name, title and telephone number of the Division Chief, AIG, DAIG, or Deputy IG.

Section F. - CERTIFICATION OF TRAINING COMPLETION

Item 30a [Certifying Official - Name and Title]

Enter the name and title of the Training Officer

- Use one-part form for work-sheet. Privacy Act information on reverse of copy 8.
- Please read instructions on the reverse side of the last copy before completing this form.
- Instructions for handling and completing copies 3, 4, 5 and 6 appear on reverse of copy 3.
- Please type form and do not remove carbons and copies 1-9 from set.
- Typewriter tab stops indicated by ▽ below.

REQUEST, AUTHORIZATION, AGREEMENT AND CERTIFICATION OF TRAINING

A Agency code, agency subelement and submitting office number
Example—12-34-5678

01

B. OFFICE USE ONLY

C. Request status: Major Minor
Initial or Re-submission Correction or Cancellation

Section A—TRAINEE INFORMATION

1 Applicant's name (Last, First, Middle Initial) (b) (6)		Enter first 3 letters of last name COLINE	2 Social Security Number 6789	03	3 Date of birth (year and month) 58/05	04
4 Home address (Number, street, city, State, ZIP code) 611 Smith Street Nowhere, Virginia 22700		5 Home telephone Area code Number 703 555-1212		6 Position (See Manual for details) <input checked="" type="checkbox"/> Non-supervisory <input type="checkbox"/> Supervisory		
7 Organization mailing address (Branch, Division, Office, Bureau, Agency) OPM/OIG, 1900 E Street, NW., 6400 Washington, DC 20415		8 Office telephone Area code Number Extension 202 606 1200		9 Continuous civilian service Years Months 12 3		
11a. Position title/function Auditor	11b. Applicant handicapped or disabled (See instructions)	12 Pay plan series grade step GS-511-12/2		13 Type of appointment C 16		

Section B—TRAINING COURSE DATA

15a. Name and mailing address of training vendor (No. street, city, State, ZIP code) OPM/OWTDS 1121 Vermont Ave., NW., P.O. 7230 Washington, DC 20044-7230		15b. Location of training site (if same, mark box) <input type="checkbox"/>	
16. Course title and training objectives (Benefits to be derived by the Government) Technology Issues in Management - To understand the impact of technology on management.			
17. Catalog / Course No	18. Training period (6 digits) Year Month Day 9201 06	19. No. of course hours (4 sig. figs.) a. During duty 0008 b. Non-duty 0000 c. TOTAL 0008	20. Training codes (See instructions) a. Purpose 08 b. Type 09 c. Source 1 d. Special training 0

AGENCY USE ONLY

Section C—ESTIMATED COSTS AND BILLING INFORMATION

Section D—APPROVALS

21. Direct costs and appropriation / fund chargeable			26a. Training officer—Name and title (b) (6) Chief, MRAB			Area code / Tel. No. / Extension 202/606-1200		
Item	Amount Dollars Cents		Appropriation / fund			b. Signature		
a. Tuition	\$	860 00				Date		
b. Books or materials						27a. Second-line supervisor—Name and title Kenneth D. Huffman Asst. IG for PRMO		
c. Other (Specify)						Area code / Tel. No. / Extension 202-606-1200		
d. Enter 4 digits in dollar column TOTAL 12						b. Signature		
22. Indirect costs and appropriation / fund chargeable			26b. Training officer—Name and title (b) (6) Training Officer			Area code / Tel. No. / Extension 202-606-1200		
Item	Amount Dollars Cents		Appropriation / fund			b. Signature		
a. Travel	\$					Date		
b. Per diem						27b. Authorizing official—Name and title Kenneth Huffman Asst. IG for PRMO		
c. Other (Specify)						Area code / Tel. No. / Extension 202-606-1200		
d. Enter 4 digits in dollar column TOTAL 13	\$	0000				b. Signature		
23. Document / Purchase Order / Requisition No			28. Section E—APPROVAL / CONCURRENCE			28a. Approving official—Name and title (b) (6) Training Officer		
24. 8-Digit station symbol Example—12-34-5678			28b. Approving official—Name and title (b) (6) Training Officer			Area code / Tel. No. / Extension 202-606-1200		
25. BILLING INSTRUCTIONS (Furnish invoice to) U.S. Office of Personnel Management Finance and Budget Division 1900 E Street, NW., Room 2326 Washington, DC 20415			28c. Approving official—Name and title (b) (6) Training Officer			Area code / Tel. No. / Extension 202-606-1200		
			b. Signature			Date		



UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, D.C. 20415-0001

Exhibit F

January 25, 1995

MEMORANDUM FOR OFFICE OF AUDITS STAFF

FROM: HARVEY D. THORP
ASSISTANT INSPECTOR GENERAL
FOR AUDITS

SUBJECT: Office of Audits Policy on
Administrative Leave for Professional Exams

The purpose of this memorandum is to set Office of Audits (OA) policy relative to the granting of administrative leave for OA staff taking professional exams.

POLICY

The Office of the Inspector General (OIG), OA, will grant administrative leave, as described below, to employees preparing for and taking recognized professional exams. Administrative leave will be granted in connection with only one recognized professional certification per employee.

TEST DAYS

1. For the first sitting as an employee of the OPM OIG, the OIG will grant administrative leave to all OA staff for days where the staff person is actually taking a recognized professional exam. For example, two days administrative leave will be granted for taking the full CPA exam or, if not sitting for the full exam, one/two day(s) will be granted for days where the employee is actually taking exam parts.
2. If a second sitting is necessary for a specific recognized professional exam, administrative leave will be granted for the actual test days involved.
3. No administrative leave will be granted for taking additional testing (i.e., 3rd or 4th sittings for the same exam or any sittings for other certifications). However, OA staff may take such additional testing on approved annual leave or, if circumstances permit, on the basis of compensatory time earned prior to the test days.

STUDY DAYS

1. The OIG will grant OA staff two days administrative leave for study and preparation in connection with a recognized professional exam on a one time basis only. That is, two days study/preparation leave will only be granted for the initial taking of a recognized professional exam (or for taking parts of an exam if the two study days were not previously granted).
2. Time off for study beyond the two days allowed, such as study days needed for a second or subsequent sitting for the same certification, will be on the basis of approved annual leave or, if circumstances permit, on the basis of compensatory time earned prior to the study days.

DOCUMENTATION

1. To obtain administrative leave, staff members should prepare a written request to their division chief showing the exam to be taken, the dates the staff member will be sitting for the exam, and the specific days and number of hours of administrative leave requested.
2. After approval by the division chief, the memorandum should be given to the time keeper for Time and Attendance purposes and a copy should be forwarded to the OIG Training Coordinator, presently Shirley Lynch, for filing in the employees training file.
3. All employees will be required to provide documentation showing that the employee actually used Test Days administrative leave in a test taking environment, as expected.

In implementing this policy, supervisors will make every effort to provide opportunities to earn compensatory time for preparing for and taking professional exams.

This policy is effective immediately.

U.S. OFFICE OF PERSONNEL MANAGEMENT

Office of the Inspector General

OIG Training Request and CPE Tracking System

User's Guide

Table of Contents

How do I log on to the system?	2
How do I submit a request for training?	6
How do I determine the status of a training request?.....	9
What do I do after I have completed the course?.....	13
How do I know how many CPE hours I have and which courses I have taken?.....	20
How do I change my password?	22
Who do I contact if I am having problems with the system?.....	22

©Office of Personnel Management
Office of the Inspector General
1900 E. Street N.W. Rm. 6400
Washington, DC 20415

Introduction

Welcome to the OIG's Continuing Professional Education (CPE) Training Registration and Tracking System. This system allows you to submit your request for training, monitor the approval/registration status and submit your training certificate electronically. It can also be used to quickly verify your training history and determine if additional CPEs are required to meet your minimum "yellow book" requirements. (Note: Please maintain a hard copy of the completion certificate in your personal files.) We will guide you through a step by step process of each activity. If you have any questions feel free to contact (b) (6) (b) (6) or Lewis Parker (b) (6).

How do I log on to the system?

To begin the log on process you must first open your Internet Explorer. Then access the OIG web portal at the following address: (b) (7)(E). You should see the following screen (see next page).

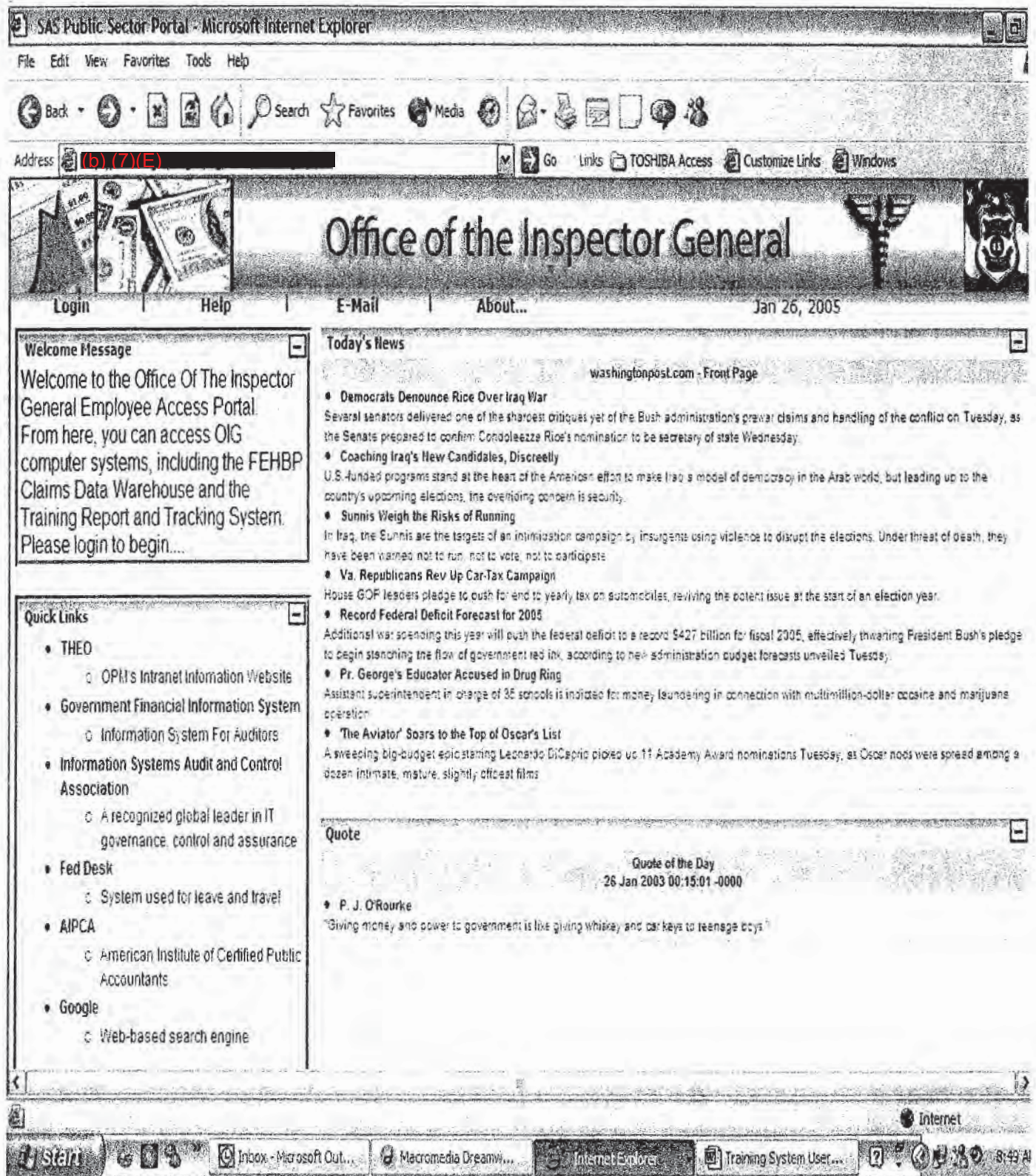


FIGURE 1. OIG Portal HomePage
 In the upper left hand corner of the screen, click on the “Login” link. This will take you to the following screen on the next page:

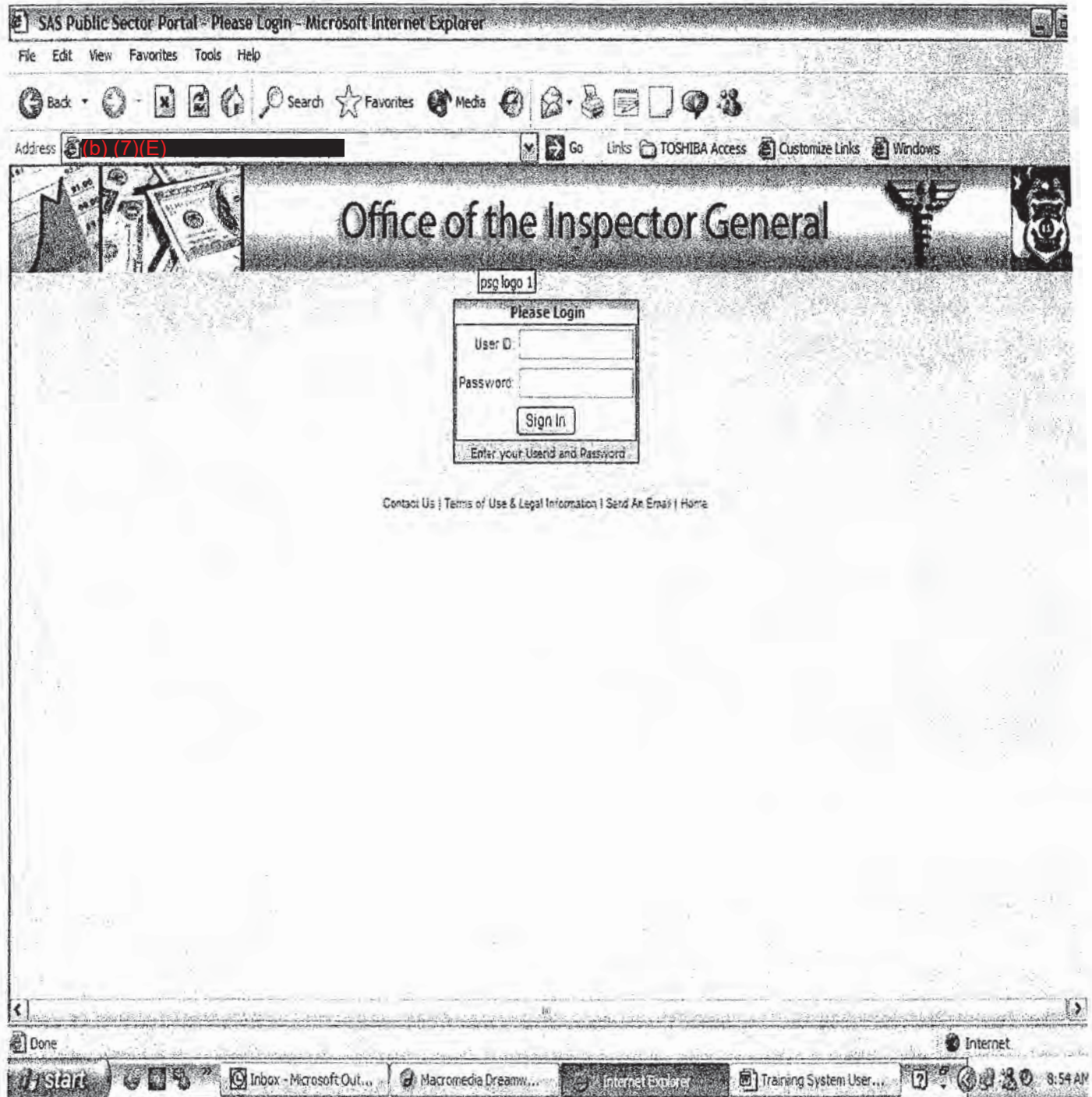
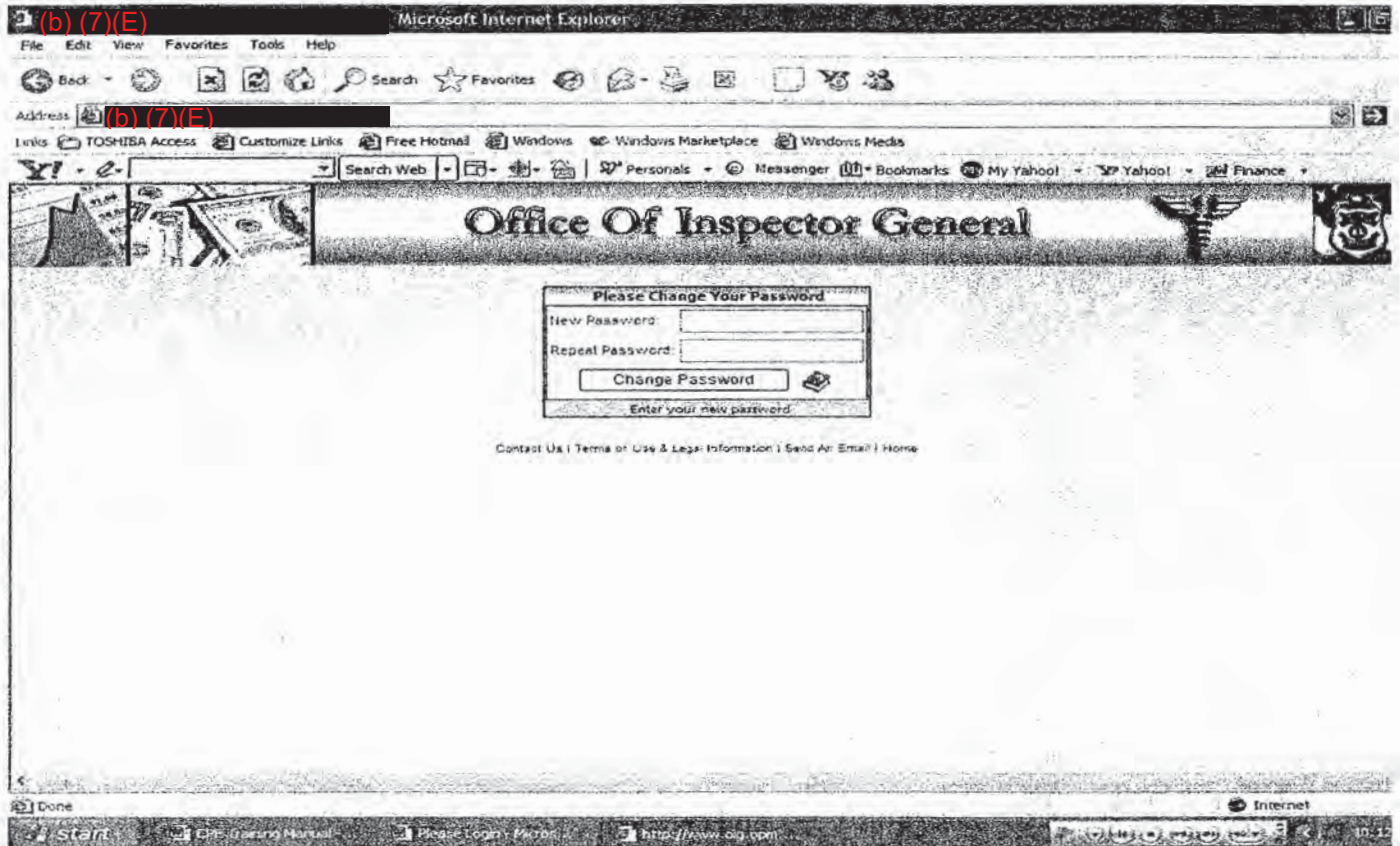


FIGURE 2. OIG Portal Login Page.



Password



(b) (7)(E)

(b) (7)(E)

Once your password is accepted by the system you will be directed to your own personal "OIG Portal" page. From here you can access the CPE Training Request and Tracking system, as well as other OIG applications.

How do I submit a request for training?

At the OIG Portal front page select the “Click Here to Register for Course” link to begin registration for your course.

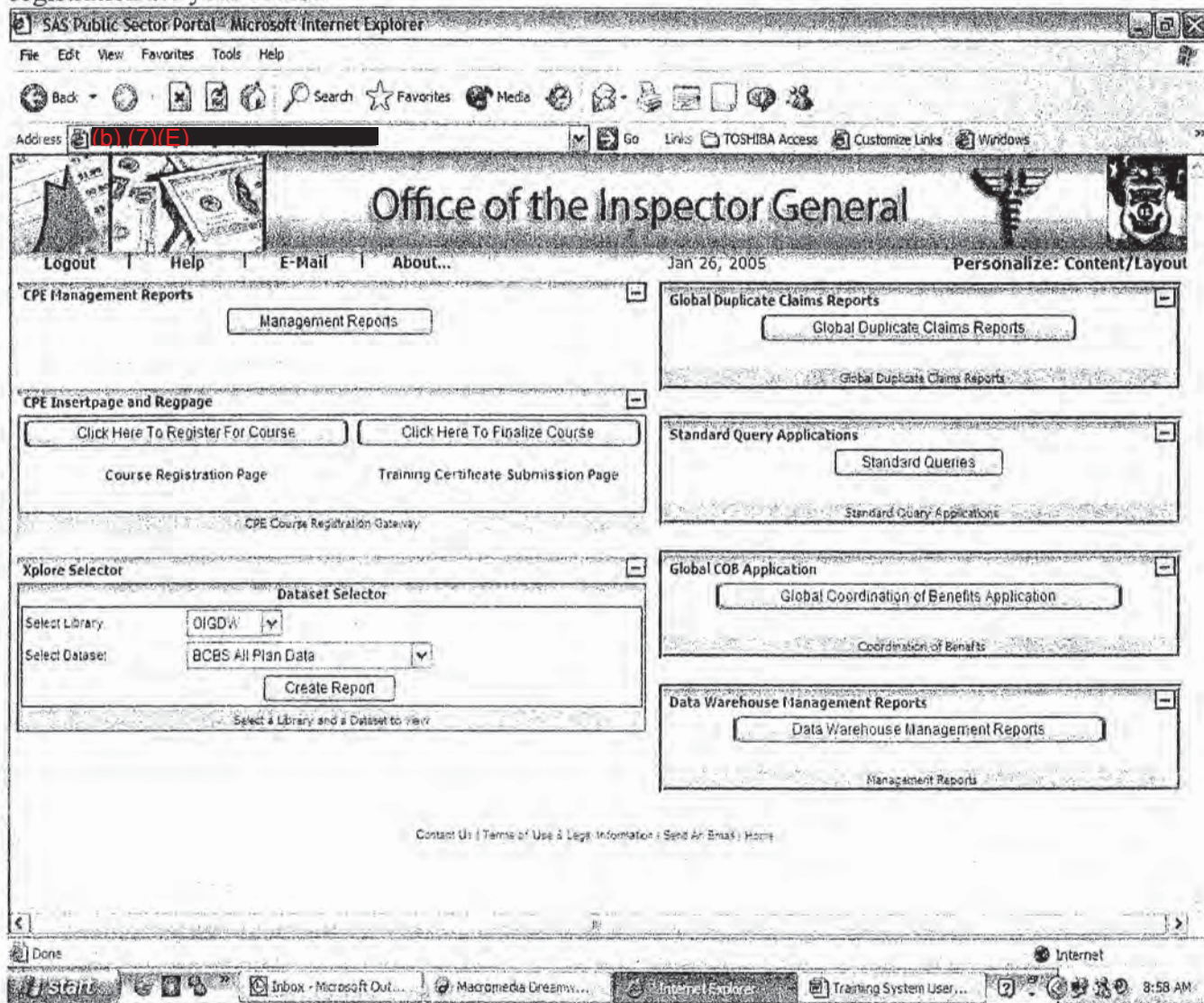


FIGURE 4 OIG Portal Front Page

Your registration entry screen will look like the following:

- Please complete the information below.
- When finished click the Submit Course button at the bottom of the form.

IG Course Registration System

Welcome Kishma N. Brown

** All Fields Are Required **

Employee Information

Entries Will be **Automatically** Generated. If you would like to change user information please check the correct box.

Employee Name:

(b) (6)

Employee Email:

(b) (6)

Division:

ISAD

Telephone:

202-606-0946

Fax:

(202) 606-2153

Home Address:

No Address Provided

[Modify Employee Address](#)

Office Address:

1900 E. St NW Room 6400, Washington DC 20415

Course Information

Training Facility :

Association of Government Accountants

Course Name :

Please Select Course

Beginning date:

1/1/06

Course # :

No Course # Provided

Ending date:

1/1/06

CPE Units:

Course Cost:

Please Click Browse and Submit a Digital Copy of your Registration Form

Registration Form: Browse...

Course Description/Justification: Browse...

[Submit](#)

[Clear Form](#)

[Portal](#)

[Contact US](#)

FIGURE 5 Course Request Screen .

Before you begin your training request, please make sure you have the following information handy: a description of the course, vendor information, time, date, CPE credit and cost. You will have to input this information into the system.

As you have or will find out, most of your basic information is already in the system. However, the home address field is optional. Some staff members prefer to have course materials sent to their home address rather than the office -- an entry here facilitates this preference. PRMO, if requested, can use this information during the registration process.

We have provided a list of frequently used vendors on the drop down list. When you see the training facility that you wish to attend, click on that facility's name. The courses offered by these facilities are already in our database and will automatically populate in the appropriate fields. However, if you do not see your vendor's name please select 'other' from the drop down list, and you will be prompted to input the vendor and course information.

Please enter the course dates, course number (if applicable), CPE units and cost information as indicated in the course description. The actual CPE units earned will be confirmed later in the process (course finalization).

The "Registration Form" is an electronic copy of the form the training vendor needs to register you for the course. Usually the registration form can be found on the vendor's web site. Please fill it out completely and save it to your "H" drive. While the system accepts almost any file format, the easiest is to "cut-and-paste" the form to a MS Word document. To attach the form to the OIG Training System, simply click on the "Browse" button and find your saved registration form for this course. Please note, providing complete information on this form will streamline PRMO's efforts to register you for the course.

The "Course Description/Justification" is an electronic copy of any course information you believe is necessary for your supervisor to ensure that this course is appropriate for your continuing education. Once again, the system accepts almost any file format. However, using MS Word is the most efficient. By following the same instructions as the paragraph above, you can attach your course description/justification to the system.

Once you have entered the required course registration information, click the "submit" button. That's all there is to it! The system will generate an email notifying your supervisor that a training request has been submitted.

How do I determine the status of a training request?

Once you have requested a course, go to the management report tool to view the status of your training request, determine if you have been registered for the course, and ultimately to verify that your training certificate has been accepted by your supervisor and the system.

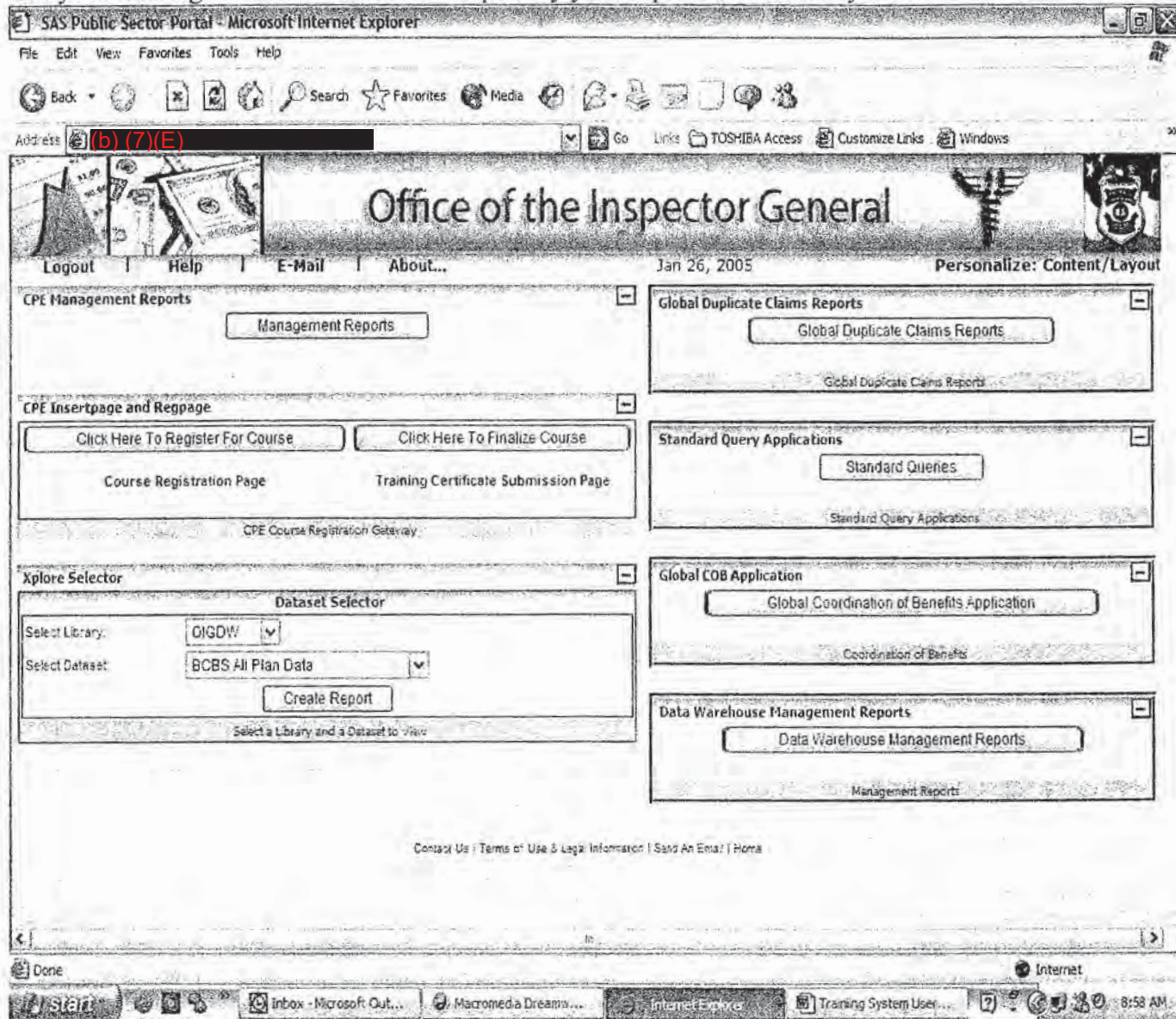


FIGURE 6 OIG Portal Front page

The status of your registration can be viewed from the CPE Reporting Tool Menu. To view the status of your registration, click the Division Link of the corresponding course (e.g. the highlighted link (ISAD) for Basic Information Systems Auditing in the figure below).

CPE Reporting Tool

Employee Name (b) (6) **Report Style** Employee Report **Arrange By** Start Date

If You Would Like To Run a Report Prior to the Current CPE Time Please Enter Year In Box Below Prior to Running Report
 2002

First Name	Last Name	Training Facility	Course Name	Start Date	End Date	CPE Units	Course Cost	DIV
(b) (6)	(b) (6)	IGATI	Basic Information Systems Auditing	1/22/2003	1/24/2003	24	\$550.00	<u>ISAD</u>
(b) (6)	(b) (6)	AGA	IT Auditing with FISCAM & COBIT	5/20/2003	5/22/2003	21	\$800.00	ISAD
(b) (6)	(b) (6)	OPME	2003 Security Awareness Training	9/10/2003	9/10/2003	NC	\$0.00	ISAD
(b) (6)	(b) (6)	IGATI	Essentials of Report Writing	9/24/2003	9/26/2003	NC	\$550.00	ISAD
(b) (6)	(b) (6)	OTHER	SDLC Methodology	12/15/2003	12/15/2003	NC	\$0.00	ISAD
(b) (6)	(b) (6)	USDA	Government Auditing Standards (NEW YELLOW BOOK)	12/16/2003	12/16/2003	NC	\$150.00	ISAD
(b) (6)	(b) (6)	AGA	Time Management	4/16/2004	4/16/2004	NC	\$445.00	ISAD
(b) (6)	(b) (6)	OPME	Security Awareness Training	6/28/2004	6/28/2004	NC	\$0.00	ISAD
(b) (6)	(b) (6)	AGA	Success Over Stress	12/20/2004	12/20/2004	NC	\$0.00	ISAD

NC - Credit hours have not been certified to date.

[Portal](#) [Contact US](#)

Copyright © 2004 OPM Inspector Generals Office

FIGURE 7 CPE Reporting Tool

Another window will open showing the status of your course in the approval process. In this window, each line is labeled with an approval person. If the line is highlighted green the approval person has signed off on the training form and it has been routed to the next approver in line. The red lines are still awaiting approval. (Note: the last two approval lines are for after the course has been taken)

(b) (6)	
Essentials of Report Writing	
Start	
User :	11/23/2004 10:39:47 AM
Div. Chief :	12/2/2004 7:16:19 AM
Deputy Asst. IG For Audits :	12/8/2004 7:37:33 AM
Training Officer :	Awaiting Approval
Registration :	Awaiting Registration
After Course Taken Progress	
User :	Awaiting Certificate Submission
Div. Chief	Awaiting Approval
Finish	
9/24/2003 - 9/26/2003	
Close	
Copyright © 2004 OPM Inspector Generals Office	

FIGURE 8 Approval Status Screen.

You will receive a computer generated email once your first line supervisor has approved your training request (usually, this will be your Senior Team Leader or Division Chief). You will also receive an email message once PRMO has registered you for the course.

Division Chief's Approval Letter

Hello,

This is an Automated Email letting you know that (b) (6) has accepted (b) (6)'s Course Submission for **Basic Information Systems Auditing**

This Message was sent on 12/9/2004 9:02:35 AM

/*****Comments*****/

/*****End Comments*****/

This is an Automated Email, please do not respond

If you would like to go directly to the OIG Portal Please Click Link Below

[OIG Portal](#)

Thank You,

CPE Management Team

Note: This is a screen Print of an email

FIGURE 9 Division Chief Approval letter

Training Request Vendor Registration Accepted

Hello,

This is an Automated Email letting you know that (b) (6) has accepted (b) (6)'s Course Request for **Basic Information Systems Auditing**. The course is now registered with the vendor for the appropriate time and date !

This Message was sent on 12/2/2004 11:01:11 AM

/*****Comments*****/

/*****End Comments*****/

This is an Automated Email, please do not respond

If you would like to go directly to the OIG Portal Please Click Link Below

[OIG Portal](#)

Thank You,

CPE Management Team,

Note: This is a screen Print of an email

FIGURE 10 Training Request Vendor Registration letter.

What do I do after I have completed the course?

Hooray! You have finally completed your training course. Now it is time for you to submit proof of your training.

Submission of training certificate

Upon completion of your training class you will receive a training certificate. Scan a copy of your training certificate and save it either on a hard drive or disk. Log into the OIG web portal and select the "Click Here to Finalize Course" link.

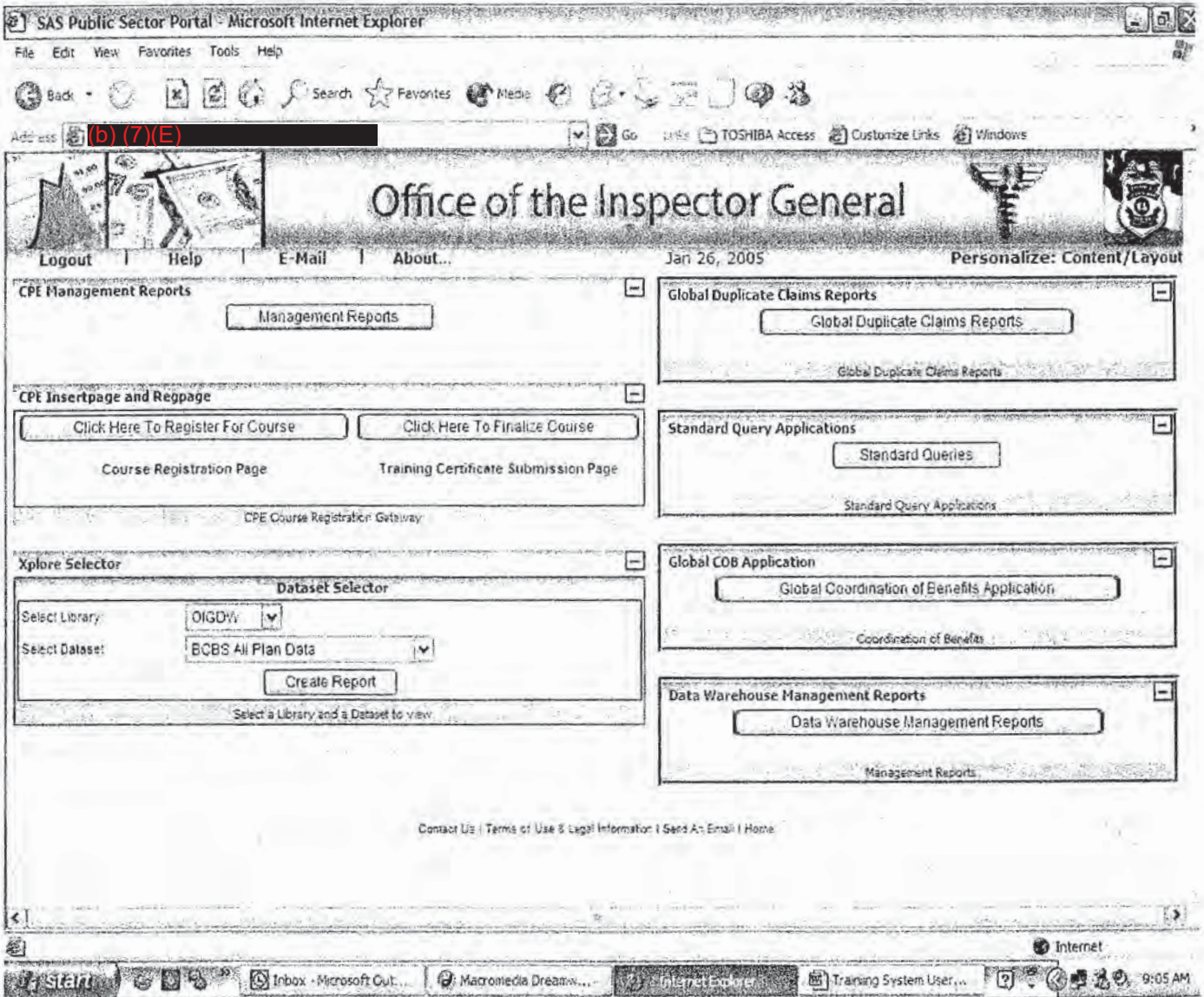


FIGURE 11 OIG Portal Front page

The following screen will appear:

- Please complete the information below.
- When finished click the Submit Course button at the bottom of the form.

IG Certification Submission

Welcome Kishma N. Brown

** All Fields Are Required **

Course Information

Entries Will **Automatically** Generate. If you would like to change user information please check the correct box.

Please Select From a List of Previously Registered Courses

(b) (6)	[2003 Security Awareness Training (9/10/2003)]
	[Government Auditing Standards (NEW YELLOW BOOK) (12/16/2003)]

Retrieve Course Data

Training Facility :

OPM General – Ethics/IT Security

Course Name :

2003 Security Awareness Training

Employee Name:

(b) (6)

CPE Units:

1

Course Cost:

0

Division:

ISAD

Beginning date:

9/10/2003

Ending date:

9/10/2003

Please Click Browse and Submit a Digital Copy of your Certificate

File: Browse...

Class Description

(Describe Your Experience in 250 characters or less)

Submit

Clear Form

[Portal](#)

[Contact US](#)

FIGURE 12 Course Certification Screen.

On this screen you will be prompted to select from a list of registered courses that have received final approval. Highlight the course for which you wish to submit your training certificate, click on the 'Retrieve Course Data' button, and the information will be automatically populated by the computer.

Towards the bottom of the page, there is a browse button. Select the browse button to upload the saved image of your certificate. There is also a section in which you can provide any comments related to the course. (Note: Your description of the experience must be 250 characters or less.) When you are finished select the submit button. Your training class is now linked to the certificate of completion. This verifies that you have attended training.

An email is now generated and sent to your division chief to validate your completion of training.

You can return to the CPE Reporting Tool and click on the Division Link of the corresponding course to view its status.

CPE Reporting Tool

Employee Name (b) (6)	Report Style Employee Report	Arrange By Start Date
---------------------------------	--	---------------------------------

If You Would Like To Run a Report Prior to the Current CPE Time Please Enter Year In Box Below Prior to Running Report

2002

First Name	Last Name	Training Facility	Course Name	Start Date	End Date	CPE Units	Course Cost	DIV
(b) (6)		IGATI	Basic Information Systems Auditing	1/22/2003	1/24/2003	24	\$550.00	ISAD
		AGA	IT Auditing with FISCAM & COBIT	5/20/2003	5/22/2003	21	\$800.00	ISAD
		OPME	2003 Security Awareness Training	9/16/2003	9/16/2003	NC	\$0.00	ISAD
		IGATI	Essentials of Report Writing	9/24/2003	9/26/2003	NC	\$550.00	ISAD
		OTHER	SDLC Methodology	12/15/2003	12/15/2003	NC	\$0.00	ISAD
		USDA	Government Auditing Standards (NEW YELLOW BOOK)	12/16/2003	12/16/2003	NC	\$150.00	ISAD
		AGA	Time Management	4/16/2004	4/16/2004	NC	\$445.00	ISAD
		OPME	Security Awareness Training	6/28/2004	6/28/2004	NC	\$0.00	ISAD
		AGA	Success Over Stress	12/20/2004	12/20/2004	NC	\$0.00	ISAD

NC - Credit hours have not been certified to date.

[Portal](#) [Contact US](#)

Copyright © 2004 OPM Inspector Generals Office

FIGURE 13 CPE Reporting Tool.

A new web page will open with the current course completion status. The first five status bars are for the request and approval of a course (i.e. employee's request for registration, approval process from management, Deputy AIG, training officer and registration officer.) The last two status bars are verification of the course completion (i.e. employee scanning in training certificate and manager approving scanned certificate.)

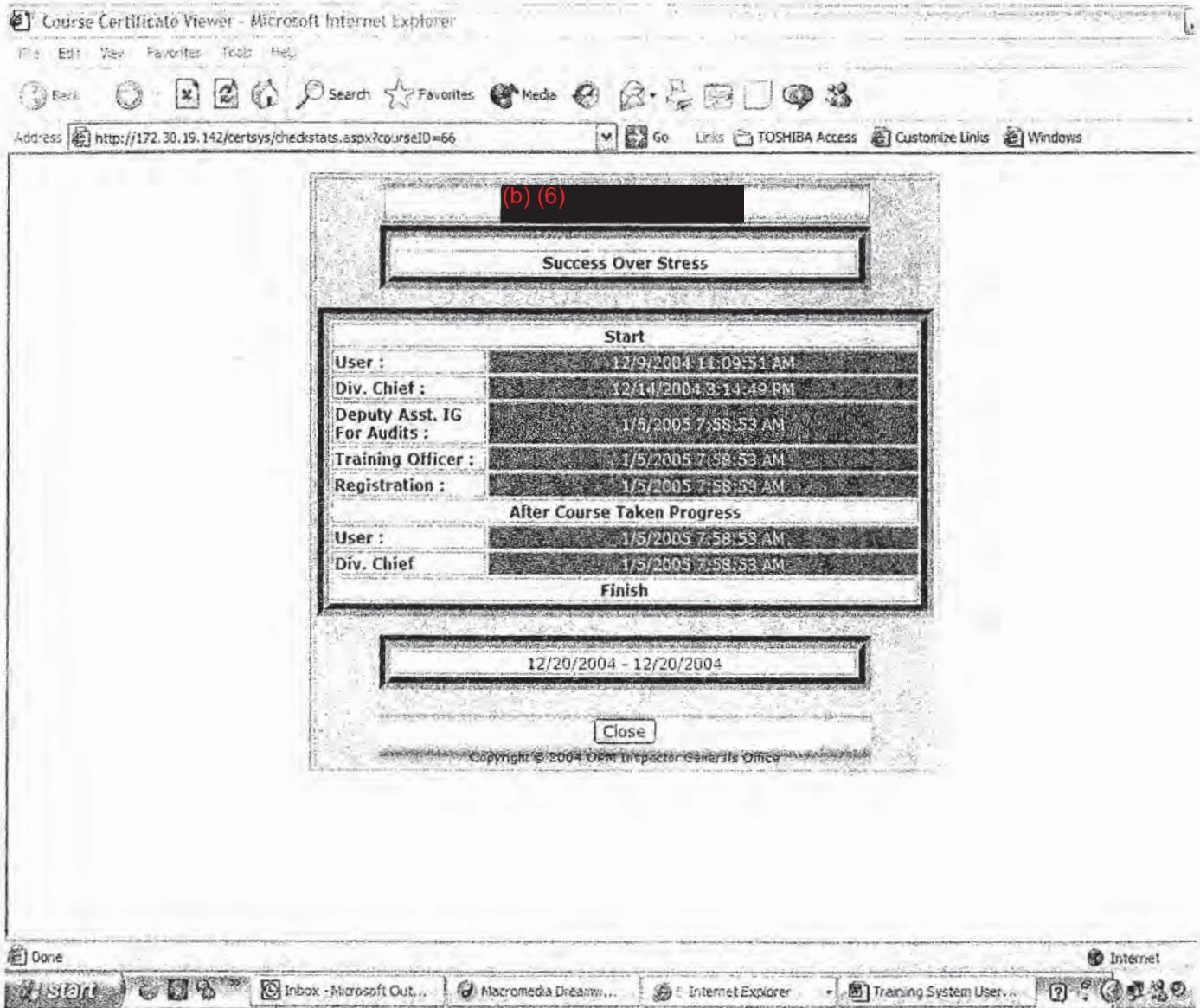


FIGURE 14 Training Status Report

Verification of certificate upload

To verify that your training certificate is associated with your course, return to the CPE Reporting Tool menu. On the CPE Reporting Tool menu all of the course names are highlighted blue; this means that they are active links. When you click on the course link, another screen will open showing the certificate that was submitted for the course.

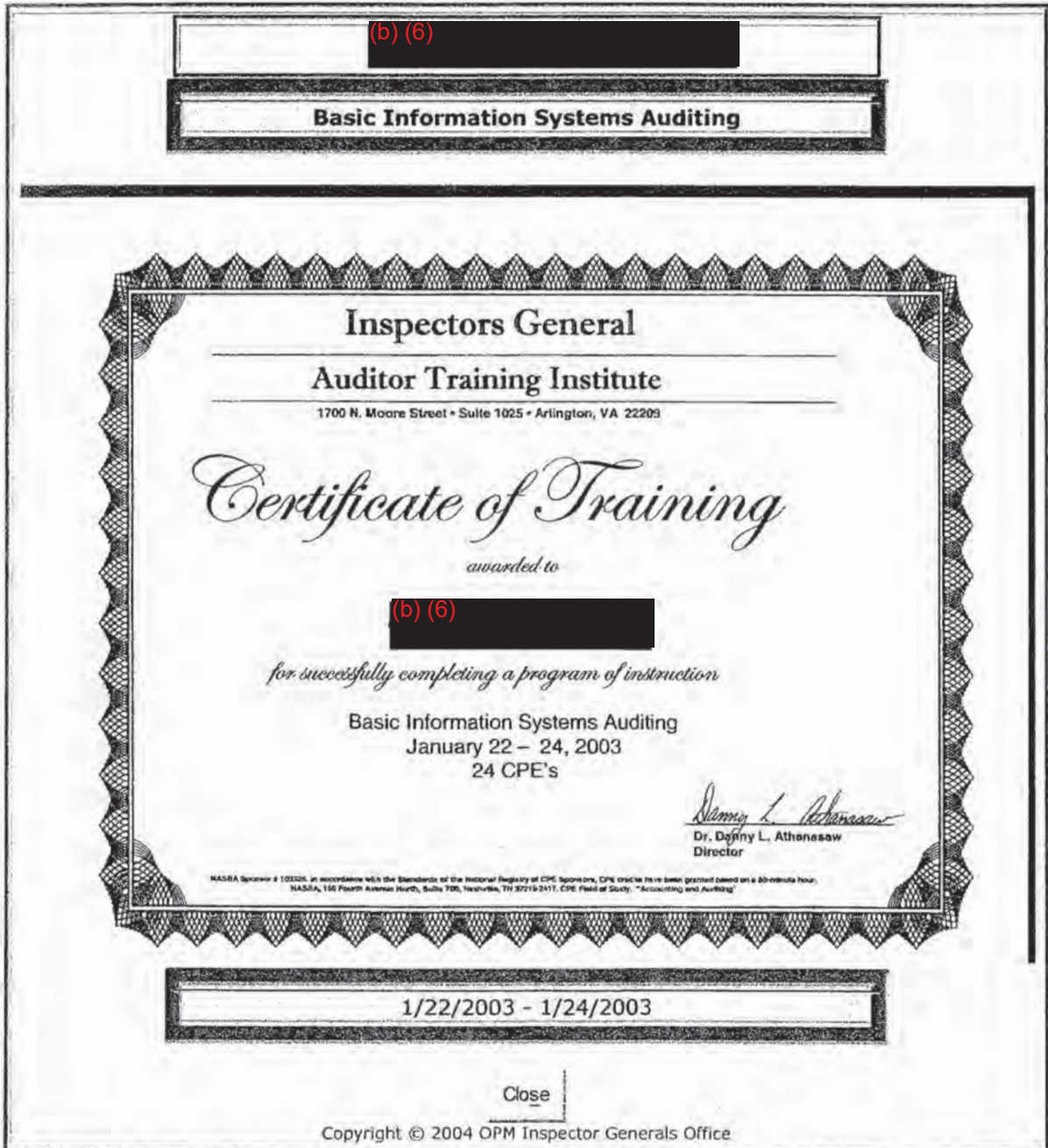


FIGURE 15 Training Certificate in the system.

If you have not submitted a certificate of completion, your screen will have the following message: "No Picture Submitted At This Time" and you will see the following screen.



FIGURE 16 CPE Training Certificate has not been submitted.

How do I know how many CPE hours I have and which courses I have taken?

The OIG Training Request and CPE Tracking system offers many options for reporting the training courses and CPEs requested and completed. From the OIG portal front page select the "Management Reports" button (see figure 11). Using the drop down menus at the top of the page select the reporting tool that best fits your requirements. The following are two sample reports (Figure 17 and 18).

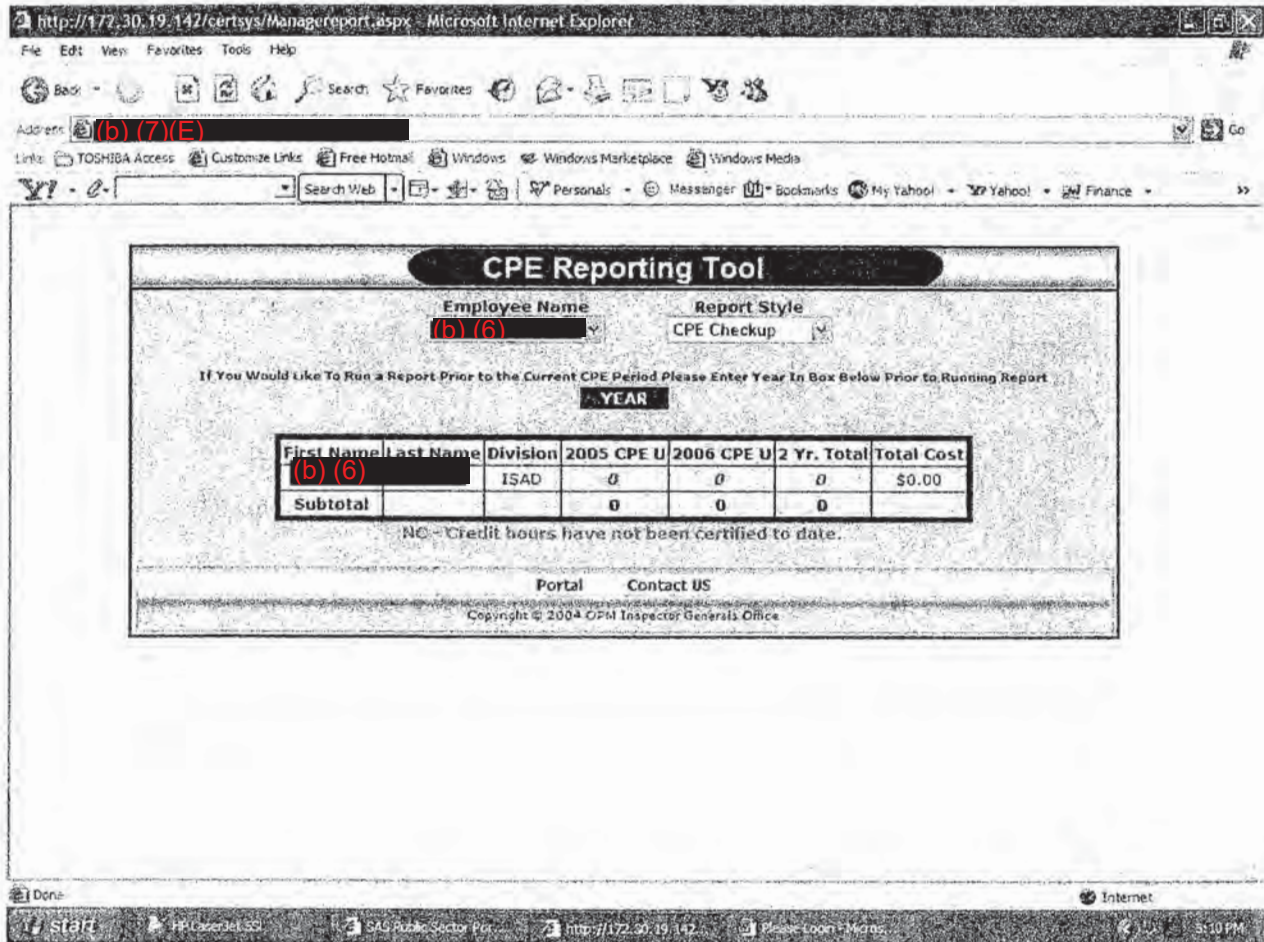


FIGURE 17 CPE Reporting Tool

U.S. OFFICE OF PERSONNEL MANAGEMENT
 OFFICE OF THE INSPECTOR GENERAL
 OFFICE OF AUDITS
 QUALITY ASSURANCE (QA)

AUDIT DOCUMENTATION REVIEW CHECKLIST FOR THE OVERSIGHT OF CONSOLIDATED FINANCIAL STATEMENT AUDIT WORK

REVIEW OF:
 REPORT NUMBER:
 REVIEWED BY:

TYPE OF REVIEW:
 GROUP CHIEF:
 DATE:

		Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL/ DATE	QA APPROVAL (DATE/ INITIAL)
<p>THE QUALITY ASSURANCE GROUP PERFORMS A REVIEW IN ACCORDANCE WITH THE PCIE GUIDELINES RELATED TO THE MONITORING OF THE AUDIT WORK PERFORMED BY THE INDEPENDENT PUBLIC ACCOUNTANTS (IPA) UNDER CONTRACT. IT SHOULD BE NOTED THAT MONITORING OF AUDIT WORK PERFORMED BY IPAS IS NOT AN AUDIT AND THEREFORE IS NOT SUBJECT TO THE REQUIREMENTS OF GOVERNMENT AUDITING STANDARDS.</p>							
<p>1. CONTRACTING PROCESS</p>							
.1	Were the auditors engaged to perform the audit licensed certified public accountants or persons working for a licensed certified public accounting firm?	X					
.2	If the OIG issued a new contract or competitive task order during the review period, did the process address the following items:	X					
	a. Qualifications and experience of the IPA?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

b. Qualifications and experience of the proposed staff?	X					
c. Technical approach?	X					
d. Independence of the IPA, to consider any existing, ongoing, or planned nonaudit services?	X					
e. Description of the IPA's system of quality control?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
	f. The IPA's latest peer review report or reports? (As discussed in GAS, 3.106, IPAs seeking to enter into a contract to perform GAGAS audits should provide the party contracting for such services with their most recent peer review report and any subsequent peer review reports received during the period of the contract.) For peer review reports older than 1 year, OIGs may also consider obtaining additional information about the IPA's system of quality control; for example, the IPA's annual summary of the results of its monitoring procedures required by GAS, 3.95.	X				
	g. References from other clients (i.e., other Federal audit organizations)?	X				
	h. Audit scope and objectives?	X				

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

i. Requirement to perform the audit in accordance with Government Auditing Standards and other statutory, regulatory, or OMB requirements?	X					
j. Establishment of milestones for completion of the audit (or major portions) and the submission of deliverables?	X					
k. Provisions for the review of deliverables and access to the audit documentation by the OIG?	X					
l. Other reports as appropriate, such as a report by a cognizant OIG of quality assurance review for the Single Audit Act purposes?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

2. Planning and Monitoring the Work of the IPA

.1	Determine the degree of responsibility the OIG accepted with respect to using the work of the IPA. This determination can be made by, for example, reviewing the OIG's contract planning documentation, the contract statement of work, the final audit report and transmittal, etc.		X				
.2	Based on the degree of responsibility accepted, did the OIG develop a reasonable strategy and plan, either as part of its policies and procedures or as a separate document, for monitoring and accepting the IPA's work?	X					

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
.3	X					

Did the OIG carry out the strategy and plan in a reasonable manner? Some possible steps the OIG may perform include:

- Participating in the audit entrance and exit conferences and periodic status meetings.
- Reviewing the IPA’s audit planning documents for consistency with the contract and GAGAS, and resolving any inconsistencies.
- Reviewing contract deliverables for consistency with the contract requirements and GAGAS in a timely manner.
- Reviewing the IPA’s audit documentation and reports for adherence to GAGAS.
- Monitoring adherence to milestones as needed.
- Monitoring significant audit and accounting issues.
- Performing supplemental audit tests, if warranted by the degree of responsibility the OIG accepted as identified in 2.1.

	Y E S	N O	QA REVIEW COMMENTS	GROUP REPLY	INITIAL DATE	QA APPROVAL (DATE/ INITIAL
--	-------------	--------	--------------------	-------------	-----------------	-------------------------------------

3. Concluding on the Adequacy of the IPA Monitoring						
.1	Based on the intended use and audience of the IPA's work, the degree of responsibility accepted by the OIG with respect to that work, and the monitoring performed, did the OIG perform adequate procedures to ensure that the work of the IPA adhered to GAGAS?	X				

Draft and Final Audit Report Review and Distribution Work Flow

Document Control:

Create a final audit report review folder on (b) (7)(E)

QAG Final Audit Review Folder (b) (7)(E) :

Each Group will have a folder under QAGFARF

Example: (b) (7)(E) - Access to the group drives should be limited to group members only, QAG staff, AIGA, DAIGA

For each final audit a folder should be created (by the group chief) using the audit report number as the folder name

Example: (b) (7)(E) – All versions of this final report will be stored in this folder once it has been submitted to QAG for review.

Copy and paste the report sub-folder structure from \QAGFARF\Report Folder Structure –Template

Process for Submitting Draft Audit Report for Review:

1. The Group Chief places a signed and dated PDF version of the draft report and transmittal memo into the folder (b) (7)(E), Transmittal Versions to Issue
2. The Group Chief notifies Front Office that a draft report is ready to be issued, and provides the file location
3. The Front Office electronically distributes the two signed PDF files from the “Draft Report, Transmittal Versions to Issue” folder. If hard copies must be prepared and distributed, this is done also.

Process for Submitting Final Audit Report for Review:

Group

4. Prepare Final audit report in **one** Word document. Eliminate all Excel schedules and scanned copies of auditee responses.
5. The Group Chief should put the audit report, transmittal memo, Independent Reference check list, and Blue sheet in their respective folder for QAG review.
6. An email should be sent to QAG stating that the final audit report is ready for review and is located in (b) (7)(E). The Group Chief should create a PDF file (print to PDF) of this version of the report and save it in the same folder.

QAG

7. QAG conducts its review in track changes. In addition to the word file containing QAG's comments, QAG should create PDF files of the report and transmittal memo with review comments and save those files to the same folder.
8. Once QAG completes its review, an email should be sent to the AIGA stating that the final audit report "name" and transmittal memo is ready for review and is located in (b) (7)(E) claim review process.

AIGA

9. The AIGA should conduct his review in track changes in the same file the QAG completed its review. Once the review is complete the AIGA should also create PDF files of the report and transmittal memo with review comments and save to the same folder.
10. The AIGA will then email the Group Chief stating that the reviewed copy of final audit report "name" and transmittal memo is located in (b) (7)(E).

Group

11. Once the Group Chief has cleared all notes and comments, the Group Chief should create another PDF of these files and save in the same folder.
12. An email should be sent to QAG stating that all notes and comments have been addressed for final report "name" and that it is located in (b) (7)(E).

QAG

13. QAG reviews the control folder and final report for completeness. Once review is complete QAG sends the AIGA an email stating that all comments have been cleared for final audit report "name" and is ready for signature, and delivers control folder with the hard copy report to the AIGA. The file is located in (b) (7)(E).

AIGA

14. The AIGA completes his review of the audit report electronically. If the AIGA has additional comments or corrections, return to Step 7. If the AIGA is satisfied with the report, he sends an email to the Group Chief stating that the report is complete and ready for DIG and IG review.

DIG/IG Review and Issuing Report

15. The Group Chief creates a sub-folder within this report folder labeled "Final Report, Transmittal Versions to Issue"
16. The Group Chief prints the Word/master copy of the report and transmittal memo, places them in a blue review folder with the Clearance and Review Sheet as a cover, and delivers the folder to AIGA. Note – add the due date of issuance of the report to meet the timeliness standards on the Clearance and Review Sheet. **The Group Chief also ensures that workpapers, checklists, coaching notes, etc. in the Teammate project have been signed off. At this point, no further edits**

should be made to the workpapers and only a signed copy of the final report should be added to project upon its issuance.

17. The AIGA gives the hard copy report to the DIG/IG for review and signature. After the IG signs transmittal, folder is returned to the AIGA.
18. The AIGA provides folder to front office, and the Front Office scans the transmittal memo with the IG's signature into a PDF file and places in the "Final Report, Transmittal Versions to Issue" folder, and notifies the AIGA.
19. The AIGA converts the Word copy of the final report to PDF and saves the PDF file to the "Final Report, Transmittal Versions to Issue" folder.
20. The Front Office combines the transmittal memo and final report PDFs into one PDF, and lets the AIGA know the report is ready to sign.
21. The AIGA electronically signs the report, dates the title page and Executive Summary, and notifies the Front Office that it is ready to issue.
22. The Front Office electronically distributes the two signed PDF files from the "Final Report, Transmittal Versions to Issue" folder. If hard copies must be prepared and distributed, this is done also. Copies of the completed final audit report will be distributed according to the transmittal memo of the final report and certain OIG personnel. The Group Chief can add the signed final report to the Teammate Project and must finalize the Teammate Project to ensure that no edits are made to the project and no workpapers are added.¹

¹ For the annual Oversight of OPM's Consolidated Financial Statement Audit, the Teammate project should be finalized within the Independent Public Accountant's contracted period of performance of the audit.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2210

Audit Planning

CHAPTER 2210 - AUDIT PLANNINGCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. AUDIT PLANNING	
2-1. General.....	2
2-2. Notifying the Audited Entity.....	3
2-3. Preparing the Survey.....	4
2-4. Preparing the Audit Planning Document.....	5
2-5. Other Planning Activities.....	5
2-6. Preparing the Audit Program.....	6
2-7. Relying on the Work of Others.....	9
2-8. Assessing Compliance.....	11
2-9. Assessing Internal Controls.....	12
2-10. Evaluating Computer Processed Data.....	15
2-11. Assessing Risk.....	17
2-12. Assessing Fraud.....	19
Exhibits	
A. Audit Staff Declaration of Personal and Financial Independence	
B. Time Phased Audit Plan	
C. Fraud Assessment Questionnaire for Healthcare Audits	
D. Fraud Assessment Questionnaire for Non-Healthcare Audits	
E. Example of an Audit Planning Document/Memorandum	
F. Annual Filing of Confidential Financial Disclosure Report (SF 450)	
G. Required Notice of Outside Employment	

CHAPTER 2210 - AUDIT PLANNINGSECTION 1. GENERAL

- 1-1. PURPOSE. Audit planning consists of thoroughly designing an audit, including notifying the audited entity, preparing an audit planning document, preparing a survey, developing an audit program, relying on the work of others, assessing compliance and internal controls, and evaluating computer processed data. Audit planning includes defining the audit objectives and planning how they can be achieved while establishing a balance between the audit scope, time frames, and total audit hours to be spent to ensure optimum use of audit resources. Audit planning is important to ensure that results will satisfy the objectives of the audit. This chapter establishes OIG Office of Audits procedures for audit planning. For additional information, see Chapter 2215 (Managing Audit Field Work).
- 1-2. POLICY. The OIG Office of Audits will plan audits in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States and OIG policies and procedures.

SECTION 2. AUDIT PLANNING

- 2-1. GENERAL. Proper audit planning helps to ensure that audit objectives are met on time; adherence to professional standards in conducting audit field work; and clear, concise, convincing reporting of audit results. Also, planning helps to ensure proper staff development through the matching of auditor skills to specific audit objectives.
- a. Auditors must adequately plan and document the planning of the work necessary to address the audit objectives. Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and conclusions. This determination is a matter of professional judgment. In planning the audit, auditors should assess the significance of previous findings and audit risk and apply these assessments in defining the audit objectives and the scope and methodology to address those objectives. Planning is a continuous process throughout the audit. Therefore, auditors may need to adjust the audit objectives, scope, and methodology as work is being completed. Also, the auditors should communicate the status of the planning and performance of the audit to management officials, those charged with governance, and other audit stakeholders.
 - b. The Auditor-in-Charge (AIC)/Team Leader will develop the audit plan. The audit plan is the overall strategy for conducting the audit assignment and covers the remaining three phases of the audit: survey, field work, and reporting. For additional information, see Chapter 2215 (Managing Audit Field Work).
 - c. Audit planning will consider the following factors: audit objectives; audit risk and materiality; the audited entity's size; OIG experience with the audited entity; prior audits and follow-up; complexity; adherence to professional standards; and reporting requirements.
 - d. The planning process may include notifying the audited entity; preparing the audit planning document; other planning activities; preparing the survey and audit program; considering the work of others; assessing compliance and internal controls; and, evaluating computer processed data.
 - e. For attestation engagements auditors are required to establish an understanding with the audited entity (client) regarding the services to be performed. Such an understanding reduces the risk that either the auditors (practitioner) or the audited entity may misinterpret the needs or expectations of the other party. The understanding includes the objectives of the engagement, responsibilities of entity management, responsibilities of auditors, and limitations of the engagement.

- 2-2. NOTIFYING THE AUDITED ENTITY. The audit notification letter will identify the audit authority (The Inspector General Act of 1978, as amended, has established audit authority for the Office of Personnel Management’s Office of the Inspector General to conduct audits); audit objectives, scope, and methodology; starting date and location of the audit; length of the audit; number of audit staff and key OIG Office of Audits contact personnel, including applicable titles and telephone numbers.
- a. The audit notification letter may request the name, title, and telephone number of the audit coordinator or those charged with governance at each audit site; documents and data, including, where applicable, completion of an audit questionnaire prior to the on-site starting date; suitable office space and equipment; and an entrance conference.
 - b. All notifications shall be signed by the Group Chief or designee. Time frames for issuing the audit notification letter differ for internal and external audits.
 - (1) For internal and Combined Federal Campaign (CFC) audits, the letter should be sent at least 30 days in advance of the audit starting date. For contract proposal audits, 15 days notice in advance of the audit is adequate unless procurement needs require shorter notice.
 - (2) For external audits, this letter should be sent 60 days in advance of the audit starting date.
 - c. The original audit notification memorandum or letter will identify the following distribution information.
 - (1) When addressed to an OPM official, the original and all copies of the audit notification letter or memorandum will contain the following annotation (following the last paragraph or the attachment line, if applicable): cc: (appropriate official(s) listed in section 2-2 d. of this chapter).
 - (2) When addressed to a contractor or CFC official, the official file copy or clearance sheet of the letter should show cc: (appropriate official(s) listed in section 2-2 d. of this chapter). The file copy or clearance sheet must identify the author, file name, and individuals who cleared the letter. The “Subject File” and the “Cross-Referenced File” at the bottom of the OIG Report Clearance and Review sheet will be completed by the auditor. The auditor will type or write the codes found in the “OIG Central Filing Index”. The auditor will type or write the codes that pertain to the work performed. The codes can be found on the (b) (7)(E) [REDACTED].

- (3) When the local CFC's are notified of the audits, general notification is made to the appropriate Federal Executive Board (FEB).
 - d. Distribution of the audit notification letter will be as follows: (1) original to the audited entity; (2) copies to the appropriate program agency official for external audits (a listing of all of the upcoming CFC audits is sent instead of letters); (3) Chief Financial Officer (except external audits); (4) OIG Office of Audits correspondence file; (5) Secretary, Office of Audits; (6) the official file copy goes into the audit documentation; and (7) officials identified on the clearance sheet.
- 2-3. PREPARING THE SURVEY. During this period, the auditors accumulate information on the audited entity's key functions and operations and attain an understanding of the policies and regulations concerning the audit. This information may lead to areas in which there may be uneconomical or inefficient operations, internal control weaknesses, or a lack of compliance with laws and regulations. A survey phase is not necessary for all audits. The AIC/Team Leader will consider whether, or the extent to which, a survey needs to be done following completion of the audit plan but prior to preparing the audit program.
- a. If a survey is applicable, it will include such things as the research of applicable laws and regulations, collection of internal and external source documents, gathering general information concerning the audited entity, and analyzing the results of collected information.
 - b. The auditors should obtain, as appropriate, mission and function statements; brochures; contracts; financial statements; budget documents; internal and external audit reports; organizational charts; and policies and procedures.
 - c. Auditors will identify unresolved audit findings and elements influencing audit risk and materiality.
 - d. Computer processing or other technical assistance requirements will be considered. Auditors should determine (and document scope and completion dates) whether in-house ADP support and/or outside specialists, experts, and consultants can meet these needs and arrange for these services.
 - e. The applicable survey information will serve as the foundation for preparing the audit program.
 - f. Auditors should prepare audit documentation to summarize and support the survey work. These documents will document the information gathered and any conclusions reached during survey. For additional information, see Chapter 2215 (Managing Audit Field Work).

- 2-4. PREPARING THE AUDIT PLANNING DOCUMENT. The AIC/Team Leader will prepare an audit planning document prior to the start of audit field work. The audit planning document may be in the format of either a narrative or a checklist. The document will precede the audit program and reflect the information initially known concerning the audit.
- a. The document will identify information relevant to the upcoming audit, including such things as: the audit title; report number; staffing requirements; audit objective; summary description of the reason for the audit; summary description of audit methodology and scope; required computer equipment and technical assistance; number of staff days estimated; and target dates for completing survey work, any computer or technical analysis, survey and review field work, summarizing audit documents, and the audit report.
 - b. The audit planning document may also serve as a very preliminary audit program. The document will assist the AIC/Team Leader in completing the audit objectives section of the audit program and estimating audit completion times.
 - c. The AIC/Team Leader will cross-reference, sign, and date the audit planning document. The AIC's/Team Leader's supervisor will approve the audit planning document. Approval is documented by signing and dating (month, day, and year) the plan. For automated audit documents, electronic signatures are acceptable for approving the audit planning document instead of scanning in signature pages. However, the Group Chiefs and Senior Team Leaders will decide the appropriate method for their group. The AIC/Team Leader will type their name and date on the audit planning document and initial and date as preparer in Teammate's (TM) signoff and edit history. The Group Chiefs and Senior Team Leaders will type their name and date on the audit planning document and initial and date as reviewer in TM's signoff and edit history. Under the name, the following statement, "See TM signoff and edit history for electronic signature and date" may be added to this document if the group chooses to use this method. The AIC/Team Leader will file the approved copy in the audit documentation.
- 2-5. OTHER PLANNING ACTIVITIES. Other planning activities requiring AIC/Team Leader action at this time include requesting that all staff who prepare, work, or review an audit report or set of work papers (including the Group Chief, Senior Team Leader, Team Leader/AIC, audit staff, and the independent referencer) sign and date the "Audit Staff Declaration of Personal and Financial Independence" form (see Exhibit A on page 19). All supervisory personnel who will be involved in the performance of the audit should also sign and date the form. Also, the AIC/Team Leader should plan where staff may be effectively assigned relative to their level of skill.

2-6. PREPARING THE AUDIT PROGRAM. Audit programs are guides in conducting the audit and will be based upon the audit objectives to be met. Each audit step in the program will be indexed to the appropriate audit documents. The AIC/Team Leader will prepare, sign, and date the audit program prior to the start of audit field work. The auditor must initial and date (month, day, and year) each step in order to document completion.

- a. Preparing the Time-Phased Audit Plan. All audit programs shall include an audit step for the preparation and the completion of a time-phased audit plan. A time-phased audit plan provides the road map for achieving the audit objectives within the time period set for the audit (see Exhibit B on page 20). The time-phased audit plan should be prepared as a separate document from the audit plan.

The AIC/Team Leader, with guidance from his/her immediate supervisor, should include the following major audit segments in the time-phased audit plan: Audit Notification, Pre-Audit, On-site/Fieldwork, and Post-Audit.

- Audit Notification – Should include the estimated and actual completion dates.
- Pre-Audit – Should include the budgeted and actual days, as well as the estimated and actual completion dates.
- On-site/Fieldwork – Should include the budgeted and actual days.
 1. The Entrance and Exit Conference and the End of the Fieldwork should include the estimated and actual completion dates.
- Post-Audit - (The columns are left blank).
 1. The Draft report should include the budgeted and actual days, as well as the estimated and actual completion dates.
 2. The Response Received to the draft report should include the estimated and actual completion dates.
 3. The Final report provided to QAG should include the budgeted and actual days, as well as the estimated and actual completion dates.

The amount of actual staff time spent on each major audit stage will be tracked against the budgeted time. All deviations/variations of greater than 20%, above or below, of the budgeted days or estimated completion dates shall be explained and documented. The time phased audit plan must be referenced to an audit time log or time tracking system. The various audit stages within the time-phased plan (audit notification, entrance conference, exit conference, end of fieldwork, and the draft, draft response and the final report) must be referenced to a work paper in TeamMate (see Exhibit B).

- b. Contents of an Audit Program. Each audit program should contain audit steps for a time-phased audit plan; review of prior audit reports; follow-up on prior

audit recommendations; entrance/exit conferences; transaction selection techniques (e.g., statistical, random, or judgmental); review for compliance (when appropriate); obtaining an understanding of the internal controls (when necessary); detection of irregularities and noncompliance (when necessary); reliability of computer-generated information (except of course when that information is the subject of the audit); and issuing audit reports. In addition, while the following processes must be reflected in the audit documentation, specific audit steps in the audit program are not required. However, as a reminder and at the discretion of the auditor, the audit program may contain steps for summarizing audit documentation sections; independently referencing the draft audit report; and preparing and completing the process for issuing the draft and final audit reports.

Each audit program will contain an introduction, background, audit objectives, scope, methodology, and specific audit steps.

- (1) The introduction should state the type of examination (i.e., audit, review, inspection, evaluation, attestation, compilation, agreed upon procedures, etc.); authority (i.e., Inspector General Act, specific statutory requirement, contract clause, request, etc.) to conduct the examination; and if initial examination of entity.
- (2) The background section may provide information on the audited entity's history and objectives; legal authority for the audited activity; previous audit experience and follow-up on prior audit findings; OPM program or contract; known deficiencies or problems, including the entity's internal control structure; percentage of government business to total business; systems used to develop, allocate, and control cost; types and flow of transactions; locations to be reviewed; and general time frame for the review.
- (3) The audit objectives are what the audit is intended to accomplish. The audit objectives should be clearly identified since they determine the extent of testing and specific audit steps required.
- (4) The scope section should be directly tied to the audit objective(s). The scope section should state the audit type, i.e., financial (statement), attestation engagements, or performance (program effectiveness and results, economy and efficiency, internal control, compliance, or providing prospective analyses, guidance, or summary information); explain the relationship between the population to what was audited; time period covered by audit; identification of the organizations and geographic locations where the audit work will be conducted; dates the field work will be performed at each location; report the kinds and sources of evidence and any problems with the evidence; any known

- limitations placed on the audit by information limitation or scope limitation, including the availability of certain records or individuals; any deviations from auditing standards; and, planned assessment of internal controls.
- (5) The methodology section comprises the work involved in gathering and analyzing data to achieve the objectives. The section should clearly explain how the audit objectives were accomplished. Also, the methodology section should provide a brief summary of the overall evidence gathering and analytical approach to be taken, including (if planned for the audit) the use of sampling or computer assisted techniques or other techniques; description of any measures or criteria used to assess performance or compliance; and any constraints. Also include any techniques used to verify evidence and why unverified information was used, if appropriate. When sampling significantly supports the audit findings, the auditor should include whether the results can be projected to the intended population. If extensive or multiple sources of information are used, the report may include a description of the procedures performed as part of the assessment of the sufficiency and appropriateness of information used as audit evidence.
 - (6) The audit step sections identify those specific tests and procedures which will permit the auditor to achieve the audit objectives. These tests should consider administrative and accounting policies and procedures unique to the audited entity; applicable standards or compliance requirements; and legislative concerns and public interest. Each series of audit steps should be prefaced with the specific audit objectives which those steps are designed to achieve. When designing audit tests, auditors should consider materiality and potential for irregularities and noncompliance.
 - (7) Audit programs should be sufficient to provide reasonable assurance of detecting irregularities and noncompliance (or other instances of noncompliance with laws, regulations, and contracts) that could have a direct and material effect on the financial statements or the results of financial audits. For performance audits, based on a risk assessment of laws, regulations, and other compliance requirements that are significant to audit objectives, the audit program should provide reasonable assurance of detecting significant instances of noncompliance with laws and regulations. For attestation engagements, the audit program should provide reasonable assurance of detecting significant irregularities or other noncompliance that could have a material effect on the subject matter or assertion of the attestation engagement. See Chapter 2325 (Fraud, Illegal Acts, and Abuse).

- (8) Audit programs should include audit steps on assessing the reliability of computer-processed information when conducting audits. These audit steps (a) require the auditor to determine whether computer-processed information will be significant to the audit objectives and (b) if applicable, take appropriate steps if the information is determined to be significant, to ascertain the reliability of the information and its impact on the audit. See this chapter (Audit Planning, Section 2-7, Relying on the Work of Others and Section 2-10, Evaluating Computer-Processed Data) and Chapter 2230 (Auditing Computer-Based Systems, Section 7-2).
 - (9) Audit programs may identify any unique terms or special instructions in a glossary or appendix.
 - (10) For automated documents, the audit program has to identify the location of the audit steps. At the end of the audit program's narrative (includes but not limited to the introduction, background, audit objectives, scope, and methodology) describe or link the location of the audit steps.
 - (11) Audit programs should, when appropriate, include steps to follow-up on prior audit findings and recommendations.
- c. The AIC's/Team Leader's immediate supervisor will review and approve each audit program prior to the start of the field work. Any individual changes will be annotated, initialed and dated within the program. Approval is documented by signing and dating (month, day, and year) each agreed upon audit program. For automated documents, electronic signatures are acceptable for approving the audit program instead of scanning in signature pages. However, the group chiefs and senior team leaders will decide the appropriate method for their group. The AIC/Team Leader will initial and date as preparer in TM's signoff and edit history. The AIC's/Team Leader's immediate supervisor will initial and date as reviewer in TM's signoff and edit history. Under the name, the following statement, "See TM signoff and edit history for electronic signature and date" may be added to this document if the group chooses to use this method. The AIC/Team Leader will file the final audit program in the audit documentation.
 - d. Once approved, the AIC/Team Leader will annotate, initial, and date any deviations (i.e., changes, additions, deletions, etc.) within the audit program due to field work conditions or issues. The AIC/Team Leader will discuss these deviations with his/her immediate supervisor and document these discussions.
- 2-7. RELYING ON THE WORK OF OTHERS. Using the work of others (auditors and non-auditors) results in the effective and efficient use of audit resources in meeting audit objectives. Normally, this work is identified during the initial audit planning and

survey phases of the audit. The extent to which OIG may rely upon the work of others depends on the adequacy and extent of the work performed by others. By considering the following guidelines, AICs/Team Leaders should be able to determine the extent of reliance on this work.

- a. During audit planning and survey, AICs/Team Leaders will identify applicable audits, reviews, and inspections and determine the extent to which this work can be used. Sources include OPM; other federal, state, and local government agencies; audit entity internal or independent auditors; and outside specialists, experts, and consultants.
- b. AICs/Team Leaders should coordinate with all responsible individuals, including participating field staff at different locations.
- c. When evaluating the adequacy of the work of others, OIG auditors must exercise sound professional judgment. Competency, independence, and objectivity are considerations. GAGAS provides the following guidelines:
 - (1) External auditors must be competent, independent, and if certified public accountants (CPA), in good standing under the requirements of the American Institute of Certified Public Accountants (AICPA) and/or state society.
 - (2) Internal auditors must be competent and objective. Competency may be determined through inquiry of the internal auditor qualifications and professional experience including professional certification, continuing education, and supervisory reviews of internal auditors' activities. Objectivity may be determined by evaluating the role of the internal auditor within the organizational structure and its policies.
 - (3) For non-auditor experts (specialists, experts, consultants, etc.), the auditors should consider the professional certification, license, or other recognition, including the views of peers regarding the competency of the specialist.
- d. When relying on the work of others, OIG should obtain and evaluate the work products, including audit documentation. Auditors should consider and evaluate the audit steps which were performed compared to those which they believe were necessary. OIG will prepare audit documents to document their evaluation process. To assess competency and usefulness of work performed, auditors should consider the following guidelines.
 - (1) For external audits, OIG auditors should consider conducting additional tests and procedures; reviewing and modifying audit programs; and/or evaluating audit documentation including the assessment of internal

controls, tests of compliance, and conclusions reached. In addition, the auditors should request the most recent external assessment review from the external audit organization.

- (2) For internal audits, OIG auditors should examine, on a test basis, documentary evidence of the work performed and consider appropriateness of the scope; adequacy of the audit programs and documentation; appropriateness of conclusions reached; and consistency of internal audit reports issued to the work performed. On a test basis, OIG auditors should sample and conduct tests of some of the transactions or balances reviewed by the internal auditors. OIG results should be compared to the results of the internal auditors' work in reaching conclusions. The extent of the tests will depend on the type and materiality of transactions and the results of any reviews.
 - (3) For non-auditors, OIG auditors should consider reviewing the procedures followed and the results of the work conducted; reviewing and evaluating the adequacy of the work program, assumptions used, and audit documentation; and conducting supplemental tests of the work performed. When using the work of a specialist, auditors should assess the independence of specialists who perform audit work. This includes identifying threats and applying any necessary safeguards in the same manner as they would for auditors performing work on those audits. If the specialist has impairment to independence, auditors should not use the specialist's work.
- e. When assessing the reliability of computer-processed data generated or provided by Plan officials or the audited entity, auditors have to ensure that information system controls are valid and reliable when the data is significant to the audit findings. This work is necessary regardless of whether the data is provided to auditors or auditors independently extract it. If the results of such work are current, auditors may be able to rely on that work. See this chapter (Section 2-10, Evaluating Computer-Processed Data) and Chapter 2230 (Auditing Computer-Based Systems, Sections 2, 3, 4 and 7).
 - f. The scope section of the audit report must state the reliance placed upon the work of others. See Chapter 2400 (Audit Report Preparation and Standards).
- 2-8. ASSESSING COMPLIANCE. Auditors are responsible for identifying and understanding laws, regulations, and other compliance requirements (i.e., provisions of contracts or grant agreements) and designing audit steps and procedures that will provide reasonable assurance that the audited entity has adhered to the requirements of the laws and regulations applicable to the audit. Audit planning assists the auditors in assessing the audited entity's compliance with applicable requirements of the laws, regulations, and other compliance requirements.

- a. To assess compliance with applicable laws, regulations, and other compliance requirements, audit plans must include explicit audit steps which assess compliance with regulatory requirements and detect errors, fraud, irregularities, major areas of noncompliance, and abuse. These tests must be designed to provide reasonable assurance, not absolute or complete, that material instances of noncompliance are detected and reported.
 - (1) To determine compliance, auditors must identify the pertinent laws, regulations, and other compliance requirements. Audit tests must measure compliance with these laws. Auditors will assess the risk that noncompliance will significantly affect program operations or financial statements and evaluate the effectiveness of related internal controls. Auditors should develop audit steps to identify noncompliance and exercise appropriate caution in investigating and reporting noncompliance so as not to interfere with potential future investigations and/or legal proceedings.
 - (2) The auditors should consult with the Office of Legal Affairs when interpreting laws, regulations, and other compliance requirements if necessary, and making decisions that are essentially legal (e.g., determining if certain actions by the agency or others violated laws and regulations). See Chapter 2915 (Requesting Legal Opinions and Interpretations).

2-9. ASSESSING INTERNAL CONTROLS. Good internal controls are essential to achieving the proper conduct of government business with full accountability for the resources made available. Audit planning and survey work must provide the auditor with an understanding of the audited entity's internal controls. See Chapter 2315 (Review of Internal Controls).

- a. For financial audits, a sufficient understanding of the internal control structure is to be obtained to plan the audit and to determine the nature, timing, and extent of audit tests to be performed. Auditors should perform procedures directed toward assessing the level of control risk. In conjunction with assessing the level of control risk, auditors will test the effectiveness of the plan or operation of the internal control structure's policy or procedures. The auditors will use the results derived from the assessment of control risk and tests of controls to plan the level of substantive testing required to meet the internal control review objectives. Also when auditors are planning and designing the audit procedures to be performed, AICPA standards and GAGAS require the auditors to assess the risk of material misstatements of financial statement amounts or other financial data significant to the audit objectives due to fraud. Auditors should refer to the guidance contained in the AICPA standard, entitled Consideration of Internal Control in a Financial Statement Audit.

- b. For attestation engagements, auditors should obtain a sufficient understanding of internal control that is material to the subject matter or assertion to plan the engagement and design procedures to achieve the objectives of the attestation engagement. In planning the examination-level attestation engagement, auditors should obtain an understanding of internal control as it relates to the subject matter or assertion to which the auditors are attesting. The subject matter or assertion may be of a financial or non financial nature, and internal controls material to the subject matter or assertion the auditor is testing may relate to:
- (1) effectiveness and efficiency of operations, including the use of an entity's resources;
 - (2) reliability of financial reporting, including reports on budget execution and other reports for internal and external use;
 - (3) compliance with applicable laws and regulations, provisions of contract, or grant agreements; and
 - (4) safeguarding of assets.
- c. For performance audits, internal controls include the plan of organization and methods and procedures adopted by management to ensure that its goals and objectives are being met; controls include the processes for planning, organizing, directing, and controlling program operations; controls include the systems for measuring, reporting, and monitoring program performance; controls serve as the first line of defense in safeguarding assets and preventing and detecting errors, fraud, and violations of laws, regulations, and provisions of contracts and grant agreements; resources used are consistent with laws, regulations, and policies; resources are safeguarded against waste, loss, and misuse; and reliable data are obtained, maintained, and fairly disclosed in reports. The need to assess internal controls and the focus of that assessment varies with the objectives of the audit.
- (1) For program effectiveness and results audits, auditors may assess those policies, procedures, practices, and controls which specifically bear on the attainment of the goals and objectives specified by the law or regulation for the organization, program, activity, or function under audit to the extent necessary, as determined by the audit objectives.
 - (2) For economy and efficiency audits, auditors may assess those policies, procedures, practices, and controls applicable to the programs, functions, and activities under audit to the extent necessary, as determined by the audit objectives.

- (3) For internal control audits, auditors may assess those policies, procedures, practices, and controls relating to management's plans, methods, and procedures used to meet its mission, goals, and objectives, as determined by the audit objectives. Internal control includes the processes and procedures for planning, organizing, directing, and controlling program operations, and the system put in place for measuring, reporting, and monitoring program performance.
 - (4) For compliance audits, auditors may assess those policies, procedures, practices, and controls relating to compliance criteria established by laws, regulations, contract provisions, grant agreements, and other requirements that could affect the acquisition, protection, and use of the entity's resources and the quantity, quality, timeliness, and cost of services the entity produces and delivers, as determined by the audit objectives. Compliance objectives also concern the purpose of the program, the manner in which it is to be conducted and services delivered, and the population it serves.
 - (5) Performance audits also encompass those policies, procedures, practices, and controls relating to audit objectives that provide prospective analyses, guidance, or summary information.
 - (6) To document the audited entity's internal controls in the audit documentation, auditors may consider using flowcharts, questionnaires, and personal observation to gather, evaluate, and analyze the internal control structure.
- d. To understand and assess the audited entity's internal control structure and meet audit objectives, auditors may use a variety of survey techniques.
- (1) Reviewing applicable laws, regulations, policies, and procedures;
 - (2) reviewing applicable studies, minutes of meetings, and audit reports;
 - (3) examining and analyzing management reports concerning entity administrative, financial, and budgetary operations;
 - (4) conducting discussions with the audited entity and technical personnel to gain an understanding of the entity's operations;
 - (5) interviewing individuals and other concerned persons directly affected by the program to define program goals and identify weaknesses;
 - (6) conducting physical inspections and/or walkthroughs to gain a quick working knowledge of the organization's operation and environment;

- (7) flowcharting the organization's operations;
- (8) outlining, testing, and verifying the general flow of typical actions or transactions; and
- (9) reviewing vulnerability assessments in order to understand and evaluate an organization's internal control structure. See Chapter 2315 (Review of Internal Controls).

2-10. EVALUATING COMPUTER-PROCESSED DATA. When computer-processed data is an important part of the audit and the data's reliability is crucial to accomplishing the audit objectives, the auditors need to satisfy themselves that the data is reliable and relevant. Should computer-processed data not be significant to the audit results, citing the source of the data in the audit report will usually satisfy the reporting standards for accuracy and completeness. In addition, if appropriate, audit programs should contain a comment on the information systems controls for the purpose of assessing audit risk and planning the audit. This would consist of internal controls that are dependent on information systems processing; include general and application controls; are significant to the audit objectives; and if significant, auditors should evaluate the design and operating effectiveness of such controls by performing audit procedures. See Chapter 2230 (Auditing Computer-Based Systems).

- a) Determining How to Assess Reliability of Data. For each assignment, the Auditor-In-Charge will determine the significance of data from the entity's information systems in developing the audit results. If the data is considered critical, then the audit team performing the test work is responsible for ensuring the reliability of computer-processed data used during the audit. However, if the information is not critical to the audit results, then citing the source of the information and stating that it was not verified will usually satisfy the accuracy and completeness reporting standards.
- b) Testing for Data Reliability. If audits of general and application controls have been performed recently, auditors may be able to cite them as a basis for relying on data from the information systems. However, if such controls have changed substantially, have not been reviewed or have been found to be unreliable, the audit staff should determine the validity and reliability of computer-processed data by direct tests of the data to assure that the information that they desire to use is reliable, current, and consistent with its intended use. Such testing could include:
 - Processing test transactions through the information systems;
 - Tracing selected information in the system to source documents or performing physical counts or inspections;
 - Confirming the accuracy and integrity of data in the system by

- interviewing sources independent of the auditee, i.e., third parties such as regular users or suppliers of data from the application; and/or,
 - Reviewing the auditee's own test procedures and results and determining whether there are limitations on how the information can be used to correct control weaknesses.
- c. Audit planning should include a determination of the relevancy and reliability of computer-processed data. If the data are not sufficiently reliable to meet the audit objective(s), the data cannot be used as primary evidence and the auditors will need to plan alternative approaches.
- (1) Factors which the auditors should weigh and document include materiality, cost, and the possibilities and cost of carrying out alternative procedures or not performing an assessment.
 - (2) When evaluating data reliability, auditors are responsible for (1) conducting tests and procedures to ensure the reliability of the data being used; and/or, (2) reviewing general and application controls. In addition to the guidance below, the GAO publication *Assessing the Reliability of Computer-Processed Data* can be helpful in designing a methodology for assessing data reliability.
 - (3) If auditors determine that internal controls over data that is significantly dependent upon computerized information systems are not effective or if auditors do not plan to test the effectiveness of such controls, auditors should include audit documentation regarding the basis for that conclusion by addressing (1) the reasons why the design or operation of the controls is ineffective, or (2) the reasons why it is inefficient to test the controls. In such circumstances, auditors should also include audit documentation regarding their reasons for concluding that the planned audit procedures, such as direct tests of the data, are effectively designed to achieve specific audit objectives. This documentation should address:
 - a. the rationale for determining the types and extent of planned audit procedures;
 - b. the kinds and competence of available evidence produced outside a computerized information system; and
 - c. the effect on the audit report if the evidence gathered during the audit does not allow the auditors to achieve audit objectives.
 - (4) When assessing the reliability of computer-processed data generated or provided by Plan officials or the audited entity, auditors have to ensure that the information systems generating the computer-processed data

have valid and reliable controls when the data is significant to the audit findings. See this chapter (Audit Planning, Section 2-7, Relying on the Work of Others).

- (5) The results of tests should be documented in the workpapers accompanied by flow charts or narratives identifying system controls over the data. Conclusions reached should be cross-indexed to the audit program and final report. If such testing is not performed or if data reliability cannot be established, auditors may need to adjust their audit program or qualify the audit report accordingly.

- 2-11. ASSESSING RISK. Risk assessments identify areas of audit risk and are important in order to complete an audit efficiently and effectively. Risk assessments provide auditors with a systematic process in determining the nature, timing and extent of audit procedures and how to utilize audit staff.

At the beginning of each audit prior to the audit field work, audit groups will meet regarding areas of risk in the audit and document this meeting in the work papers. Areas of risk that could impact the audit include, but are not limited to:

- Audit complexity;
- Findings reported in last audit;
- Adequacy of the audited entity's systems and processes to detect inconsistencies, significant errors or fraud;
- Contracting and upper management concerns;
- Delays in receiving documentation; and,
- Sensitivity of the work.

Based on areas of risk identified for the audit, audit groups will identify controls in place to mitigate these areas of risk. These controls may include adjustments to the audit program, staff expertise, changes in the audit scope or methodology, etc. The time required to complete the audit may need to be adjusted based on the risk factors. Audit groups will document these controls and adjustments in work papers. The following are documented examples of risk assessments.

Healthcare audits:

AUDIT RISK ASSESSMENT

Based on our risk assessment of our auditee, BlueCross Blue Shield of New York (Plan), we considered the complexity of the audit to be HIGH. This is because the Plan ranks 3rd in claim payments and 2nd in administrative expenses paid (both out of 65 Plans) per the CRAM and Annual Accounting Statement statistics. BlueCross Blue Shield of New York paid approximately \$7 billion in FEHBP claim payments and \$500 million in administrative expenses in 2009. Our initial claims scope was from 2007 to 2008, but due to the Plans large benefit payments, we will request an extension of the scope to

include 2009. In addition, since the Plan is one of the largest, we will request approval for an additional auditor to assist in the review of health benefit claims.

Our risk assessment is MODERATE for findings from our previous audit of the Plan (Rpt. No. 1A-10-85-04-100, dated August 18, 2003, for contract years 1999 through 2003) because all findings have been resolved except for the “Amounts Paid Greater than Covered Charges” totaling \$5 million. We will perform reviews to determine if “Amounts Paid Greater than Covered Charges” claim payments are reoccurring during our scope years. The OPM Contracting Officer has concerns about the Plans excessive lobbying charges to the contract of \$1.1 million in 2005. The Plan did not receive pre-approval from OPM for these charges which causes our risk assessment for this factor to be MODERATE. The risk assessment for the sensitivity of our audit work is MODERATE because of our expanded review of health benefit claims and administrative expenses.

We have repeatedly requested for the administrative expense data from the Plan, but they have failed to provide the OIG auditors with the information. Our risk assessment for this factor is MODERATE. If we do not receive the data prior to the start of our on-site audit, we will request assistance from the FEP Director’s Office or we will request approval for an audit extension by one week.

Non-Healthcare audits:

AUDIT RISK ASSESSMENT

Based on our risk assessment results from our initial review of the inventory and management of the OPM’s sensitive property, we considered the complexity of the audit to be HIGH. We base this on the fact that in recent years OPM mobile information devices, such as laptops, smart phones, and global positioning systems (GPS) have been reported lost or stolen and that personally identifiable information has been compromised.

The scope of the audit covers the policies and procedures for FY 2008 governing OPM’s management and inventory of mobile devices, such as laptops, smart phones and GPSs.

There were no findings or recommendations to be resolved because there were no previous audits of OPM’s controls over sensitive property. Therefore the risk assessment for this factor is LOW.

The Director of OPM has recommended that we perform this audit due to instances reported to him concerning the loss of mobile information devices, which causes our risk assessment for this factor to be HIGH.

OPM’s Center for Contracting, Facilities, and Administrative Services (CCFAS) has an automated tracking system for maintaining the inventory for OPM laptops. Our risk assessment for the system is MODERATE because the initial inventory reports received

from CCFAS were incomplete and obsolete.

OPM's CCFAS has provided the OIG auditors with all the requested policies and procedures and has allowed us to initially interview the key representatives from OPM's program offices responsible for inventory and management of sensitive property. Our risk assessment for this factor is LOW.

The risk assessment for the sensitivity of our audit work is HIGH because of the potential of the media finding out that OPM laptops containing confidential information were lost by OPM employees.

- 2-12. ASSESSING FRAUD. Fraud is an intentional misrepresentation of fact that results in the violation of a statute or implementing regulation. See Chapter 2325 for further details.

At the beginning of each audit prior to the audit field work, audit groups will meet with the Office of Investigations regarding areas of potential fraud. Areas identified need to be followed up on during the audit. The original meeting and subsequent follow-up meetings will be documented in the work papers. Furthermore, auditors will meet with the auditee's fraud representatives regarding fraud and complete a fraud questionnaire (See Exhibits C - Healthcare and D - Non-Healthcare). This questionnaire and meeting will be documented in the audit work papers. Some of the areas covered by the questionnaire include:

- Anti-Fraud Policy;
- Anti-Fraud Unit;
- Fraud Awareness Training Program;
- Fraud Hotline;
- Fraud Contact;
- Current Fraud Investigations; and,
- Fraud Recovery Amounts.

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL

*AUDIT STAFF DECLARATION OF PERSONAL
AND FINANCIAL INDEPENDENCE*

As evidenced by my signature, affixed below, I declare to the best of my belief and knowledge, that neither I nor my immediate family have a personal, employment or financial interest in the entity being audited (or its major affiliates and/or subcontractors). I know of no circumstances that might cause knowledgeable third parties to question my impartiality or independence relative to this assignment. As an auditor I have utilized the Government Auditing Standards' conceptual framework for independence including evaluating the following broad categories of threats to my independence:

- a. Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;
- b. Self-review threat - The threat that an auditor who has to review work that they previously performed might not identify shortcomings in their own work for fear of penalty (either financial or reputational).

For example: if the external auditor prepared the financial statements and then audited them.

- c. Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;
- d. Familiarity threat - the threat that aspects of a relationship with management or personnel of an audited entity, such as a close or long relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;
- e. Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;
- f. Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and
- g. Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.

I agree to report to my supervisor any circumstances which arise during the time of my assignment to this audit that may impair my independence (e.g., the offer of a job from the

audited entity or the discovery of previously unknown circumstances).

I understand that the Office of the Inspector General's Ethics Officer and my supervisor may review my Financial Disclosure Statement if deemed necessary under the circumstances.

_____ date

_____ date

_____ date

_____ date

_____ date

_____ date

_____ date

_____ date

_____ date

_____ date

Exhibit B

[Name of the Plan]
[Location]
[Report Number]
[Contract Years 200X and 200X]

TIME PHASED AUDIT PLAN:

AUDIT STAGES	BUDGET DAYS	ACTUAL DAYS*	ESTIMATED COMPLETION DATE **	ACTUAL COMPLETION DATE*
Audit Notification			01/01/08	xx/xx/08
Pre-audit	XX	XX	03/28/08	xx/xx/08
On-Site/Fieldwork	XX	XX		
- Entrance Conference			04/01/08	xx/xx/08
- Exit Conference			05/01/08	xx/xx/08
- End of Fieldwork			06/01/08	xx/xx/08
Post Audit				
- Draft	XX	XX	08/01/08	xx/xx/08
- Response Received			10/01/08	xx/xx/08
- Final to QAG	XX	XX	01/01/09	xx/xx/08
TOTALS . . .	XX	XX		

**Time estimate based on audit performed by AIC and staff.

***Variance:**

If actual days exceed the budgeted days or actual completion date exceeded estimated completion date for any section please explain why.

Fraud Assessment Questionnaire for Healthcare Audits

1. Does the Plan have a fraud unit or a Special Investigative Unit? Is it specific to certain lines of business or does it cover all lines of business? Does it include FEHBP claims? Are there or were there any FEHBP specific investigations?
2. How long has the Plan's fraud unit been in operation?
3. Does the Plan have a written Anti-Fraud policy statement? If yes, please provide a copy with your response. If no, please explain why not?
4. If your response to question No. 3 is yes, to whom and how is this policy communicated?
5. Does the Plan have written policies and procedures to be followed by all personnel for the deterrence and detection of fraud?
6. Does the Plan have a formal training program on fraud awareness?
7. Does the Plan have both an internal and external fraud hotline? If yes, how is the existence of the hotline communicated to its targeted user?
8. Does the Plan have a subscriber/member education program?
9. In the Plan's claim or health care delivery system, does the Plan use fraud protection (or detection) software?
10. Does the Plan have any programs in place to prevent or detect fraudulent enrollments?
11. Does the Plan have systems in place to protect claims, member, and provider information from unauthorized use or access?
12. How does your fraud and abuse program address "patient safety" when fraud issues turn into patient safety issues?
13. Who is the primary Plan contact for fraud and abuse issues? Is this person the primary contact for all lines of business? Please provide a business card.
14. Describe the background of SIU staff (i.e., does the Plan employ experienced and trained investigators?)
15. Does the Plan maintain a log/listing of corporate fraud recoveries?
16. Does the Plan maintain a log/listing of FEHBP fraud recoveries?

Exhibit C
2 of 2

17. How does the Plan obtain repayment of fraud recoveries?
18. Are any fraud recovery amounts settled? If so, (and if FEHBP is included in the overpayments) how is the FEHBP allocation determined?
19. Obtain an explanation of the Plan's process for returning fraud recoveries to the FEHBP.
20. Who is your contact at OPM with regard to fraud and abuse matters?

Exhibit D

Fraud Assessment Questionnaire for Non-Healthcare Audits

1. Does the program office have a fraud unit in operation? Who is the primary contact for fraud issues?
2. Does the program office have a formal fraud policy which defines fraud and appropriate actions to be taken with respect to instances of fraud? The policy should be formally communicated and available on the program offices intranet.
3. Does the program office react to and deal with acts of fraud, or suspected fraud, in a manner that sends a strong message throughout the program office that helps reduce the likelihood of future incidents?
4. Does the program office exhibit a positive workplace environment which minimizes employees' sense of feeling abused, threatened, or ignored?
5. If the program office has experienced any frauds in the past, have they evaluated the reasons that led to the fraud and taken corrective action? The auditors should review all fraud cases that have occurred over a five-year period.
6. Does the program office have a written code of ethics and business conduct?
7. Does the program office conduct fraud, ethics, and security training for new employees and periodic updates for existing employees?
8. Has the program office explicitly considered the need for fraud prevention in the design and maintenance of the system of internal controls?
9. Does the program office have controls over physical and logical access, i.e.:
 - locking doors, desk, and cabinets when unattended?
 - use of ID's and passwords?
 - installed, for especially sensitive areas, computerized security or electronic surveillance systems, or both?
10. Does the program office have written, specific job description and are they adhered to?
11. Do supervisors have adequate fraud awareness, that is, are they alert to the possibility of fraud whenever an unusual or exceptional situation occurs, i.e. customer or annuitant complains about their accounts or payments?
12. Do supervisors diligently review their subordinates work, when appropriate?
13. Has there ever been an internal audit done of this program office? Is there a copy of the audit for our review?

EXAMPLE OF AN AUDIT PLANNING DOCUMENT/MEMORANDUM**Name of Group****Audit Title****Audit Report Number****AUDIT PLANNING MEMORANDUM****INTRODUCTION/BACKGROUND/AUDIT AUTHORITY**

- The Type of Examination (i.e. audit, review, inspection, evaluation, agreed upon procedures, etc.)
- Legal Authority:
Authority to conduct the examination (i.e., Inspector General Act, specific statutory requirement, etc.).
- Summary Description of the Reason for the Audit
- Audit Location:
Location(s) where the audit will take place.
- Auditee's Background
- OIG Audit History:
Previous audit experience and the status of prior audit findings.
- Office of Insurance Programs and Investigation Concerns:
Detail any concerns raised by Insurance Programs or Investigations
- OPM Program or Contracts
- Known Deficiencies or Problems
- Systems Used to Develop, Allocate, and Control Costs
- Types and Flow of Transactions

AUDIT OBJECTIVE

The audit objective(s)

AUDIT SCOPE AND METHODOLOGY

- The Type of Audit (i.e. performance, financial, etc.)
- Audit Scope:
State the areas to be reviewed.
- The Time Period Covered by the Audit
- Audit Limitations Placed on the Audit by Data or Scope
- Summary of the Overall Procedures to be Performed
- Sampling Methods:
Identify sampling techniques and if appropriate, whether the results will be projected to the population
- Relying on the Work of Others:
Identify applicable audits, reviews, and inspections and determine the extent to which this work can be used. Evaluate the adequacy, competency, and usefulness of the work of others.
- Assessing Compliance with Applicable Requirements of Laws and Regulations:
Identify laws, regulations, and other compliance requirements (i.e. provisions of contracts or grant agreements) and design audit steps and procedures that will provide reasonable assurance that the audited entity has adhered to the requirements of the laws and regulations applicable to the audit.
- Assessing Internal Controls:
Determine if the objective and scope requires an understanding of the audit entity's internal control structure to help determine the nature, timing, and extent of audit tests to be performed to ensure that management objectives are met. If the assessment of internal controls is not required, state that no consideration of internal controls was necessary; the audit approach consisted mainly of substantive testing; and, no opinion was expressed.
- Assessing Fraud:
Identify areas of potential fraud by meeting with Office of Investigations and auditee's fraud representatives. Evaluate identified areas.

- **Assessing Risk:**
Based on areas of risk identified for the audit, audit groups will identify audit procedures necessary to audit these areas of risk. These procedures may include adjustments to the audit program, staff assignments, audit scope, etc. Audit groups will document any audit process adjustments in work papers.
- **Evaluating Computer Processed Data:**
Determine the significance of data from the entity's information systems controls in developing the audit results. Determine the validity and reliability of computer-processed data by direct tests of the data to assure that the information that they desire to use is reliable, current, and consistent with its intended use.
- **Using Computers:**
Identify the use of any computer assisted techniques

AUDIT BUDGET AND STAFF RESOURCES

- Staff Days
- Estimated Travel Costs
- Staffing Requirements/Assignments
- Time Table:
General time frame for the audit. Estimated completion dates for Pre-Audit, Field Work, Post Field Work, Draft Report, and Final Report.

TECHNICAL ASSISTANCE

- Use of Specialists or Assistance from Other Groups

PREPARED BY:

Staff name, Auditor-In-Charge Date

APPROVED BY:

Staff name, Senior Team Leader Date

APPROVED BY:

Group Chief, (name of group) Date

United States of America
**Office of
Personnel Management**

EXHIBIT F

Office of the General Counsel
Washington, D.C. 20415

In Reply, Refer To

Your Reference

October 1, 1993

MEMORANDUM FOR CONFIDENTIAL FINANCIAL DISCLOSURE REPORT FILERS
OFFICE OF THE INSPECTOR GENERAL

THROUGH:

E. JEREMY HUTTON *E. Jeremy Hutton*
SPECIAL COUNSEL
OFFICE OF THE INSPECTOR GENERAL
(ETHICS POINT OF CONTACT)

FROM:

[REDACTED] (b) (6)
ALTERNATE DESIGNATED AGENCY ETHICS OFFICIAL

SUBJECT:

Annual Filing of Confidential Financial Disclosure
Report (SF 450)

(b) (5)
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b) (5)
(b) (5)

[REDACTED]

Thank you for your cooperation and for your assistance in maintaining high standards of ethical conduct in the U.S. Office of Personnel Management.

Attachments

cc: The Honorable Patrick E. McFarland
Inspector General

Executive Branch Personnel
CONFIDENTIAL FINANCIAL
DISCLOSURE REPORT

Instructions for Completing SF 450

A. Who Must File

Your agency will inform you if the position in which you serve or will serve has been designated as requiring confidential financial disclosure. Agencies are required to designate positions at or below GS-15, O-6, or comparable pay rates, in which the nature of duties may involve a potential conflict of interest. Examples include contracting, procurement, administration of grants and licenses, regulating/auditing non-Federal entities, other activities having a substantial economic effect on non-Federal entities, or law enforcement. Additionally, all special Government employees (SGE's) (those appointed pursuant to 18 U.S.C. 202(a) to serve no more than 130 days in a period of 365 days) must file, unless exempted or subject to the public reporting system. Agencies may also require certain employees in positions above GS-15, O-6, or a comparable pay rate to file.

B. Reporting Periods

New entrant reports: The reporting period is the preceding twelve months from the date of filing.

Annual reports: The reporting period is the preceding twelve months ending September 30 (or any portion thereof not covered by a new entrant report). However, no report is required if you performed the duties of your position for less than 61 days during that twelve-month period.

C. When to File

New entrant reports: Reports are due within 30 days of assuming a position designated for filing (including reappointment as a special Government employee (SGE)), unless your agency requests the report earlier. No report is required if you left another (different) filing position within 30 days prior to assuming the new position.

Annual reports: Reports are due not later than October 31, unless extended by your agency.

D. Where to File

With ethics officials at the agency in which you serve or will serve, in accordance with their procedures.

E. General Instructions

1. Confidential filers must provide sufficient information about their outside interests and activities, as well as those of their spouse and dependent children, so that an informed judgment can be made by agency ethics officials as to compliance with applicable conflict of interest laws and standards of conduct regulations. Therefore, it is important that you carefully complete the attached form. This report is a safeguard for you as well as the Government. It provides a mechanism for determining actual or potential conflicts between your public responsibilities and your private interests and activities, and allows you and your agency to fashion appropriate protections against such conflicts.

2. This form consists of five parts, which require identification of certain specific financial interests and activities. No disclosure of amounts or values is required. You must complete each part (except as indicated for Part V) and sign the report. If you have no information to report in any part or do not meet the threshold values for reporting, check the "None" box. If you are a new entrant or special Government employee

(SGE), you are not required to complete Part V; in all other instances, a report is incomplete if any part is left blank.

3. The information to be disclosed on this form is required by regulation. You may include other information beyond these requirements that you wish to disclose for clarification. However, disclosure of any information does not authorize holdings, income, liabilities, affiliations, positions, gifts or reimbursements which are otherwise prohibited by law, Executive order, or regulation.

4. You can combine on one form the information applicable to yourself, your spouse, and dependent children which is required by Parts I, II, and V. (Parts III and IV require disclosures about yourself only.) You may, if you desire, distinguish any entry for a family member by preceding the entry with S if it is for a spouse or DC if it pertains to a dependent child. Joint assets may be indicated by J. Information about your spouse is not required in the case of marriage dissolution, permanent separation, or temporary separation with the intention of terminating the marriage or permanently separating.

5. In the case of references to trades or businesses which do not have publicly traded securities, you must provide sufficient information about these private entities to give the reviewers an adequate basis for conflict analysis. Thus, you must disclose the location and primary trade or business of private entities, as well as their separate financial interests and liabilities which are not solely incidental to the business. For instance, if your family swimming pool services corporation purchases an apartment house for investment in addition to its pool services business, you will have to disclose the apartment house investment, in addition to the family corporation.

6. In the case of a mutual fund, pension, IRA, or investment account, you must disclose information about portfolio holdings and sources of income, unless the entity is "an excepted investment fund." See definition below. In that case, identify it by name and

indicate "excepted investment fund" in the appropriate block; no further disclosure is required.

7. In the case of a trust, you must disclose information about its underlying assets and sources of income, unless it is an "excepted trust." See definition below. In that case, identify it by name and date of creation, and indicate "excepted trust" in the appropriate block; no further disclosure is required. (Additionally, you may, in rare cases, have an interest in a trust specifically certified by the Office of Government Ethics to be a qualified blind or diversified trust, pursuant to statute; for such qualified trusts, you will also be exempt from disclosures about underlying holdings.)

8. If you need assistance in completing this form, contact the ethics officials of the agency in which you serve or will serve.

F. Definition of Terms

o Dependent Child

The term "dependent child" means your son, daughter, stepson, or stepdaughter if such person is either:

- (1) unmarried, under age 21, and living in your household; or
- (2) a "dependent" of yours within the meaning of section 152 of the Internal Revenue Code of 1986, 26 U.S.C. 152.

o Excepted Investment Fund (EIF)

An "excepted investment fund" is a mutual fund, common trust fund of a bank, pension or deferred compensation plan, or any other investment fund, which is:

- (1) widely held;
- (2) either publicly traded (or available) or widely diversified"; and
- (3) you neither exercise control over nor have the ability to exercise control over the financial interests held by the fund.

*A fund is widely diversified when it holds no more than 5% of the value of its portfolio in the securities of any one issuer (other than the U.S. Government) and no more than 20% in any particular economic or geographic sector.

o Excepted Trust (ET)

An "excepted trust" is one which:

- (1) was not created by you, your spouse, or dependent children; and
- (2) the holdings or sources of income of which you, your spouse, and dependent children have no past or present knowledge.

o Honoraria

The term "honoraria" means payments (direct or indirect) of money or anything of value to you or your spouse for an appearance, speech or article, excluding necessary travel expenses. Also included are payments to charities in lieu of honoraria.

o Personal Savings Account

The term "personal savings account" includes a certificate of deposit, a money market account, a savings account, an interest-bearing checking account, or any other form of deposit in a bank, savings and loan association, credit union or similar financial institution. Additionally, any money market mutual fund holding is treated as the equivalent of a personal savings account.

Privacy Act Statement

Title I of the Ethics in Government Act of 1978 (5 U.S.C. App.), Executive Order 12674, and 5 CFR Part 2634, Subpart I, of the Office of Government Ethics regulations require the reporting of this information. The primary use of the information on this form is for review by Government officials of your agency, to determine compliance with applicable Federal conflict of interest laws and regulations. Additional disclosures

of the information on this report may be made: (1) to a Federal, State, or local law enforcement agency if the disclosing agency becomes aware of a violation or potential violation of law or regulation; (2) to a court or party in a court or Federal administrative proceeding if the Government is a party or in order to comply with a subpoena; (3) to a source when necessary to obtain information relevant to a conflict of interest investigation or decision; (4) to the National Archives and Records Administration or the General Services Administration in records management inspections; (5) to the Office of Management and Budget during legislative coordination on private relief legislation; and (6) in response to a request for discovery or for the appearance of a witness in a judicial or administrative proceeding, if the information is relevant to the subject matter. This confidential report will not be disclosed to any requesting person unless authorized by law.

Falsification of information or failure to file or report information required to be reported may subject you to disciplinary action by your employing agency or other appropriate authority. Knowing and willful falsification of information required to be reported may also subject you to criminal prosecution.

Public Burden Information

This collection of information is estimated to take an average of one and a half hours per response, including time for reviewing the instructions, gathering the data needed, and completing the form. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Associate Director for Administration, U.S. Office of Government Ethics, Suite 500, 1201 New York Avenue NW., Washington, DC 20005-3917; and to the Office of Management and Budget, Paperwork Reduction Project (3209-0006), Washington, DC 20503. Do not send your completed financial disclosure report to these addresses; it should be filed as indicated above in section D.

Executive Branch CONFIDENTIAL FINANCIAL DISCLOSURE REPORT

PARTS I - II

Employee's Name (Last, first, middle initial)		Position/Title	Grade	Date of Appointment	Page No.
Agency		Branch/Unit and Address	Work Phone	Check box if special Government employee (SGE) <input type="checkbox"/>	
I certify that the statements I have made on this form and all attached statements are true, complete, and correct to the best of my knowledge.			Signature of Employee	Date	Reporting Status: <input type="checkbox"/> New entrant <input type="checkbox"/> Annual
Date Received by Agency	On the basis of information contained in this report, I conclude that the filer is in compliance with applicable laws and regulations (except as noted in "comments" box below).		Signature of Supervisor/Other Intermediate Reviewer	Printed Name/Title	Date
Signature of Agency's Final Reviewing Official and Title		Date	Comments of Reviewing Officials		(Check box if continued on reverse) <input type="checkbox"/>

(Use additional copies of this form as continuation pages, if necessary, to complete any part.)

Part I: Assets and Income

None

Identify for you, your spouse, and dependent children: 1) each asset held for investment or the production of income which had a fair market value exceeding \$1,000 (\$5,000 for personal savings accounts) at the close of the reporting period; and 2) each asset or source of income (other than U.S. Government salary or retirement, including the Thrift Savings Plan) which generated over \$200 in income during the reporting period (\$1,000 for your spouse's earned income, other than honoraria). This includes but is not limited to employers, stocks, bonds, tax shelters, personal savings accounts, realty, mutual funds, pensions, annuities, IRA assets, trust assets, commodity futures, trades and businesses, partnership interests, and honoraria. Exclude your personal residence, unless you rent it out, and any earned income of your dependent children. If the holding is an excepted trust (ET) or an excepted investment fund (EIF) (see instructions), indicate that in the designated column, and you need not disclose underlying holdings.

Assets and Income Sources (Identify specific employer, business, stock, bond, mutual fund, financial institution, type/location of real estate, etc.)	(X) if no longer held	Nature of Income (Rent, interest, dividends, capital gains, salary, etc.)	If EIF or ET, so indicate	Date (Only for honoraria)
1				
2				
3				
4				
5				
6				
7				
8				

Part II: Liabilities

None

Report liabilities over \$10,000 owed to any one creditor at any time during the reporting period (over \$10,000 at the end of the period if revolving charge accounts) by you, your spouse, and dependent children. Exclude a mortgage on your personal residence unless it is rented out; loans secured by automobiles, household furniture or appliances; and liabilities owed to a spouse, dependent child, or parent, sister or child of you or your spouse.

Creditors (Name and address)	Type of Liability (Mortgage, promissory note, etc.)
1	
2	
3	
4	

Executive Branch CONFIDENTIAL FINANCIAL DISCLOSURE REPORT

PART III - END

Employee's Name (<i>Last, first, middle initial</i>)	Agency	Branch/Unit	Work Phone	Page No.
--	--------	-------------	------------	----------

Part III: Outside Positions

None

Report any positions, whether or not compensated, which you held outside the U.S. Government during the reporting period. Positions include but are not limited to those of an employee, officer, director, trustee, general partner, proprietor, representative, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities or those solely of an honorary nature. You need not report any positions of your spouse or dependent children.

Organization (<i>Name and address</i>)	Type of Organization	Position	(X) if no longer held
1			
2			
3			
4			
5			

Part IV: Agreements and Arrangements

None

Report your agreements or arrangements for future employment, leaves of absence, continuation of payment by a former employer (including severance payments), or continuing participation in an employee benefit plan. You need not report agreements or arrangements of your spouse or dependent children.

Terms of Any Agreement or Arrangement	Parties	Date
1		
2		
3		
4		

Part V: Gifts and Travel Reimbursements

None

Do not complete this part if you are a new entrant or special Government employee (SGE).

Report the source and a brief description of gifts from one source totalling \$250 or more during the reporting period, and travel reimbursements from one source totalling \$250 or more during the reporting period, which are received by you, your spouse, and dependent children. Exclude anything valued at \$100 or less; anything from relatives or from the U.S. Government; anything given to your agency in connection with your official duties; and food, lodging, or entertainment as personal hospitality at the donor's residence or premises.

Source	Description (<i>For travel-related items, include itinerary and date</i>)
1	
2	
3	
4	
5	
6	



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, D.C. 20415-0001

EXHIBIT G

October 13, 1993

MEMORANDUM TO ALL OIG EMPLOYEES

FROM: E. JEREMY HUTTON
SPECIAL COUNSEL TO
THE INSPECTOR GENERAL

SUBJECT: Required Notice of Outside Employment

(b) (5)
[Redacted]

[Redacted]

[Redacted]

[Redacted]

Please contact me if you have any questions.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2215

Managing the Audit

CHAPTER 2215 - MANAGING THE AUDIT

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. MANAGING THE AUDIT	
2-1. Background.....	2
2-2. Audit Management and Supervision.....	2
2-3. Audit Cycles.....	5
2-4. Pre-Audit: Survey.....	5
2-5. Pre-Audit: Planning.....	7
2-6. Field Work.....	7
2-7. Reporting.....	9
2-8. Entrance/Exit Conference Protocol.....	10

CHAPTER 2215 - MANAGING THE AUDITSECTION 1. GENERAL

- 1-1. Purpose. Audit management consists of audit planning, including preparing audit programs, conducting pre-survey, survey, field work, and, if applicable, the report preparation and issuance. Each phase requires oversight by management to ensure that audit objectives and professional standards are met and staff are properly supervised. This chapter establishes OIG Office of Audits procedures for managing the audit.
- 1-2. Policy. The OIG Office of Audits will manage audits and attestation engagements in accordance with the Government Auditing Standards issued by the Comptroller General of the United States and OIG policies and procedures.
- a. The Group Chief or designee (Senior Team Leader) will maintain overall responsibility for the management of the audit.
 - b. The Auditor-in-Charge (AIC) or Team Leader is primarily responsible for the daily administration and conduct of the audit. The AIC/Team Leader will assign audit segments to audit staff for completion; provide guidance and assistance to audit staff to ensure appropriate staff development; assess the adequacy of field work; review the staff work products; and communicate and document audit progress to his/her immediate supervisor.
 - c. Staff auditors will complete assigned responsibilities and provide the results to the AIC/Team Leader. Auditors will also prepare a TeamMate document that documents work performed. See Chapter 2220 (Audit Documentation and Files).

SECTION 2. MANAGING THE AUDIT

- 2-1. Background. Proper audit management is critical to the success of the audit. To ensure that the audit meets its objective and work meets professional standards, the audit should be properly conducted and supervised. Responsibilities for overseeing and completing the audit should be assigned. Audit progress should be documented and communicated.
- 2-2. Audit Management and Supervision. The AIC/Team Leader will oversee all aspects of the audit ensuring the accomplishment of audit objectives and preparation of the draft and final reports within established time frames.
- a. To provide proper administrative and technical control over the audit, the AIC/Team Leader shall utilize a TeamMate audit program to implement the audit strategy and plan field work; determine staff requirements and assign staff; select and describe the testing and sampling techniques; estimate time requirements; and record and measure audit progress. See Chapter 2210 (Audit Planning).
 - b. The AIC/Team Leader should attend interviews conducted by audit staff to confirm oral information gathered. The AIC/Team Leader will also inform his/her immediate supervisor/Senior Team Leader regarding difficulties in obtaining information or management refusals to provide information. The AIC/Team Leader and his/her immediate supervisor/Senior Team Leader will decide the appropriate action required to resolve audit problems or difficulties.
 - c. The AIC/Team Leader will ensure that the audit staff receives appropriate guidance, effective on-the-job training, and supervision in conducting the audit and preparing the audit report. Timely supervisory reviews will ensure that audit objectives are met and professional standards are maintained. Since supervision is a continuing process:
 1. The AIC/Team Leader or an experienced auditor should perform sufficient supervisory reviews after the audit staff completes the TeamMate document and/or within 30 days from the end of field work; or
 2. the AIC/Team Leader or an experienced auditor should document in TeamMate the reason for any review that takes place more than 30 days after the field work is completed.
 - d. Supervisory notes, arising from the review of the audit team's automated documentation, must be documented in TeamMate's "coaching notes". To create

or author a coaching note, click on the coaching note icon on the floating TeamMate application bar. The supervisor or an experienced auditor will provide the auditor with coaching notes for any review comments concerning any automated document. The auditor will address the comments and electronically sign off on the coaching note. The supervisor or an experienced auditor will review the response and sign off on the coaching note or send another coaching note if the response is insufficient. See Chapter 2220 (Audit Documentation and Files).

1. In conducting the audit documentation review, the supervisor should consider whether the TeamMate audit program was followed; adequate evidence of work performed; sufficient and appropriate evidence was obtained to support the audit findings; and whether GAS and OIG's policies and procedures were followed.
 2. Supervisors will not be required to check off or tick mark spreadsheet calculations to demonstrate evidence that calculations have been verified if the spreadsheets are prepared using work paper software technology such as Excel or TeamMate. However, the math calculations and/or formulas should be reviewed to ensure that the amounts are correct. See Chapter 2205 (Quality Control and Quality Assurance).
- e. The AIC/Team Leader should keep in mind the following guidance in providing supervision:
1. Determine that audit objectives are met and adheres to professional standards;
 2. review the audit documentation to ensure that it supports the audit findings, conclusions, recommendations and report;
 3. ensure that audit reports and TeamMate summaries are accurate, objective, clear, concise, constructive, and timely;
 4. assign work that is consistent with the abilities and experience of the staff; and
 5. provide suitable instructions that implement the approved TeamMate audit program.

- f. During the audit, the supervisor should also monitor the progress of the audit by: tracking the budgeted/actual time expended and recorded in the planning and/or administration section of TeamMate; and visiting the audit site as necessary to meet with the audit staff to address specific concerns and review audit documentation. See Chapter 2205 (Quality Control and Quality Assurance).
- g. As early as possible, the AIC/Team Leader will contact the audited entity on potential audit findings and recommendations. In addition, the auditors will discuss and document the audited entity's responses in TeamMate.
 - 1. The preferable method for presenting all potential audit findings and recommendations is through written communication between the audit team and the audited entity. Another method for presenting audit findings and recommendations is in some retrievable format. This can be in the form of briefing slides (Microsoft's Power Point) or photographs; electronic media such as video or compact disc formats. When auditors use electronic media to present audit reports, they should be retrievable by the report users and the audit organizations. The audited entity should be asked to respond in writing to all proposed audit findings and recommendations. However, oral comments are acceptable as well, and in some cases, may be the only or most expeditious way to obtain comments. Auditors should prepare a summary of the officials' oral comments and provide a copy of the summary to officials of the audited entity to verify that the comments are accurately stated prior to finalizing the report.
 - 2. In the absence of a written representation, the potential audit findings and recommendations should be presented verbally and a written response should be requested.
 - 3. The AIC/Team Leader will ensure that each finding contains sufficient documentation to demonstrate condition, criteria, cause, and effect, including appropriate recommendations. Also the AIC/Team Leader should ensure that the audit documentation contains support for the findings before the issuance of the audit report. Findings will identify monetary and nonmonetary (procedural) results.
- h. Upon completing the audit, the AIC/Team Leader and staff will discuss the audit results with the managing supervisor/Senior Team Leader. A TeamMate document should be prepared showing attendees and documenting the results of the meeting.

- i. The AIC/Team Leader and appropriate supervisors/Senior Team Leaders will meet with the Group Chief and other senior OIG management as necessary to inform them on all potential audit issues. The meeting should be documented in TeamMate.
- 2-3. Audit Cycles. Audit field work progresses through three phases: pre-audit; field work; and reporting. The pre-audit phase includes: pre-survey; planning; and survey.
- 2-4. Pre-Audit: Survey. During this phase, the auditor conducts initial data gathering and analysis to obtain preliminary background information on the audited entity's operations. The auditor will also acquire a working knowledge of applicable laws and regulations pertaining to the audit. Furthermore the auditor should assess the likelihood of achieving the audit objectives, as well as, continuing to gather information to meet these objectives. Information gathered will be used in preparing the audit planning document and the TeamMate audit program during the planning phase.
- a. The auditors should keep in mind the following guidance for conducting the survey:
 1. Avoid becoming overburdened with detail;
 2. visualize the audit's purpose, particularly identifying problems or limitations that may be encountered, and develop appropriate audit steps;
 3. identify potential areas subject to illegal acts, fraud, waste, and/or abuse;
 4. identify areas that are not material or sensitive and that have strong internal controls to omit from further audit;
 5. perform analytical procedures such as trend and ratio analysis of the audited entity's program or operation inputs, outputs, and results;
 6. prepare TeamMate summaries that identify information for use in conducting the audit; and
 7. isolate potential audit findings including other problem areas warranting review
 - b. Information sources auditors consult may be within the Office of Personnel

Management (OPM), the audited entity, or external to OPM. Some external OPM sources include the U.S. Government Accountability Office, Office of Management and Budget, General Services Administration, other Inspectors General, and state insurance departments.

- c. Information that may be obtained includes the audited entity's mission and function statements; delegations of authority; work load data; contracts; brochures; financial statements and payment data; budget documents; audit reports; laws; bylaws; regulations; and information regarding the responsible officials, personnel, facilities, policies, procedures, computer capabilities and data generated.
- d. Auditors will identify procedural changes and unresolved findings from the prior audit; other applicable audits or reviews; and pertinent management and other characteristics influencing audit risk and materiality. If unresolved findings are identified, auditors should inquire of officials of the audited entity why corrective action wasn't taken to address significant findings and recommendations. Auditors should use professional judgment in determining the prior periods to be considered for follow-up as well as the level of audit work necessary to follow-up on significant findings and recommendations. This places reasonable limits on the accepted level of follow-up on audit findings and recommendations.
- e. Auditors will gain an understanding of the audited entity's internal control structure and assess the impact on the audit scope. In addition, the auditor should ensure that controls are in effect for the audited entity's compliance with applicable laws and regulations. Information systems controls are often an integral part of an entity's internal control. When obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls. See Chapter 2315 (Review of Internal Controls).
- f. When appropriate, auditors will prepare a TeamMate summary document documenting the survey work performed and conclusions and recommendations made. The audit documentation will identify areas for on-site review; describe potential problems, including possible effects and causes; provide conclusions on whether the audit should be conducted; adjusted estimates of required audit resources; and any revisions to the audit program.
- g. The managing supervisors/Senior Team Leaders, AIC/Team Leader, and auditors will decide whether to proceed with the field audit work based on the survey

results. This decision will, in part, depend upon the significance of any deviations from the audit objectives as well as the need for any additional information to fully develop the cause and effect of these deviations. The audit scope, time, and objectives should also be appropriately revised.

- 2-5. Pre-Audit: Planning. During this phase, the AIC/Team Leader will develop and document the audit strategy and prepare the audit planning document and TeamMate audit program. See Chapter 2210 (Audit Planning).
- a. A pre-audit meeting will be held before the entrance conference discussing the information obtained during the survey phase, audit scope, audit assignments, and time estimates for completing the audit. The managing supervisor/Senior Team Leader, AIC/Team Leader, and audit staff will attend this meeting. This meeting will be documented in TeamMate.
 - b. The AIC/Team Leader will keep his/her immediate supervisor/Senior Team Leader informed of the progress throughout the audit. When appropriate, the AIC/Team Leader will provide a written progress report on the status and problems encountered during the audit. Also, the AIC/Team Leader will keep the Group Chief informed on the progress of the audit.
- 2-6. Field Work. During this phase, audit work must be sufficient to draw a conclusion regarding each audit objective and to sufficiently support those audit conclusions.
- a. Auditors will identify applicable criteria; confirm the existence of potential findings; determine the effect of any deficiency; and determine the specific causes of any problems and corrective actions required. Internal audit organizations in government entities may follow the IIA's International Standards for the Professional Practice of Internal Auditing in conjunction with GAGAS for performance audits. In addition, the American Institute of Certified Public Accountants (AICPA) has established professional standards that apply to financial audit engagements for non-issuers performed by certified public accountants (CPA). For financial audits, GAGAS incorporate the AICPA field work and reporting standards and the related Statements on Auditing Standards (SAS) unless specifically excluded or modified by GAGAS. Also, the Public Company Accounting Oversight Board (PCAOB) has established professional standards that apply to financial audit engagements for issuers. Auditors may use GAGAS in conjunction with the PCAOB standards.
 - b. Auditors may request access to personnel, facilities, records, reports, data bases,

documents, and other materials when conducting audits. The auditors shall maintain in TeamMate a record of each request for data identifying the date of the request; to whom the request was made; and date the request was satisfied.

1. When requests are denied, they must be documented in TeamMate and communicated to the AIC/Team Leader; and
 2. the AIC/Team Leader will meet with the audited entity regarding any problems satisfying the request.
- c. Auditors will collect, analyze, interpret, and document information that is sufficient, competent, and relevant to provide a sound basis for audit findings and recommendations.
- d. Audit tests and procedures should be selected in advance and, if appropriate, modified to meet field work conditions.
- e. Documenting and evaluating results may require obtaining written representations from management, including responses to specific audit inquiries. Written representation concerns the competence and completeness of certain evidence from officials of the audited entity. Written representations can take several forms, including summary documents prepared by the auditors and signed by the entity's management.
1. Management's refusal to furnish written representations constitutes an audit scope limitation and may result in the issuance of a qualified audit report. Auditors will document refusals in TeamMate.
 2. For financial audits, the specific written representations obtained by the auditors will depend on the particular circumstances and the nature and basis of management's presentation in the financial statements. These may include:
 - (a) Management's acknowledgement of its responsibility for the fair presentation of the financial statements of financial position, results of operations, and cash flows in conformity with generally accepted accounting principles or other comprehensive basis of accounting, including the absence of errors;
 - (b) completeness and availability of all financial records and related

- data, and minutes of meetings from the audited entity's management and committees;
- (c) information concerning subsequent events;
 - (d) irregularities involving management or employees; and
 - (e) violations or possible violations of laws, regulations, and provisions of contracts or grant agreements whose effects should be considered for disclosure in the financial statements.
- f. When performing a GAGAS examination engagement, auditors should communicate pertinent information that in the auditors' professional judgment needs to be communicated to individuals contracting for or requesting the examination engagement, and to cognizant legislative committees when auditors perform the examination engagement pursuant to a law or regulation, or they conduct the work for the legislative committee that has oversight of the audited entity. In those situations where there is not a single individual or group that both oversees the strategic direction of the audited entity and the fulfillment of its accountability obligations or in other situations where the identity of those charged with governance is not clearly evident, auditors should document the process followed and conclusions reached for identifying the appropriate individuals to receive the required auditor communications.
- 2-7. Reporting. During this phase, the AIC/Team Leader will prepare a draft audit report in written or some retrievable format for the field work results that is complete, accurate, objective, and convincing, and as clear and concise as the subject matter permits.
- a. The AIC/Team Leader is responsible for having the draft report cross-referenced and submitted to the managing supervisor/Senior Team Leader for review and approval. See Chapter 2400 (Audit Report Preparation and Standards).
 - b. The signer of the draft audit report has the option of having the cross-referenced copy of the draft report independently referenced before issuance. The draft audit report is then submitted to the Group Chief or designee (Senior Team Leader), for review and approval. See Chapter 2415 (Indexing and Independent Referencing).
 - c. The Group Chief or designee (Senior Team Leader) will review and approve the draft report. The Group Chief, Senior Team Leader or AIC/Team Leader, will sign the draft report.

- 2-8. Entrance/Exit Conference Protocol. The entrance conference is an introductory meeting while the exit conference summarizes the audit results. Attendees should include the AIC/Team Leader, audit staff, senior OIG officials, and representatives of the audited entity. Shortly after the end of each meeting, auditors will prepare a TeamMate document documenting the results of the meeting. Attendees should provide their name, position, organization and telephone number.
- a. Entrance conference protocol requires the AIC/Team Leader to introduce OIG attendees; explain the OIG function, including audit authority; identify the purpose, scope, and anticipated length of the audit; address any audited entity's concerns about the audit impact on their resources; if applicable, identify and define the audit inquiry process; and explain the reporting process. AIC/Team Leaders should entertain any questions and request a tour of the facilities at the end of the meeting, if feasible.
 - b. The exit conference should be scheduled by the AIC/Team Leader for the last week of the on-site audit to discuss the audit results. Exit conference protocol requires the AIC/Team Leader to introduce OIG attendees; discuss the audit results and determine the audited entity's concurrence or disagreement with audit results; and describe the reporting process.
 - c. During the fiscal year, each Group Chief and managing supervisor/Senior Team Leader should occasionally attend these conferences. The AIC/Team Leader will transmit the expected list of conference attendees to his/her immediate supervisor/Senior Team Leader who will notify the Group Chief.
 1. For those audits conducted outside the Washington, D.C. area, the Group Chief will consider whether the managing supervisor/Senior Team Leader should attend each exit conference and, if the problems are sufficiently critical, whether to attend themselves and to invite the AIGA or DAIGA.
 2. For audits conducted in the Washington, D.C. metropolitan area, the responsible Group Chief should consider attending all entrance and exit conferences.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2220

Audit Documentation and Files

CHAPTER 2220 – AUDIT DOCUMENTATION AND FILESCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. AUDIT EVIDENCE	
2-1. Background.....	4
2-2. Categories of Evidence.....	4
2-3. Tests of Evidence.....	4
2-4. Overall Assessment of Evidence.....	6
2-5. Reasonable Assurance.....	6
2-6. Significance.....	6
2-7. Audit Risk.....	7
2-8. Reporting Insufficient/Inappropriate Evidence.....	7
SECTION 3. PREPARATION AND REVIEW OF AUDIT DOCUMENTATION	
3-1. Planning.....	8
3-2. Audit Documentation Preparation.....	8
3-3. Finalization.....	10
3-4. Indexing.....	10
3-5. Cross-Referencing.....	10
3-6. Procedure Summaries.....	11
SECTION 4. AUDIT DOCUMENTATION REVIEWS	
4-1. General.....	13
4-2. Supervisory Reviews.....	13
4-3. Review Documentation and Follow Up.....	13
4-4. Independent Referencing Review.....	13
SECTION 5. AUDIT DOCUMENTATION FILES	
5-1. Safeguarding and Retaining Audit Documentation Files.....	14

EXHIBITS

- A. Audit Documentation Review Checklists
- B. Auditor Time Log
- C. Finalization

CHAPTER 2220 - AUDIT DOCUMENTATION AND FILESSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter prescribes the policies, criteria, and guidelines for preparing, formatting, reviewing and retaining audit documentation for the OIG Office of Audits.
- 1-2. POLICY. The preparation and review of audit documentation will conform to Government Audit Standards (GAS) issued by the Comptroller General of the United States.
- a. Audit documentation is the link between the field work and the audit reports. It serves as the record of work performed and must contain sufficient, competent, and relevant evidence to support the auditors' findings, opinions, conclusions, and recommendations in the audit reports.
 - b. Audit findings must be adequately supported in the auditors' audit documentation. Evidence is necessary to demonstrate how the conclusions were reached and to provide the basis for determining whether the conclusions are reasonable and correct. Good audit documentation is evidence of properly planned, well-organized, and effectively controlled audits.
 - c. The following basic principles must be observed when preparing audit documentation:
 1. Audit documentation must be complete and accurate, will provide proper support for findings, opinions, and conclusions and will document the nature and scope of the auditors' examination. Audit documentation should contain support for findings, conclusions, and recommendations before auditors issue their report.
 2. Audit documentation must be in sufficient detail to enable a reviewer to ascertain the conclusions reached and the work done to support those conclusions. It should not ordinarily require supplementary oral explanations.
 3. Audit documentation must contain information relating to matters that are materially important and relevant to the objectives of the assignment.
 - d. Under the American Institute of Certified Public Accountants (AICPA) standards and GAGAS, auditors must prepare audit documentation in connection with each audit in sufficient detail to provide a clear understanding of the work performed (including the nature, timing, extent, and results of audit procedures performed),

the audit evidence obtained and its source, and the conclusions reached. Under AICPA standards and GAGAS, auditors should prepare audit documentation that enables an experienced auditor, having no previous connection to the audit, to understand:

1. the nature, timing, and extent of auditing procedures performed to comply with GAGAS and other applicable standards and requirements;
 2. the results of the audit procedures performed and the audit evidence obtained;
 3. the conclusions reached on significant matters; and
 4. that the accounting records agree or reconcile with the audited financial statements or other audited information.
- e. Audit documentation for performance audits should contain at least the following items addressed in GAGAS:
1. the objectives, scope, and methodology of the audit, including sampling and other selection criteria used;
 2. the auditors' determination that certain standards do not apply or that an applicable standard was not followed, the reasons therefore, and the known effect that not following the applicable standard had, or could have had, on the audit;
 3. the work performed to support significant judgments and conclusions, including descriptions of transactions and records examined; and
 4. evidence of supervisory reviews, before the audit report is issued, of the work performed that supports findings, conclusions, and recommendations contained in the audit report.
- f. Audit documentation files must be adequately safeguarded with access restricted to authorized personnel for a time period sufficient to satisfy legal and administrative requirements. Also, if audit documentation is retained electronically, the Office of Audits should ensure that the electronic documentation is capable of being accessed throughout the specified retention period established for audit documentation and that it is safeguarded through sound computer security.

- g. Auditors organize and maintain audit documentation electronically in an automated audit file. The OIG uses the audit management system software called TeamMate, originally developed by PriceWaterhouseCoopers and is currently supported by Wolters Kluwer. TeamMate enables the auditor to move towards a paperless audit environment and bring efficiencies to the audit planning, fieldwork, review, and archival processes. TeamMate provides a common platform for documenting, reviewing, and sharing work during and after the audit.
- h. When performing GAGAS audits and examination engagements and subject to applicable provisions of laws and regulations, auditors should make appropriate individuals, as well as audit and engagement documentation, available upon request and in a timely manner to other auditors or reviewers. Underlying GAGAS audits and examination engagements is the premise that audit organizations in federal, state, and local governments and public accounting firms engaged to perform an audit or examination engagement in accordance with GAGAS cooperate in auditing or performing examinations of programs of common interest so that auditors may use others' work and avoid duplication of efforts. The use of auditors' work by other auditors may be facilitated by contractual arrangements for GAGAS audits and examination engagements that provide for full and timely access to appropriate individuals, as well as audit documentation.

SECTION 2. AUDIT EVIDENCE

- 2-1. BACKGROUND. Audit documentation is the auditors' evidence of the work performed in conducting the audit. This term encompasses all documents, which support the auditors' findings, opinions, conclusions, and recommendations.
- 2-2. CATEGORIES OF EVIDENCE. Evidence required to support audit findings may be categorized and defined as follows:
- a. Physical evidence is obtained by direct inspection or observation of (a) activities of people, (b) property, or (c) events. Such evidence must be documented by a written narrative summarizing the evidence inspected or observed. The summary should include photographs, charts, maps, or actual samples.
 - b. Documentary evidence consists of created information such as laws, manuals, letters, contracts, accounting records, invoices, information systems, and management information on performance. Auditors should refer to Section 4-4 of Chapter 2325 (Fraud, Illegal Acts, and Abuse) for additional information on documenting evidence when fraud, illegal acts, or abuse are suspects.
 - c. Testimonial evidence is obtained from others through statements received in response to inquiries or through interviews. Statements important to the audit must be corroborated when possible with additional evidence. Testimonial evidence also needs to be evaluated from the standpoint of whether the individual may be biased or only have partial knowledge about the area. Auditors should refer to Section 4-4 of Chapter 2325 (Fraud, Illegal Acts, and Abuse) for additional information on documenting testimonial evidence when fraud, illegal acts, or abuse are suspected.
 - d. Analytical evidence includes computations, comparisons, reasoning, and the separation of information into components.
- 2-3. TESTS OF EVIDENCE. The evidence obtained by the auditors must meet the basic tests of sufficiency and appropriateness:
- a. Sufficiency is the measure of the quantity of evidence used to support the findings and conclusions related to the audit objectives. In determining the sufficiency of evidence, auditors should determine whether enough appropriate and convincing evidence exists to address the audit objectives and support the findings, conclusions, and recommendations. Determining the sufficiency of evidence requires judgment. The following statements are useful in judging the sufficiency of evidence:

- a. The greater the audit risk, the greater the quantity and quality of evidence required;
- b. Stronger evidence may allow less evidence to be used;
- c. Having a large volume of audit evidence does not compensate for a lack of relevance, validity, or reliability.

When appropriate, statistical methods may be used to establish sufficiency. See Chapter 2505 (Statistical Sampling Techniques).

- b. Appropriateness is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions. Relevance refers to the relationship of evidence to its use. The information used to prove or disprove an issue is relevant if it has a logical relationship to that issue. Information that has no logical relationship to the issue is irrelevant and, therefore, should not be included as evidence. Validity refers to the extent to which evidence is based on sound reasoning or accurate information. Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported.
- c. In evaluating the appropriateness of evidence, the auditors must carefully consider whether reasons exist to doubt its validity or completeness. If there is a reason for doubt, the auditors should obtain additional evidence or reflect the situation in the audit report. To determine the appropriateness of evidence, the following factors should be considered:
 - (1) Evidence obtained from an independent source provides greater assurance of reliability than that secured from the audited entity.
 - (2) Evidence developed under a good system of internal control is more likely to be reliable than that obtained when such control is weak or nonexistent.
 - (3) Evidence obtained by the auditors through physical examination, observation, computation, and inspection is more reliable than evidence obtained indirectly.
 - (4) Original documents are more reliable than copies.
 - (5) Testimonial evidence obtained under conditions in which persons may speak freely is generally more reliable than evidence obtained under circumstances in which the persons may be intimidated.

- (6) Testimonial evidence obtained from an individual who is not biased and has direct knowledge about the area is generally more reliable than testimonial evidence obtained from an individual who is biased or has indirect or partial knowledge about the area.

2-4. OVERALL ASSESSMENT OF EVIDENCE. Auditors should determine the overall sufficiency and appropriateness of evidence to provide a reasonable basis for the findings and conclusions, within the context of the audit objectives.

When assessing the sufficiency and appropriateness of evidence, auditors should evaluate the expected significance of evidence to the audit objectives, findings, and conclusions, available corroborating evidence, and the level of audit risk. The steps to assess evidence may depend on the nature of the evidence, how the evidence is used in the audit or report, and the audit objectives.

- a. Evidence is sufficient and appropriate when it provides a reasonable basis for supporting the findings or conclusions within the context of the audit objectives.
- b. Evidence is not sufficient or not appropriate when (1) using the evidence carries an unacceptably high risk that it could lead to an incorrect or improper conclusion, (2) the evidence has significant limitations, given the audit objectives and intended use of the evidence, or (3) the evidence does not provide an adequate basis for addressing the audit objectives or supporting the findings and conclusions. Auditors should not use such evidence as support for findings and conclusions.

2-5. REASONABLE ASSURANCE. Performance audits that comply with GAGAS provide reasonable assurance that evidence is sufficient and appropriate to support the auditors' findings and conclusions. Thus, the sufficiency and appropriateness of evidence needed and tests of evidence will vary based on the audit objectives, findings, and conclusions. Objectives for performance audits range from narrow to broad and involve varying types and quality of evidence. In some engagements, sufficient, appropriate evidence is available, but in others, information may have limitations.

2-6. SIGNIFICANCE (similar to Materiality). Significance in a performance audit occurs throughout the audit, including when deciding the type and extent of audit work to perform, when evaluating results of audit work, and when developing the report and related findings and conclusions. Significance is defined as the relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors. Such factors include the magnitude of the matter in relation to the subject matter of the audit, the nature and effect of the matter, the relevance of the matter, the needs and interests of an objective third party with knowledge of the relevant information, and the impact of the matter to the audited program or activity.

Professional judgment assists auditors when evaluating the significance of matters within the context of the audit objectives.

- 2-7. AUDIT RISK. Audit risk is the possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of factors such as evidence that is not sufficient and/or appropriate, an inadequate audit process, or intentional omissions or misleading information due to misrepresentation or fraud. Factors such as the time frames, complexity, or sensitivity of the work; size of the program in terms of dollar amounts and number of citizens served; adequacy of the audited entity's systems and processes to detect inconsistencies, significant errors, or fraud; and auditors' access to records, also impact audit risk. Audit risk includes the risk that auditors will not detect a mistake, inconsistency, significant error, or fraud in the evidence supporting the audit. Audit risk can be reduced by taking actions such as increasing the scope of work; adding experts, additional reviewers, and other resources to the audit team; changing the methodology to obtain additional evidence, higher quality evidence, or alternative forms of corroborating evidence; or aligning the findings and conclusions to reflect the evidence obtained.
- 2-8. REPORTING INSUFFICIENT/INAPPROPRIATE EVIDENCE. If after the report is issued, the auditors discover that they did not have sufficient, appropriate evidence to support the reported findings or conclusions, they should communicate with:
- those charged with governance,
 - the appropriate officials of the audited entity, and
 - the appropriate officials of the organizations requiring or arranging for the audits, so that they do not continue to rely on the findings or conclusions that were not supported.

If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report with revised findings or conclusions.

SECTION 3. PREPARATION AND REVIEW OF AUDIT DOCUMENTATION3-1. PLANNING.

- a. Well-planned and organized audit documentation is necessary to achieve a professional quality audit. Adequate planning is also the key to the development and preparation of good audit documentation. See Chapter 2210 (Audit Planning) and Chapter 2215 (Managing Audit Field Work).
- b. When preparing audit documentation, the auditors must have a clear concept of the primary purpose of the audit document, i.e., understand how the subject of the audit document relates to other audit areas, and what will be done with the written information. Before the auditors develop audit documentation analyses, exhibits, and schedules, the following must also be determined:
 1. What are the objectives or what needs to be proven?
 2. What data or information is needed to complete the analysis?
 3. Where is the data or information located that is required?
 4. What comparisons must be made to prove the condition(s) or conclusion(s)?

3-2. AUDIT DOCUMENTATION PREPARATION.

- a. The purpose of audit documentation files is to document the auditors' work. Audit documentation serves as the basis for the conclusions in the audit report; provide a record of the work done; serve as a basis for the review and evaluation of the work performed; and demonstrate adherence to the applicable auditing standards and procedures. Audit documentation must document:
 - (1) audit planning;
 - (2) the study of evaluation of internal controls;
 - (3) auditing procedures performed and evidence obtained;
 - (4) conclusion reached; and
 - (5) supervisory reviews.
- b. Automated evidential audit documentation may be cross-referenced to a procedure summary template (i.e., B.1.PS), which provides an area to

prepare/write or type information relating to work done on a specific audit step in the audit program. The procedure summary template includes:

1. purpose of the procedure. This information describes why the procedure was performed, and what audit work is being presented. The auditor should try and avoid excessive use of generalized terms in describing the audit work (i.e., "to document");
2. source of information. The source information must specifically identify the records, files, and person(s) (include name, title, and area located) from which the evidence was obtained. The source information must be sufficiently detailed to enable the auditors and others to evaluate the competence or reliability of information and to locate the original documents;
3. scope of the examination. The scope describes the universe being examined in terms of: time and quantity; how evidence was obtained; the basis of selection of items examined; the work performed; and the techniques employed. When factors restrict the scope of the audit or interfere with the auditors' ability to form objective opinions and conclusions, this must be explained in the audit documentation; and
4. conclusions. These are the results drawn from auditors' tests, analysis, and other evidence. When the conclusions recorded on one audit document are based in part on information in other documents, these other documents will be appropriately cross-referenced.

Automated audit documentation prepared by team members and reviewed by supervisory staff is electronically initialed and dated by the individual preparing or reviewing the working papers. Any signs, symbols, tick marks, or acronyms are electronically defined when used for automated audit documentation and schedules. Audit documentation is automatically assigned an index number in TeamMate.

- c. Administrative documentation. From the planning phase of the audit through the reporting phase, the auditor prepares audit documentation or completes required OIG audit forms that assist in the management and supervision of the audit and fieldwork. These documents are usually self-explanatory and considered administrative in nature, e.g., the financial disclosure form or auditor's time log. These types of audit documents do not require information regarding the purpose of the audit document, source of information, scope of the examination, and conclusions reached for understanding individual audit documentation.

3-3. FINALIZATION

Finalization is a unique feature to TeamMate. Finalization of an audit provides the option of retaining or removing all signoff dates and edits. It also provides the option of retaining or removing all coaching notes (See Exhibit C). Before finalizing an audit, the retention option will be selected to retain all signoff dates and edits and all coaching notes. Once the finalization is completed, the audit will be marked "read only" and no changes will be permitted. **Finalization should take place right after the final report is issued.**¹ QA randomly selects completed audit documentation for review after the final report has been issued and after finalization takes place during the semi-annual reporting (SAR) period.

3-4. INDEXING.

- a. The primary purpose of indexing is to facilitate the creation of an audit trail. A secondary purpose is to indicate the relationship of the audit documentation to the particular areas or sections of the audit. This will facilitate cross-referencing on an ongoing basis and will help the AIC to maintain control of audit documents during the course of the audit.
- b. The indexing system will show the logical groupings of interrelated audit documents. Logical groupings will contribute to the ease of referencing and will assist the auditors' analyses, interpretations, and summaries of the results of the audit by major audit sections and audit subjects as well as facilitate the supervisory review. See Chapter 2415 (Indexing and Independent Referencing).
- c. In TeamMate, the Browser is the auditor's Audit Documentation Index within the audit file (Refer to your TeamMate User Manual). TeamMate will automatically assign an index to an audit document.

3-5. CROSS-REFERENCING.

- a. The audit will not be considered complete until the audit documentation files are thoroughly and accurately cross-referenced. Cross-referencing is the audit trail through the audit documentation. Cross-referencing indicates where audit document data or information came from and data and information is carried to. The final audit report is developed through an evolutionary process which begins

¹ For the annual Oversight of OPM's Consolidated Financial Statement Audit, the Teammate project should be finalized within the Independent Public Accountant's contracted period of performance of the audit.

with detailed supporting audit documentation, and follows through to the summaries, findings, and the draft audit report. Cross-referencing at each step in the process ensures that all pertinent facts and conclusions have been considered and that support exists for the auditors' position. This also decreases the probability of a defective final audit report. Further, cross-referencing logically documents the work performed, thereby permitting the reviewer to examine the work performed more efficiently.

- b. Changes and/or corrections made to supporting information must also be referenced to other affected sections of the audit documentation. To be effective, cross-referencing must be done concurrently with the audit work. At a minimum, applicable cross-referencing should be made to the audit documentation from the audit program and the audit document summaries. The draft and final audit reports should be thoroughly cross-referenced to the detailed audit documents.
 - c. TeamMate provides for extensive cross-referencing capabilities (Refer to your TeamMate User Manual). Cross-referencing in TeamMate allows the auditor the ability to automatically navigate or jump from one location to another by clicking a reference link indicator. Cross-referencing is done by using "Hyper links" which provide electronic links back to supporting audit documents. Teammate cross-referencing includes:
 - Point-to-point referencing
 - Point-to-document referencing
 - Automatic Teammate cross-referencing
 - Cross-referencing to external electronic files
 - Two-way number to number cross-referencing
 - d. TeamMate audit documents may cross-reference to a hard copy document. Hard copy audit documents supporting an audit in TeamMate should use the same TeamMate index number that the hard copy supports.
- 3-6. PROCEDURE SUMMARIES. TeamMate's procedure summaries must be prepared for each major audit section and each audit subject where audit evidence, upon which conclusions are based, is developed on multiple audit document pages. The procedure summaries do not qualify as administrative audit documents, and therefore should contain a purpose, scope, source, and conclusion section. These summaries will be used to: (a) consolidate the results of various audit steps; (b) control and administer the audit; and (c) analyze and interpret the audit results.
- a. Summaries will support the development of audit findings and clearly spell out deficiencies, surrounding facts, criteria, causes, effects, and recommended

actions. If no deficiencies are found, that information will also be summarized. Information contained in the procedure summaries must be thoroughly cross-referenced to the detailed audit documents.

- b. Conclusions (both negative and positive) on individual audit documents should be carried forward to summaries. The summaries should be cross-referenced back to the supporting audit documentation. Cross referencing should permit a reviewer to go backwards from the summaries to supporting details.

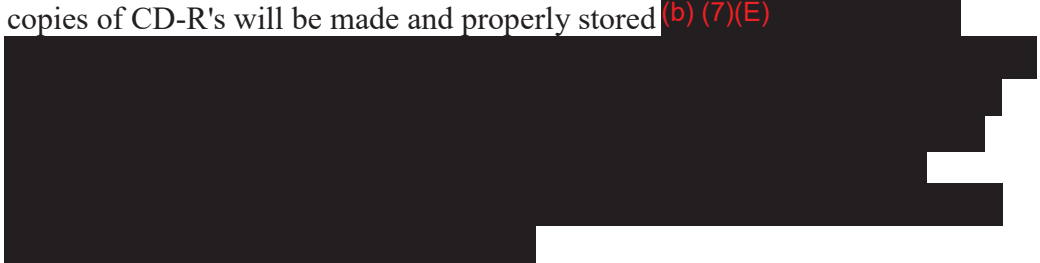
SECTION 4. AUDIT DOCUMENTATION REVIEWS

- 4-1. GENERAL. Audit documentation must be reviewed to ensure that the audit work complies with GAS and established OIG policies and procedures. The reviewer needs to appraise the quality of the audit documentation, the relationship of the audit work to the objectives, and the completeness of the auditors' examination. The reviewer must also assess the auditors' conclusions, determine what additional steps are necessary, and decide whether to expand or cut back the audit coverage.
- 4-2. SUPERVISORY REVIEWS. Individually completed audit documentation will be reviewed by the first line supervisor. Reviews should usually be performed concurrently with the audit work. Higher level audit supervisory personnel should review the overall work to ensure that audit standards have been met; there is adequate support for the auditors' conclusions and recommendations; and, the audit work was conducted with due professional care. Audit Documentation Review Checklists contained in hard copy or automated audit documentation should be completed, initialed, and dated by appropriate supervisory personnel (See Audit Documentation Review Checklists in Exhibit A).
- 4-3. REVIEW DOCUMENTATION AND FOLLOW UP. The reviewer will provide the auditors with the results of the audit documentation reviews in TeamMate's coaching notes.

During the course of the audit fieldwork, supervisory personnel may want to ask questions or write comments about the auditor's work. Within TeamMate, any questions or comments are created and contained in "Coaching Notes" (Refer to your TeamMate User Manual). To create or author a coaching note, simply click on the coaching note icon on the floating TeamMate application bar. The reviewer will provide the auditor with TeamMate coaching notes for any review comments on the paperless audit document. The auditor will address the comments and electronically sign off on the coaching note. The reviewer will review the response and sign off on the coaching note or send another coaching note if the response is insufficient. All coaching notes should be closed before finalizing an audit. However, coaching notes should be kept in the finalizing process. Teammate provides the option of retaining all coaching notes (See Exhibit C). See Chapter 2215 (Managing Audit Field Work).

- 4-4. INDEPENDENT REFERENCING REVIEW. To ensure the accuracy of the facts and figures in the audit reports, an Independent Referencer will review the cross-referenced copy of the final audit report. The signer of a draft report has the option of having the cross-referenced copy of the draft audit report independently referenced. The Referencer must have a minimum of three years of auditing experience and not be directly involved in the field work of the audit work being reviewed. This review will be documented in the audit documentation, the Report Control Folder or both and must contain the Referencer's comments or coaching notes, including how the issues raised were resolved. See Chapter 2415 (Indexing and Independent Referencing).

SECTION 5. AUDIT DOCUMENTATION FILES5-1. SAFEGUARDING AND RETAINING AUDIT DOCUMENTATION FILES.

- a. Audit documentation files must be adequately safeguarded, i.e., locked up when unattended. Access to audit documentation files must be restricted to authorized personnel. Special precautions must be taken with any audit documentation, including draft audit reports, to prevent premature disclosure of their contents and to protect them from theft or destruction. Sensitive audit documentation material must be safeguarded when not in use to prevent leaks and unauthorized disclosure.
- b. Automated audit documentation files must be retained and backed up onto a CD-R after finalization. CD-R's must be properly stored and labeled with the audited entity's name, title/location, report number, and contents. Applicable back-up copies of CD-R's will be made and properly stored (b) (7)(E)

- c. Even when audit documents are automated, it may be necessary to maintain hard copy documentation for certain parts of the audit documentation. This is important when certain documents require official signatures or when proper storage conditions for automated audit documents cannot be ensured.
- d. Automated data tapes and records must be retained until the audit reports have been issued and all audit findings resolved. When data is extracted from a data base system, the sampling plan, the criteria used to select records, the computer program designed to generate the output, and the resulting output must be described and retained.
- e. As a general rule, audit documentation must be retained until completion of the succeeding audit or for a minimum of ten years from the date of the final audit report resolution. Audit documentation relating to a closeout audit must be retained until all issues reported in the final audit report have been resolved. Audit reports that are controversial, unsettled, or of current interest may necessitate holding audit documentation for longer periods. Obsolete or superseded audit material that is no longer needed will not be sent to the records holding centers and may be destroyed.

- f. Audit organizations should establish policies and procedures for the safe custody and retention of audit documentation for a time sufficient to satisfy legal, regulatory, and administrative requirements for record retention. Whether audit documentation is in paper, electronic, or other media, the integrity, accessibility, and retrievability of the underlying information could be compromised if the documentation is altered, added to, or deleted without the auditors' knowledge, or if the documentation is lost or damaged. For audit documentation that is retained electronically, the audit organization should establish information systems controls concerning accessing and updating the audit documentation.

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST
ASSOCIATED WITH THE FINAL REVIEW OF THE AUDIT DOCUMENTATION**

GROUP CHIEF

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

I, _____, have reviewed the audit documentation for the aforementioned audit and have determined that they have been completed in accordance with generally accepted government auditing standards and Office of Inspector General policy.

GROUP CHIEF

1. Are supervisory reviews documented (Date, Name and Comments/Recommendations) including any required follow-up work?

Did reviewer consider:

- a. Whether audit work conforms with professional standards?
- b. Whether audit objectives were accomplished?

2. Does the audit documentation contain evidence that all audit exceptions have been resolved?

Y/N	COMMENTS	DATE

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST
ASSOCIATED WITH THE FINAL REPORT**

SENIOR TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

SENIOR TEAM LEADER

1. Does the audit documentation contain the final report and are they cross-referenced to the final report?

2. Have any changes or corrections made to supporting information been documented and referenced in the:
 - a. Appropriate audit documentation section?
 - b. Audit report control file?

3. Has the audit documentation and audit reports been properly filed for future reference?

Y/N	COMMENTS	Reviewer's Initials	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

SENIOR TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

I, _____, have reviewed the audit documentation for the aforementioned audit and have determined that they have been completed in accordance with generally accepted government auditing standards and Office of Inspector General policy.

SENIOR TEAM LEADER

1. Have the results, conclusions, and recommendations noted in the survey/preaudit summary been approved?
2. Does the survey/preaudit summary incorporate a staffing plan, including the use of specialists, experts, and consultants when needed?
3. Have the survey/preaudit results been incorporated into the audit program?
4. Does the survey/preaudit summary address the possible use of computer hardware/software?
5. Does the audit documentation explain uncompleted portions of the audit program?
6. Are deviations from audit procedures and standards explained in the audit documentation?

Y/N	Comments	Reviewer's Initials	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

SENIOR TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

SENIOR TEAM LEADER

- 7. Are final conclusions based on sufficient, competent and relevant evidence?
- 8. Are adequate audit documentation/procedure summaries prepared for major audit sections and subject areas?
- 9. Are findings properly developed, i.e., condition, cause, criteria, effect, and recommendations in the audit documents?
- 10. Has the Auditor-in-Charge/Team Leader completed all review responsibilities:
 - a. Completed checklist?
 - b. Reviewed each audit document?
 - c. Cross-referenced audit documentation to other audit documents?
 - d. Cross-referenced audit documents to audit documentation/procedure summaries?
 - e. Cross-referenced audit documentation to the audit program?
 - f. Cross-referenced audit documentation to the draft report?
 - g. Completed the audit documentation?

Y/N	Comments	Reviewer's Initials	Date

Legend

Y/N Yes/No
N/A Not Applicable

05/15

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

SENIOR TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

SENIOR TEAM LEADER

- 11. Has all necessary audit work been completed?
- 12. Are changes to or corrections made to audit documents documented and referenced to other affected sections of the audit documentation?
- 13. Are magnetic tapes and diskettes write-protected, labeled, and properly stored?
- 14. Have backup copies of computer diskettes been made and stored in a physically separate location?
- 15. If the audit disclosed illegal acts, were the appropriate investigators consulted?

Y/N	Comments	Reviewer's Initials	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

AUDITOR-IN-CHARGE/TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

I, _____, have reviewed the audit documentation for the aforementioned audit and have determined that they have been completed in accordance with generally accepted government auditing standards and Office of Inspector General policy.

AUDITOR-IN-CHARGE/TEAM LEADER

1. Are the audit documentation binders/files:
 - a. Logically organized?
 - b. Labeled?
 - c. Numbered?
 - d. Properly indexed?

2. Does the audit documentation contain:
 - a. A statement of audit objectives, scope, and methodology (audit program)?
 - b. Audit Documentation Review Checklists and Reviewer Comment Sheets/Coaching Notes?
 - c. The Audit Staff Declaration of Personal and Financial Independence?

3. Does the audit documentation contain and are they cross-referenced to:
 - a. Other hard copy and automated audit documentation?
 - b. Draft report?
 - c. Audit program?
 - d. Audit documentation/Procedure summaries?

Y/N	Comments	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

AUDITOR-IN-CHARGE/TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

AUDITOR-IN-CHARGE/TEAM LEADER

- 4. Was all the work indicated in the audit program completed and documented, or if not were explanations provided?
- 5. Does each major audit section and subsection in the audit documentation contain an audit documentation/procedure summary?
- 6. Does the audit documentation/procedure summaries include the objective of the section, work performed, results achieved, conclusions and recommendations?
- 7. Does each audit document include:
 - a. Identification that the audit documentation is part of the OPM-OIG audit files (written or stamped)?
 - b. Identification and location of the organization, activity or function being reviewed?
 - c. Report number?
 - d. Subject of the audit document?
 - e. The audit period covered by the audit document?
 - f. Purpose, source, scope, conclusion?
 - g. Explanation of any signs, symbols or acronyms used (tick marks)?
 - h. Completed index reference stamp?

Y/N	Comments	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

AUDITOR-IN-CHARGE/TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

AUDITOR-IN-CHARGE/TEAM LEADER

- 8. Are audit documents legible and neat?
- 9. Does audit documentation document that findings were presented to and discussed with the auditee as findings were developed?
- 10. Do the audit documents contain only material that is significant and relevant to the objectives of the assignment?
- 11. Do audit documents stand on their own and require no oral explanation?
- 12. Do the audit documents show the basis for the judgmental techniques used in selecting items for audit?
- 13. If statistical sampling was used, does the audit documentation include:
 - a. A description of how the sampled items were selected?
 - b. Size and characteristics of the audit universe?
 - c. Attributes of the sample (error rates, sampling interval confidence levels, etc)?
 - d. Results of the sample?
 - e. Basis for projecting sample results?
 - f. Other information or data considered appropriate by the auditor?

Y/N	Comments	Date

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

AUDITOR-IN-CHARGE/TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

AUDITOR-IN-CHARGE/TEAM LEADER

- 14. Does the audit documentation contain evidence of a compliance review with applicable laws and regulations?
- 15. Did the audit steps provide reasonable assurance of detecting errors, irregularities, and illegal acts?
- 16. If the audit disclosed indications of irregularities or illegal acts did the auditor:
 - a. Expand testing to substantiate indications?
 - b. Consult with supervisors?
- 17. Does the audit documentation show evidence that the audited entity's internal control system was reviewed?
- 18. Does the audit documentation contain notations or copies of written correspondence sent to the audited entity describing reportable conditions in the internal control system?

Y/N	Comments	Dates

Legend

Y/N Yes/No
N/A Not Applicable

**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF INSPECTOR GENERAL
AUDIT DOCUMENTATION REVIEW CHECKLIST**

AUDITOR-IN-CHARGE/TEAM LEADER

[Auditee Name]

[Audit Title or Auditee Location]

[Report Number]

[Dates of Audit]

AUDITOR-IN-CHARGE/TEAM LEADER

- 19. If using computers, does the audit document:
 - a. All automated procedures and data files used during the audit?
 - b. Processes used for data entry, data verification and the results obtained?
 - c. Conclusions on reliability of computer generated data including documentation of tests performed to reach conclusions?
 - d. Procedures followed to review a computer-based system's general and application controls or to conduct other tests to determine the relevance and reliability of data?
- 20. Entrance/Exit Conferences:
 - a. Documented?
 - b. Supervisor attended?
- 21. Are there any open items that require attention?

Y/N	Comments	Dates

Legend

Y/N Yes/No
N/A Not Applicable

EXHIBIT B

AUDITOR TIME LOG

LOCATION: _____

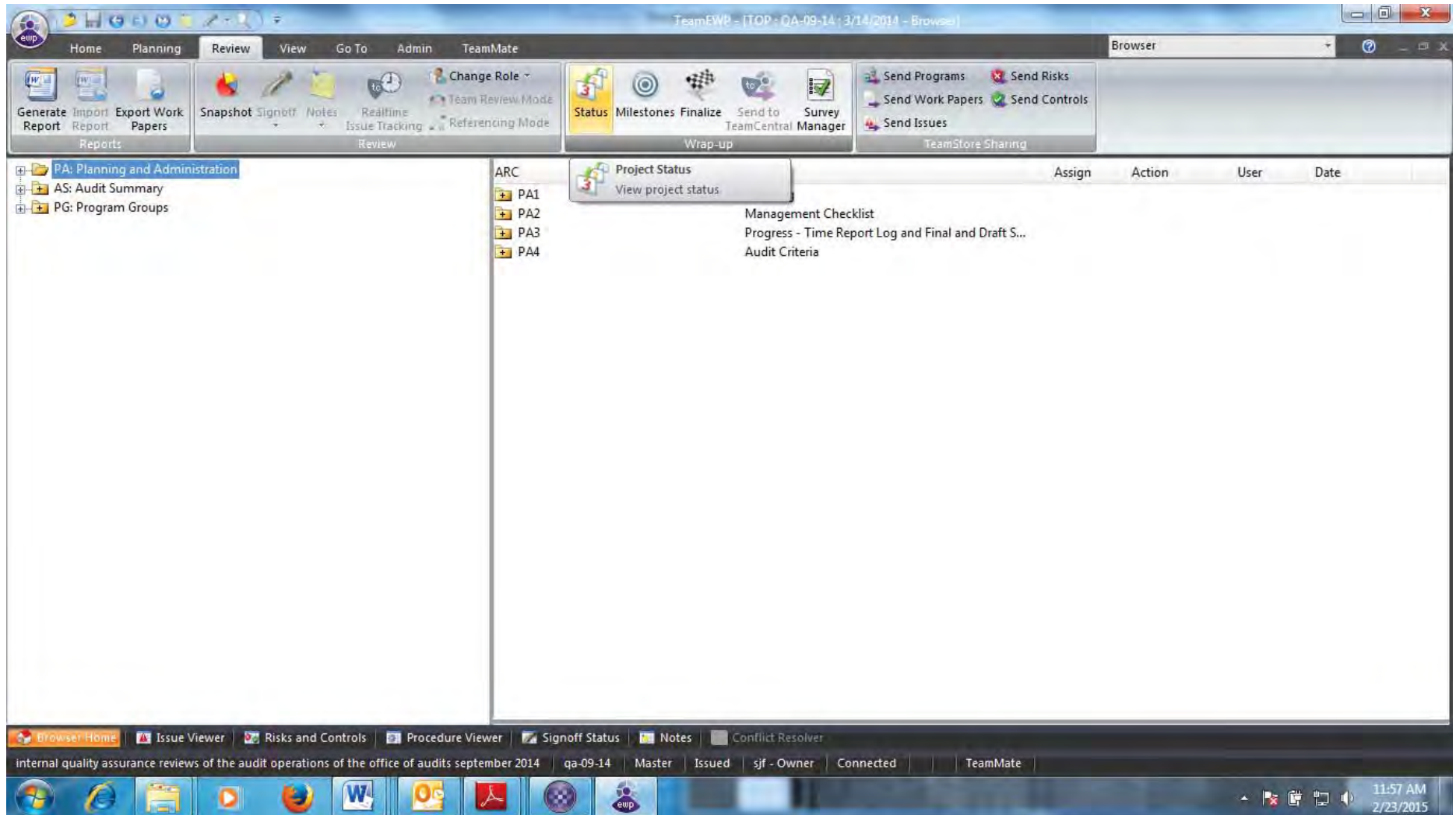
Employee Name	CALENDAR DAYS																																																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																					

MONTH OF: _____

LEGEND

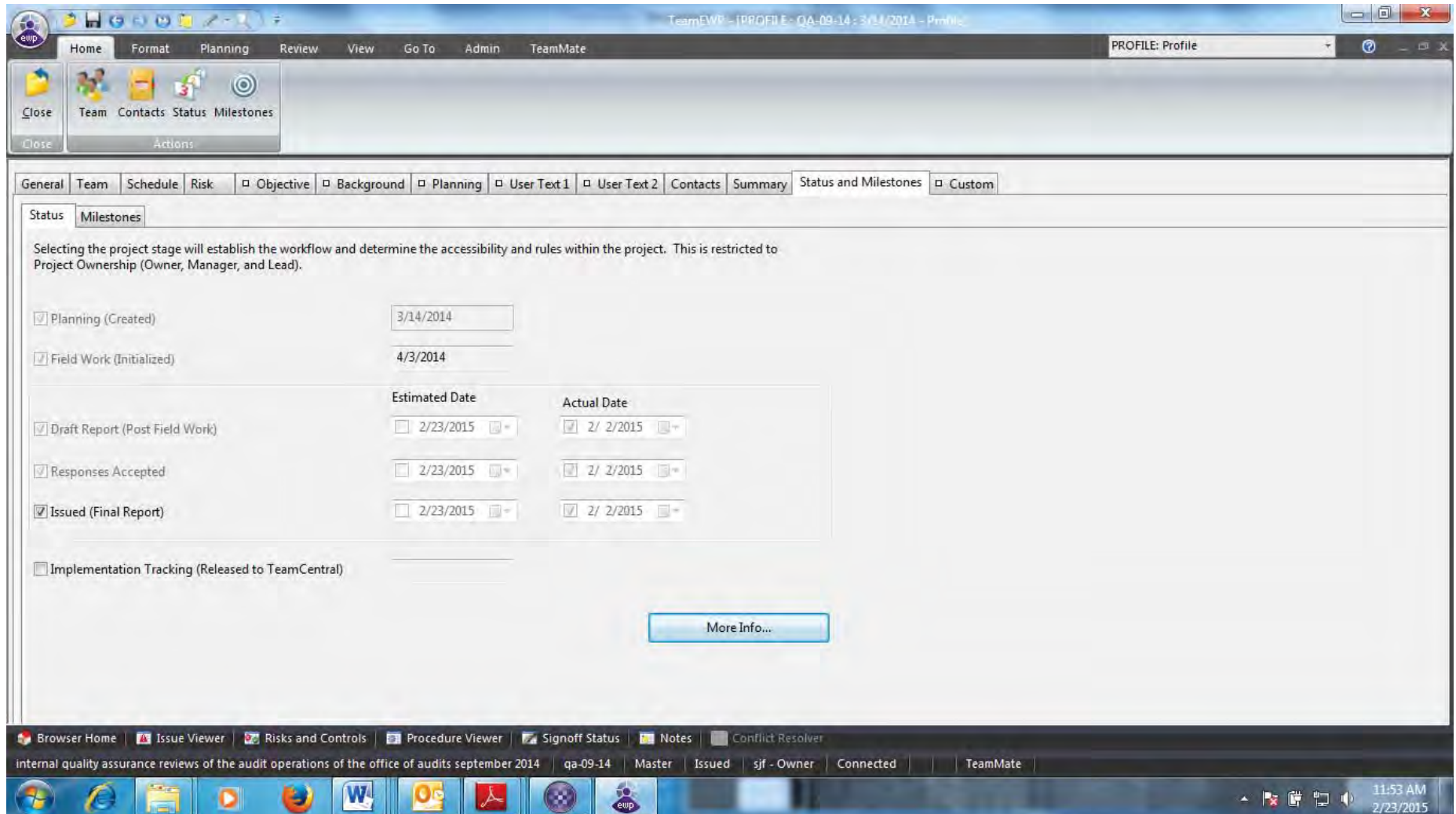
- | | |
|----------------|-----------------------|
| P - PREAUDIT | W - WASHINGTON OFFICE |
| T - TRAVEL | L - LEAVE |
| X - ON-SITE | H - HOLIDAY |
| S - POST AUDIT | R - TRAINING |

FINALIZATION



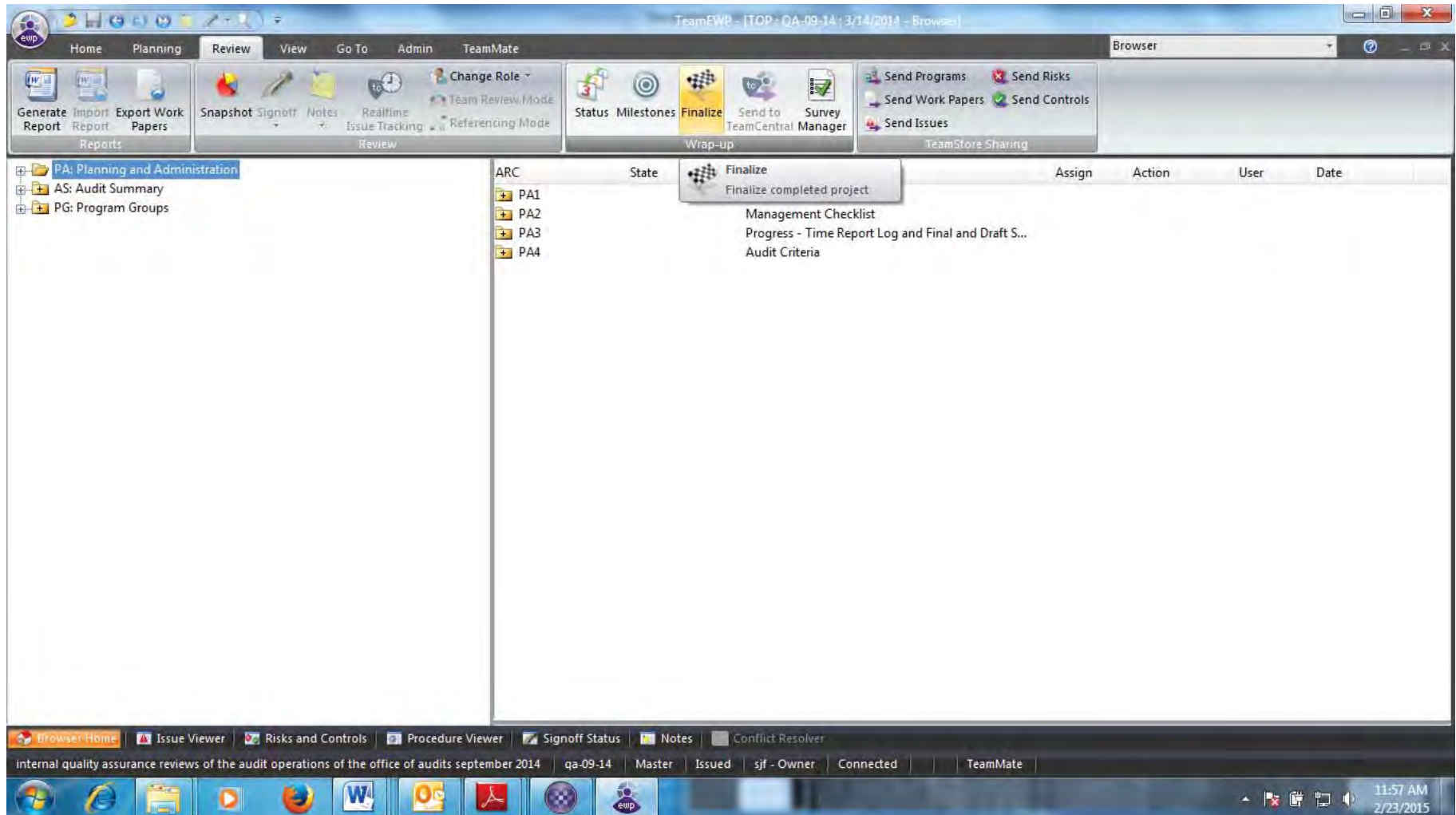
Go to Review Tab in TeamMate Browser and click on "Status" icon.

FINALIZATION



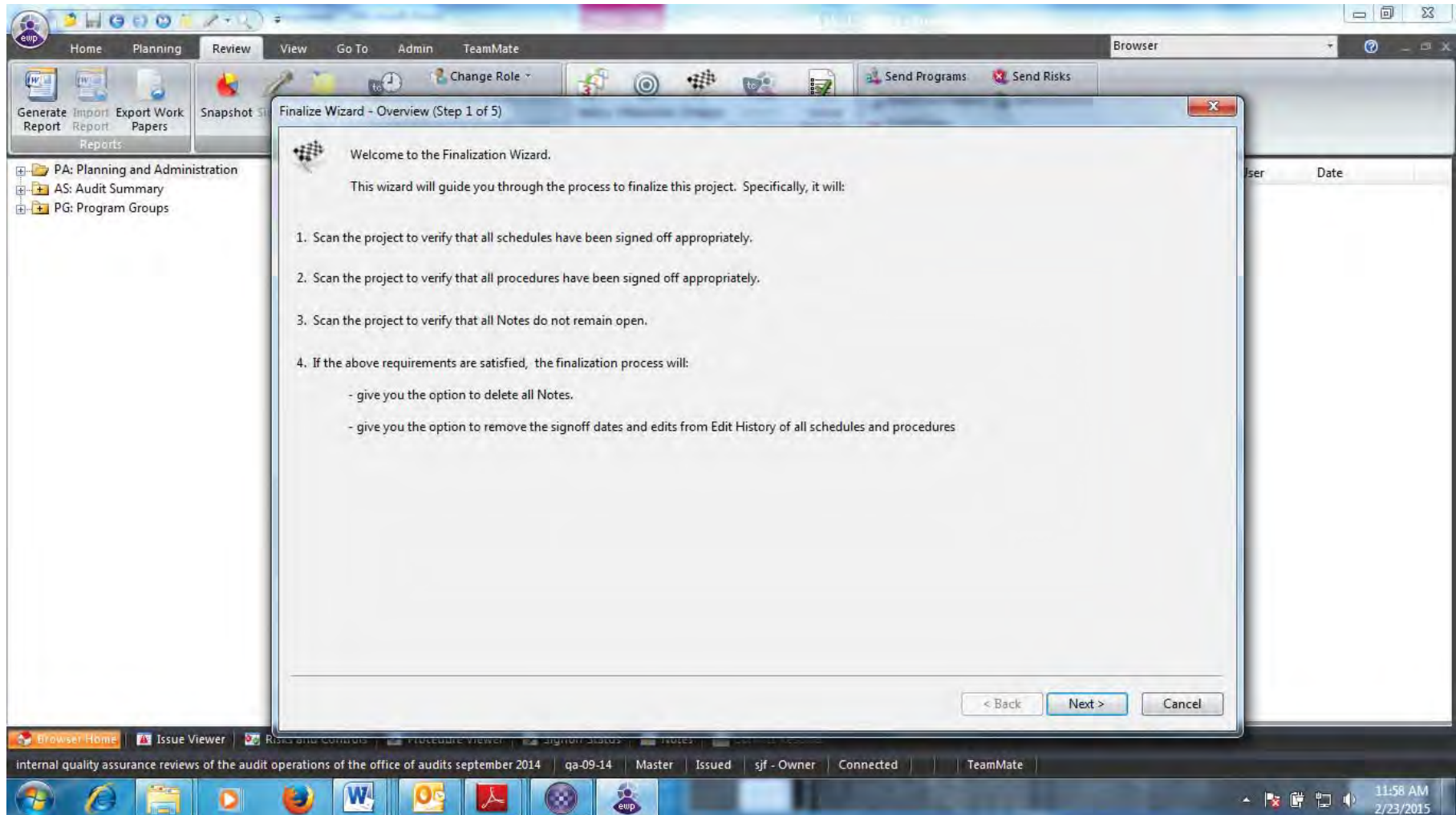
In "Status" Tab check the Issued (Final Report) box.

FINALIZATION



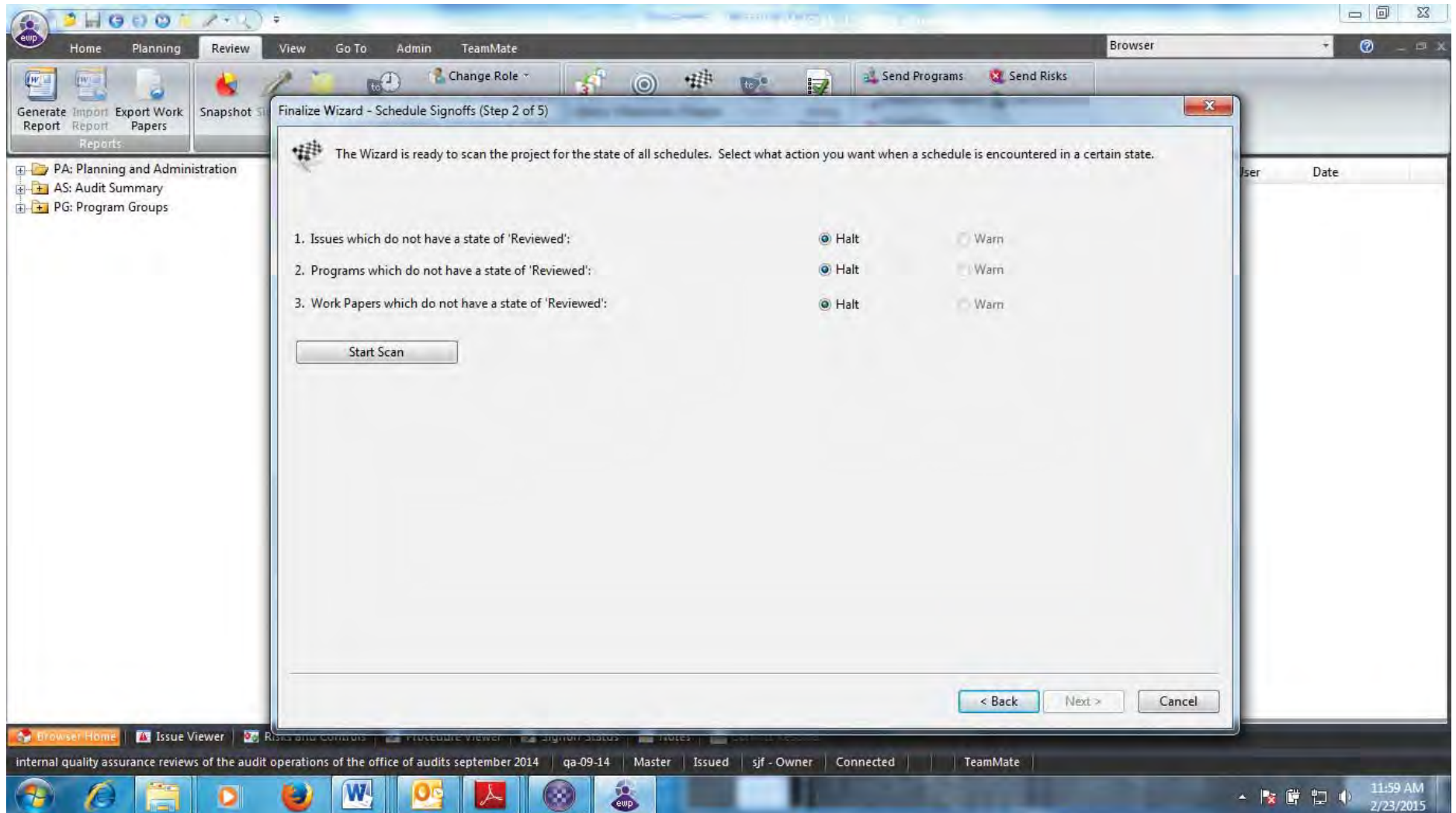
Go to Review Tab in TeamMate Browser and click on “Finalize” icon.

FINALIZATION



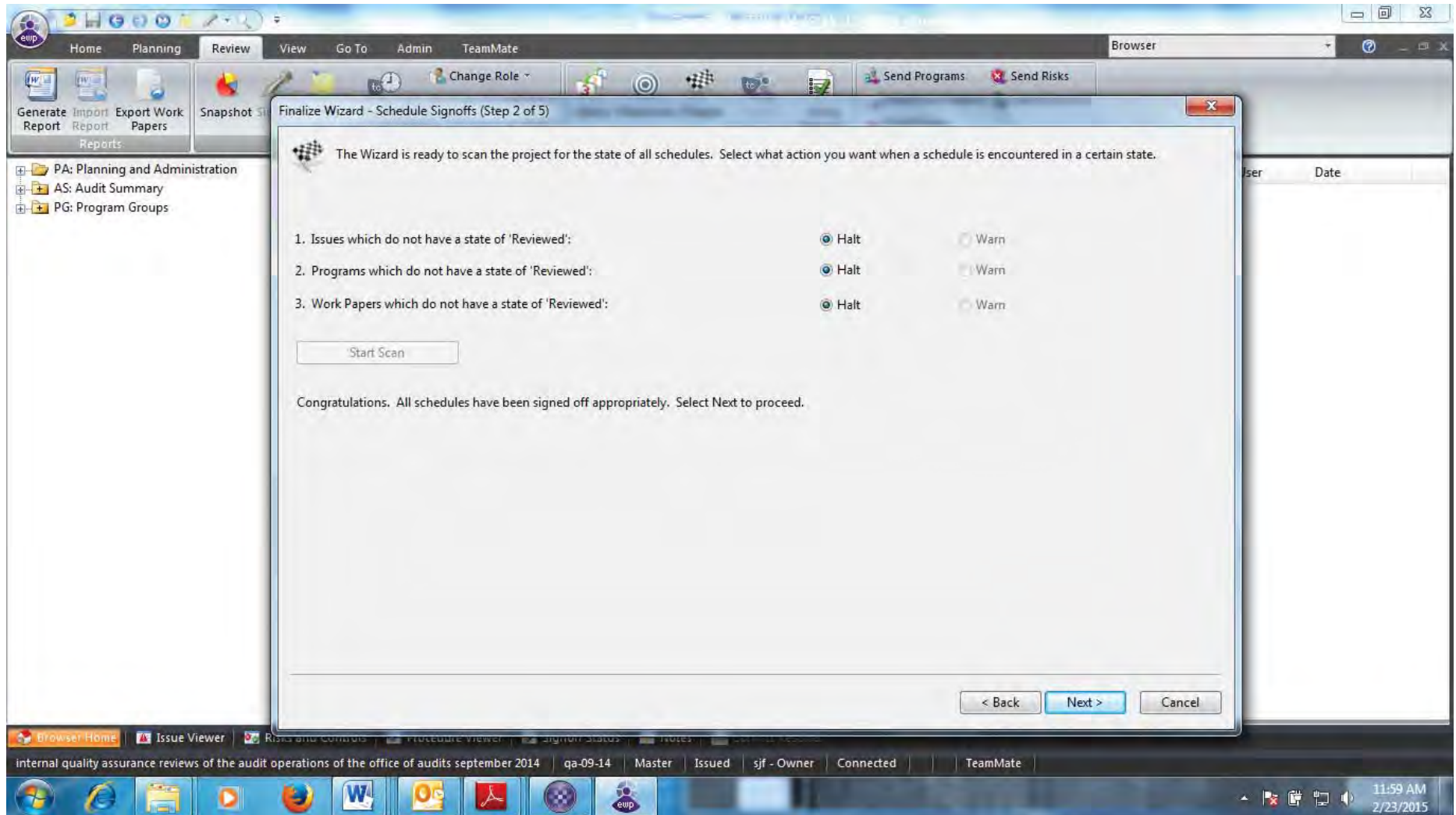
Click Next

FINALIZATION



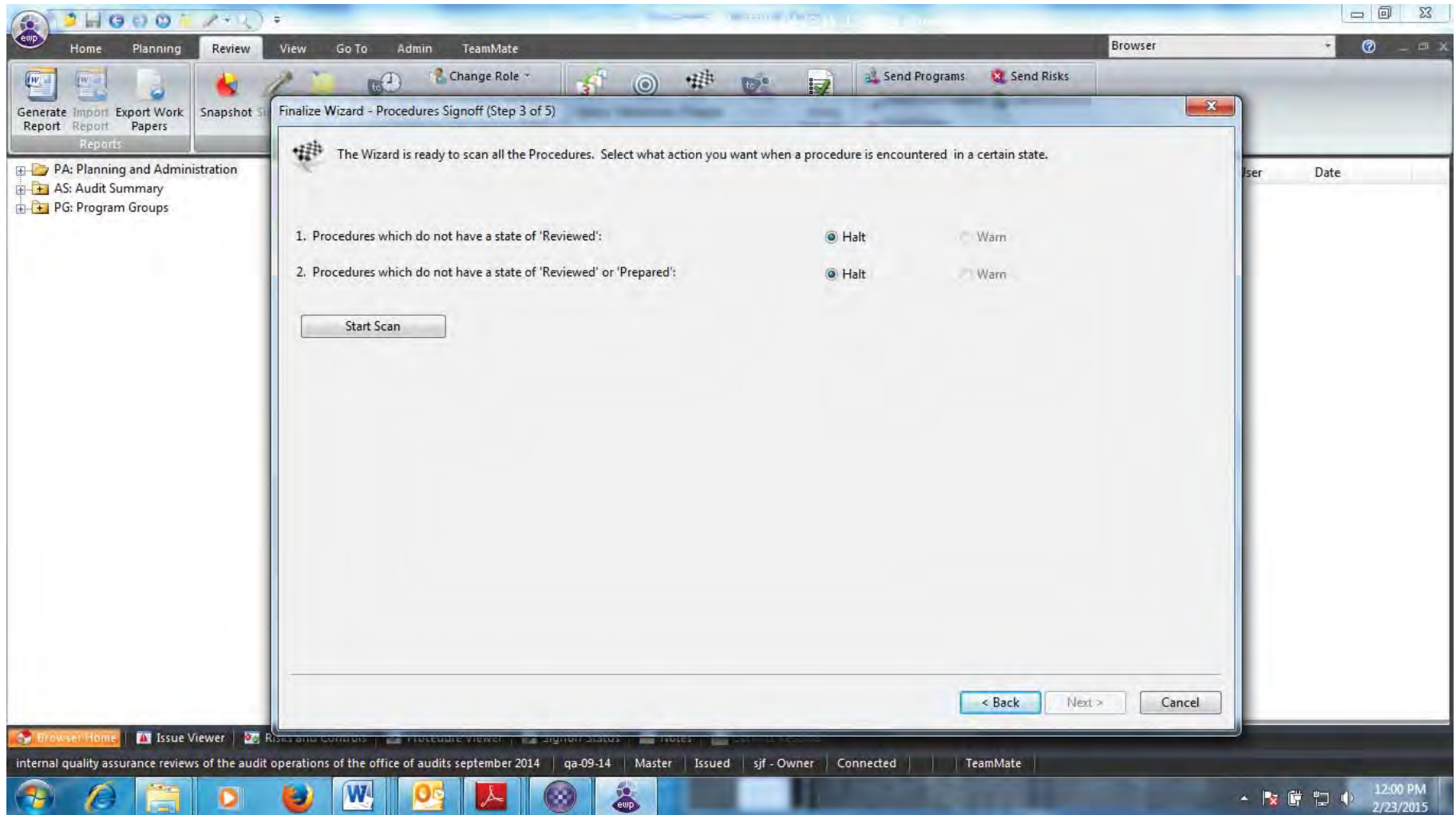
Click Start Scan

FINALIZATION



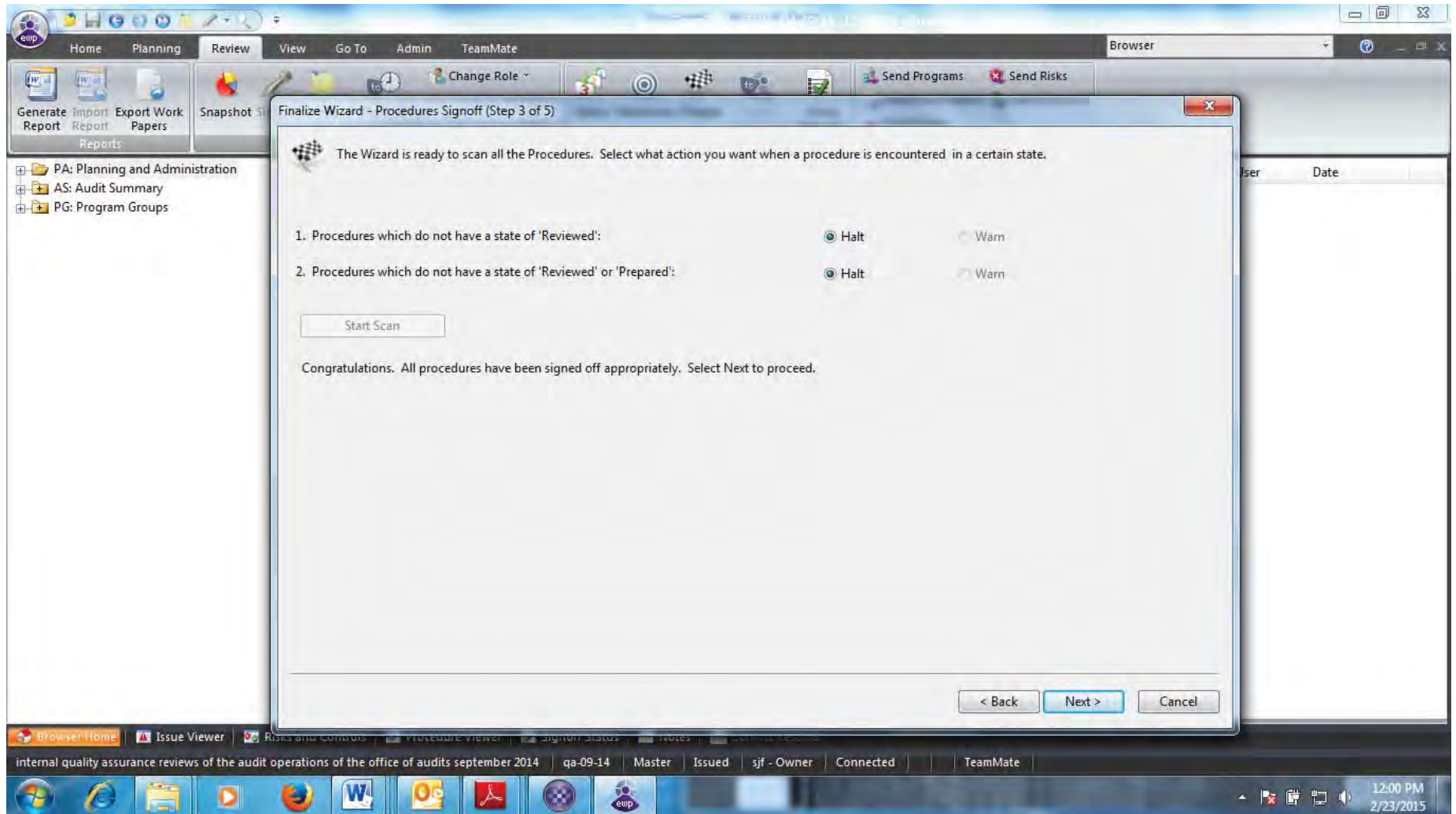
Click Next

FINALIZATION



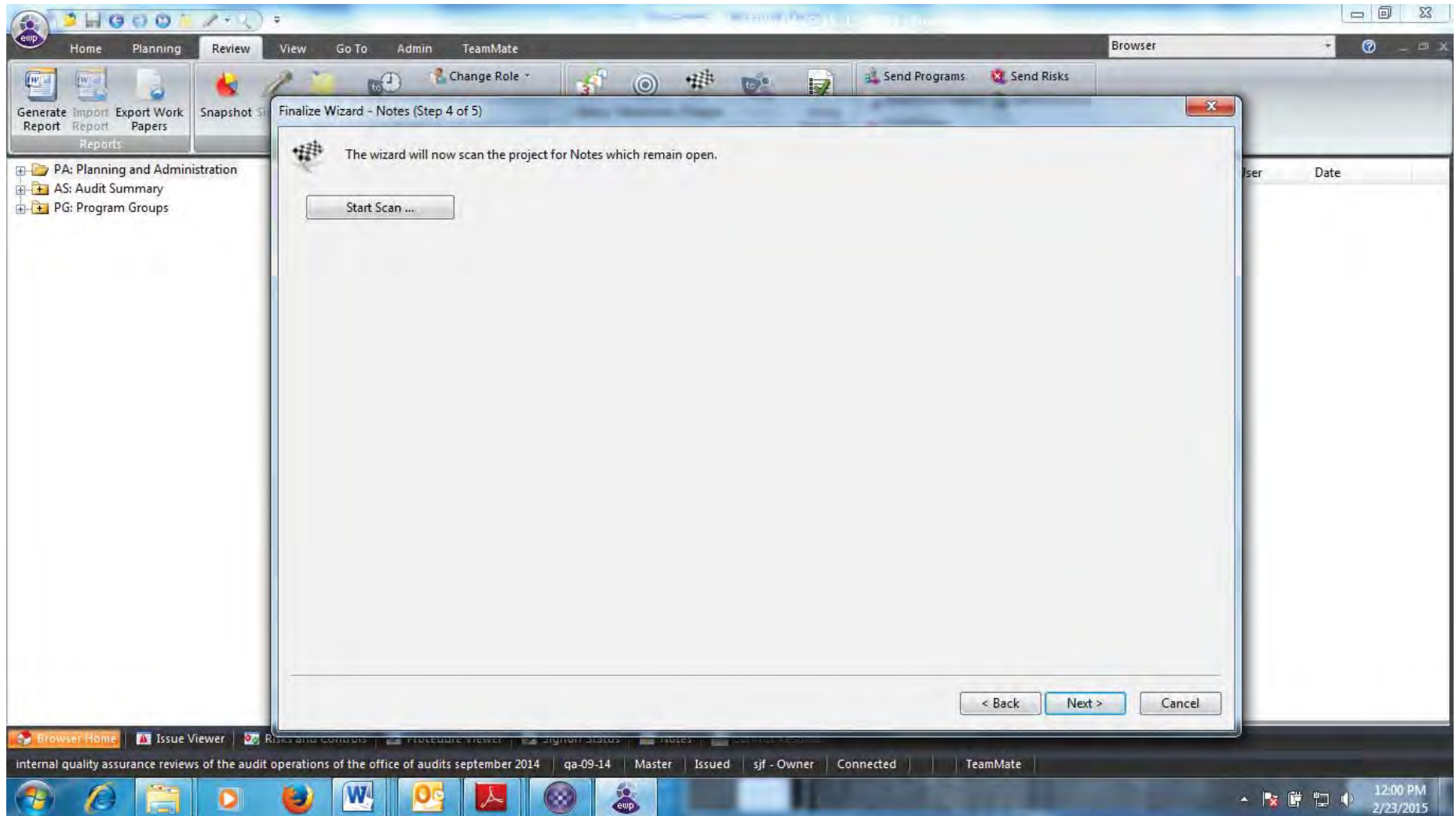
Click Start Scan

FINALIZATION



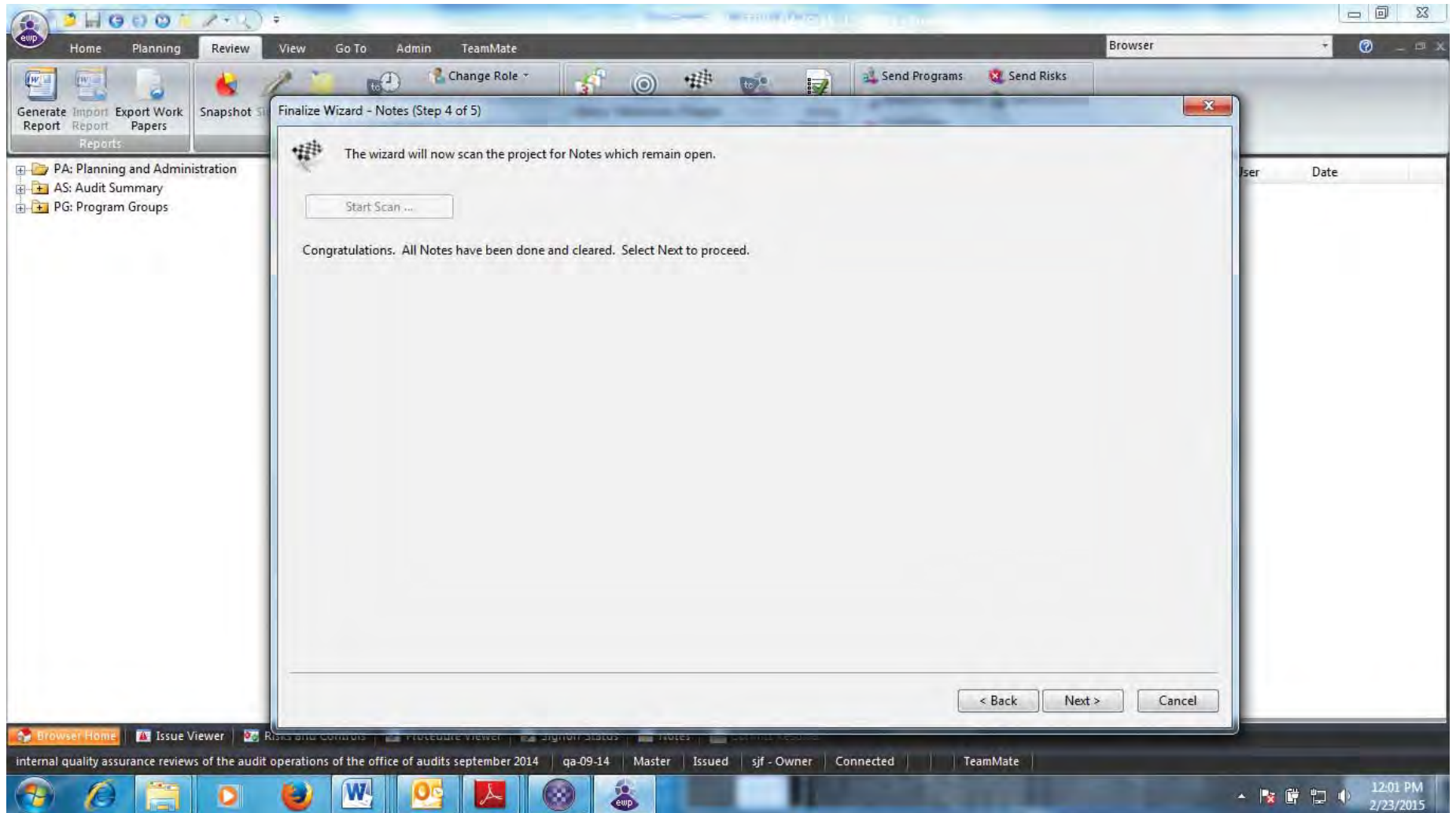
Click Next

FINALIZATION



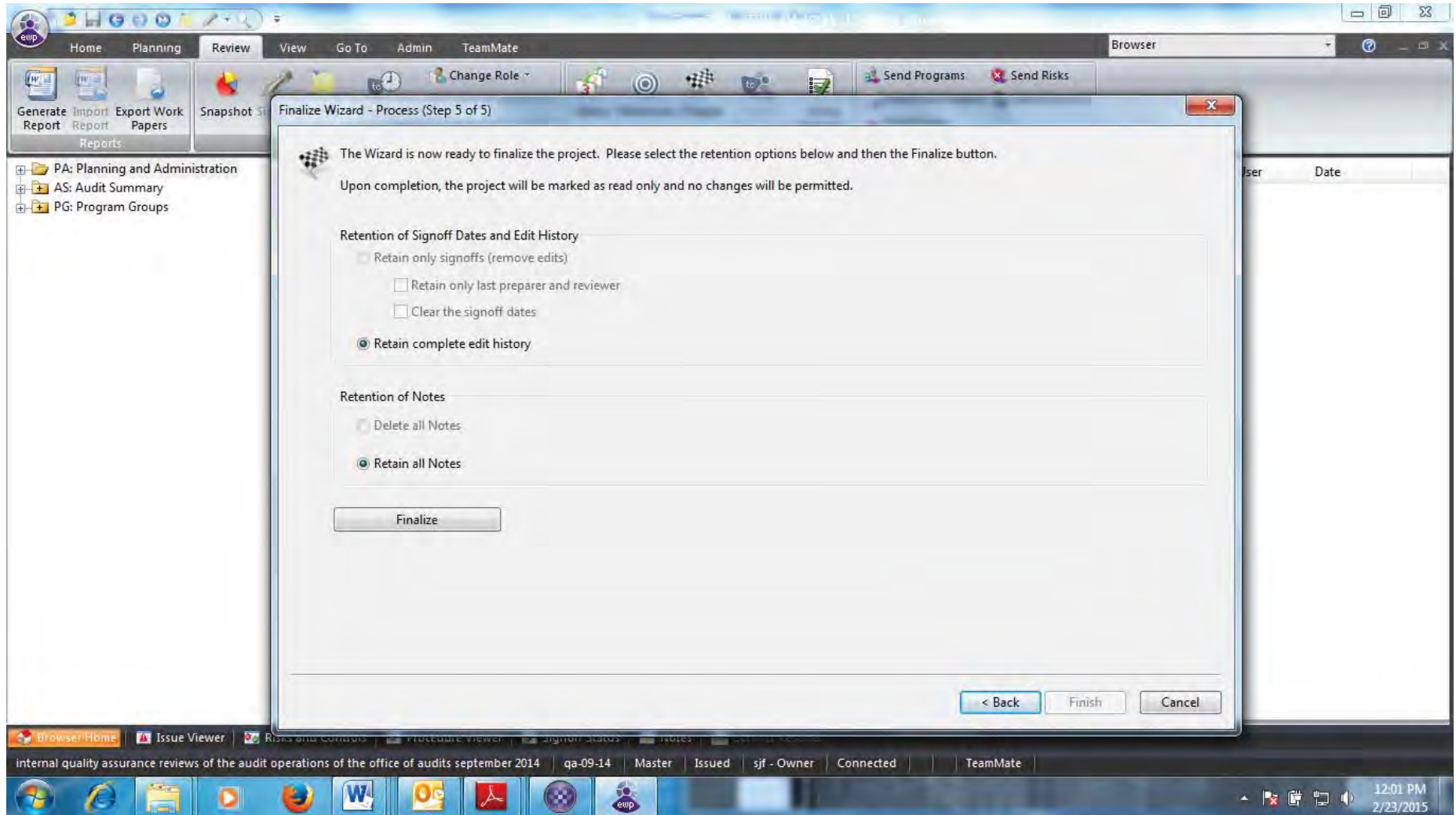
Click Start Scan

FINALIZATION



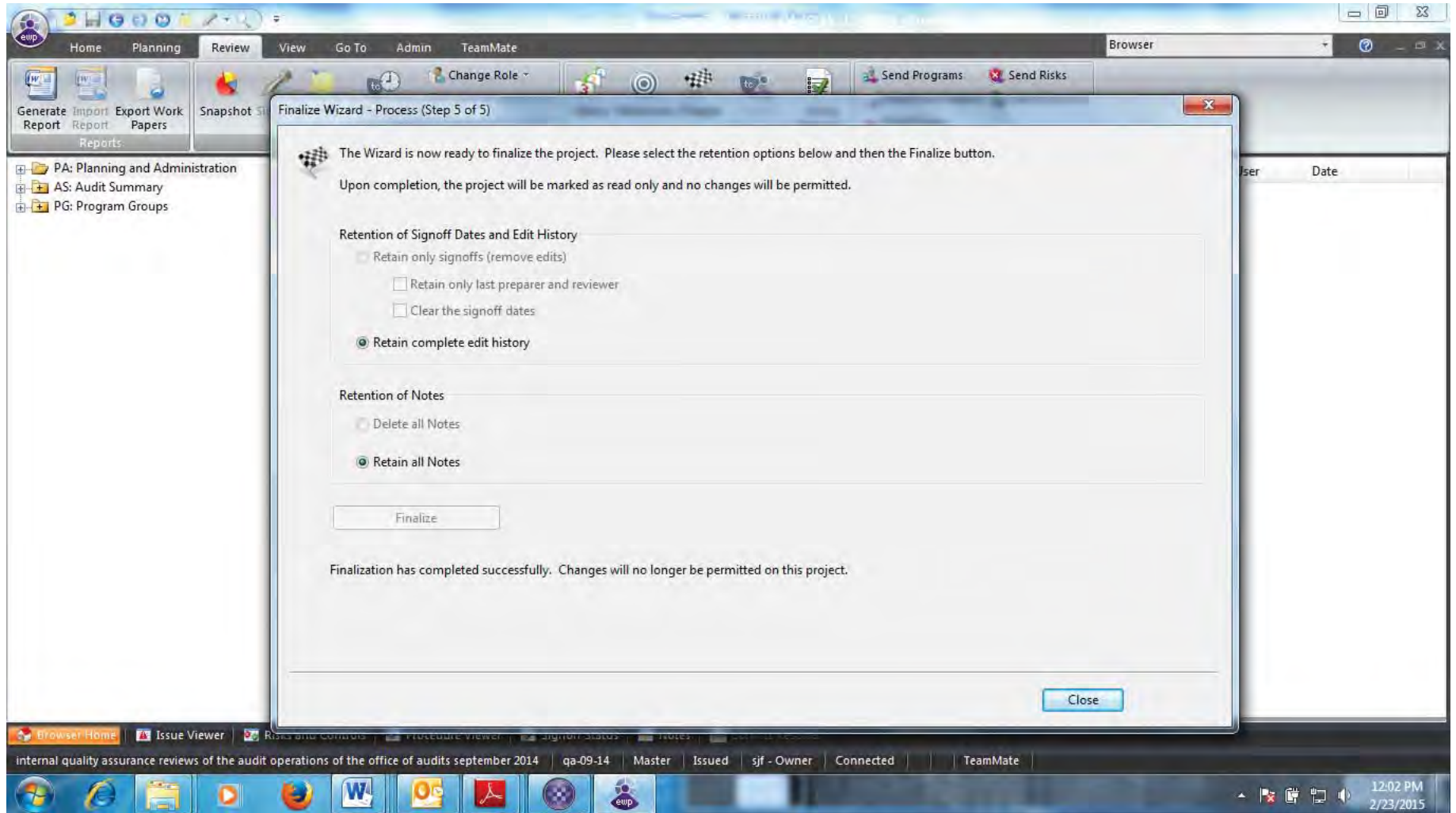
Click Next

FINALIZATION



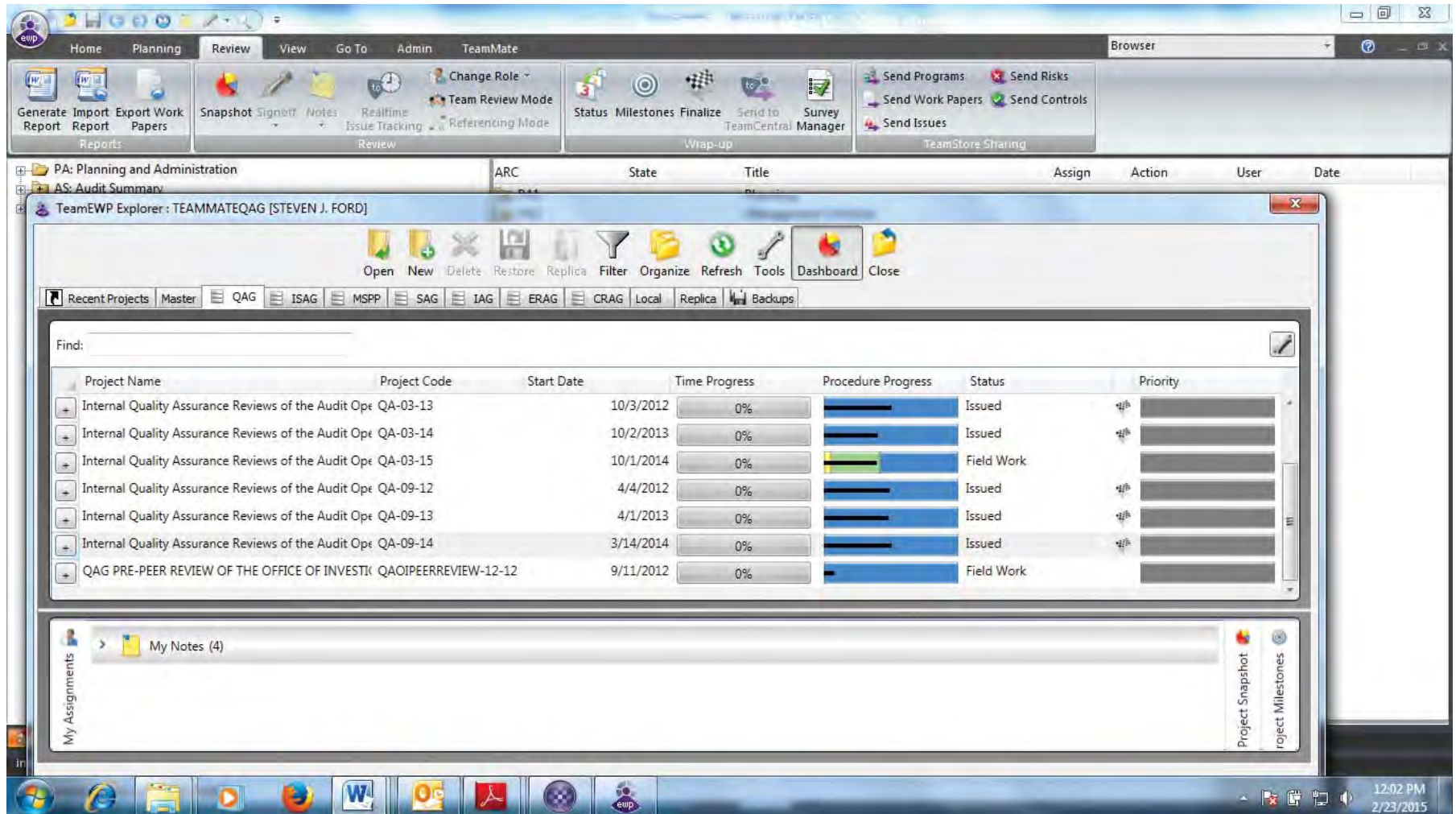
Make sure “Retain complete edit history” and “Retain all Notes” are checked and the click Finalize.

FINALIZATION



Click Close.

FINALIZATION



The project Status will show “Issued” and there will be a checkered flag next to the Status.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2230

Auditing Information Systems

CHAPTER 2230 - AUDITING INFORMATION SYSTEMSCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. BACKGROUND	
2-1. Background.....	2
2-2. Definitions.....	3
2-3. References.....	4
SECTION 3. STANDARDS AND PLANNING	
3-1. GAO Audit Standards and Guidelines.....	6
3-2. Policy.....	8
3-3. Reimbursement for IT Services.....	9
SECTION 4. REVIEW OF GENERAL AND APPLICATION CONTROLS	
4-1. General.....	10
4-2. Review of General Controls in Information Systems.....	10
4-3. Review of Application Controls in Information Systems.....	12
4-4. Testing for Data Reliability.....	13
SECTION 5. REVIEW OF INFORMATION SYSTEMS DESIGN AND DEVELOPMENT	
5-1. General.....	14
5-2. Guidelines.....	14
5-3. Risks Frequently Associated with Information Systems.....	15
5-4. Audit Objectives.....	15
5-5. Controls.....	16
5-6. Economy and Efficiency.....	16
5-7. Legal Requirements.....	17
5-8. Documentation.....	17
5-9. Audit Approaches.....	18

CHAPTER 2230 - AUDITING INFORMATION SYSTEMS

CONTENTS

	<u>Page</u>
SECTION 6. REVIEW OF COMPUTER SECURITY	
6-1. General.....	20
6-2. OMB Requirements.....	20
SECTION 7. ASSESSING THE RELIABILITY OF COMPUTER OUTPUT FROM INFORMATION SYSTEMS	
7-1. General.....	21
7-2. Reliability Assessments.....	21

CHAPTER 2230 - AUDITING INFORMATION SYSTEMSSECTION 1. GENERAL

- 1-1. PURPOSE. In conducting accounting, administration, and oversight and management activities, audit entities may use IT systems. This chapter provides OIG guidance for auditing information systems in operation or under development.
- 1-2. POLICY. When an audit objective involves information systems, the auditor will evaluate the computer system as a component of the internal control structure. When computer data are used as evidence, the auditor will establish the reliability of the data.

SECTION 2. BACKGROUND

- 2-1. BACKGROUND. Automated resources represent significant investments of time and money to support many information system requirements. Information systems are used to manage the organization's assets and information. If not properly controlled, they may be used to commit fraud or waste resources. The potential for misuse increases auditors' responsibilities to assist management by evaluating whether:
- a. The design and operation of information systems and their controls safeguard assets; minimize opportunities for misuse; and provide accurate, timely, and reliable information; and
 - b. automated resources are used efficiently, effectively, and economically.

Information systems impact an auditor's work in two ways. First, computer-processed data is frequently integral to an entity's processes. Secondly, the auditor may use computer generated data as audit evidence. Therefore, when audit objectives include reviewing the reliability of the data produced by the information system, it is essential that the auditor evaluate the data's relevancy as well as credibility.

There are two basic methods available to assess the reliability of computer-based data. The first method is called a "system review" and is normally performed by IT audit specialists and/or computer specialists. The review examines: (1) an information system's general and application controls, (2) tests whether the information controls are in compliance, and (3) tests the data produced by the system. The second method is known as the "limited review" and is targeted to particular data, requires less extensive understanding of general and application controls, and is designed for the use of general auditors and evaluators. The limited review examines selected pertinent controls in particular attention on the pertinent controls selected for examination. Pertinent controls should be of sufficient quantity and quality in order to render a professional conclusion on the reliability of data.

Auditing standards provide two alternatives for establishing the reliability of computer generated data: 1) performing a general and application review of the controls over the information systems, or 2) conducting other tests and procedures when general and application controls are not examined or are found unreliable.

This chapter deals with assessing the information systems as a component of the internal control structure and establishing the reliability of computer-generated data by performing a "limited approach" general and application review of the information systems.

2-2. DEFINITIONS.

- a. Information Technology (IT) Auditing. The IT audit focuses on auditing the computer systems as opposed to using the computer solely as an audit tool in selecting samples or analyzing data.

The IT audit may represent evaluations of a data processing installation's management; IT functional area; or new or substantially modified systems that are proposed, under design, in development, undergoing testing, or ready for implementation.

- b. Information System Controls. Policies and procedures that provide reasonable assurance that computer-based data are complete, valid, and reliable. They include both general and application controls.

- (1) General Controls. These controls include the structure, organization, methods, and procedures that apply to the overall computer operation. General controls include:

- (a) Security Management Controls – These controls provide the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. These controls include developing IT security policies and procedures, periodically assessing risk, establishing a security management structure, implementing effective security-related personnel policies, and monitoring the security program's effectiveness;
- (b) Access Controls – These are the logical controls that restrict and authorize users to only those applications or application functions pertinent to the performance of their assigned duties and responsibilities. Access controls also include the physical barriers designed to prevent individuals from gaining access to facilities containing sensitive data and computing resources;
- (c) Network Security Controls – These are the technical controls that are designed to keep a network environment secure from threats such as viruses, malware, and hacking;
- (d) Configuration Management – These controls regulate design, development, and implementation of computer applications and the operating platforms that support these applications. They also provide

appropriate controls of system changes;

- (e) Contingency Planning – These controls ensure an entity’s continued capability to process, retrieve, and protect information maintained electronically during disruptions; and
 - (f) Segregation of Duties – These controls ensure that one individual does not control all critical stages of a process.
- (2) Application Controls. These controls are designed to ensure the authority of data origination, accuracy of data input, integrity of processing, verification and distribution of output, integrity of data communication, and security of data storage. These controls apply on an individual basis and may vary among applications.
- c. Data Reliability. The state that exists when data is sufficiently complete and error free to be convincing for its intended objective.
 - d. Data Testing. Testing to determine if particular computer-generated data are valid and reliable. Data testing does not confirm the existence or adequacy of system controls or whether such controls are being complied with, but may disclose indications of control weaknesses.
 - e. Limited Review. A review that targets particular data and examines pertinent controls in order to determine the level of testing required to render a conclusion on the reliability of data. A limited review is designed for the use of general evaluators.
 - f. System Review. A review in which the objective is to assess and test all controls in a computer system for the full range of its application functions and products. A system review is generally performed by IT specialists and/or computer specialists.
- 2-3. REFERENCES. Auditors can consult the following references for additional information:
- a. U.S. General Accounting Office - Federal Information System Controls Audit Manual (FISCAM).
 - b. Federal Information Resources Management Regulation (FIRMR).
 - c. Federal Acquisition Regulation (FAR).

- d. System Development Auditor; published by Elsevier Advanced Technology.
- e. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.
- f. E-Government Act of 2002 (P.L. 107-347), Title III, “Federal Information Security Management Act of 2002.”
- g. The National Institute of Standards and Technology ‘800 Series’ of Special Publications.
- h. The Health Insurance Portability and Accountability Act of 1996 Security and Privacy Standards.

i. SECTION 3. STANDARDS AND PLANNING

3-1. GAO AUDIT STANDARDS AND GUIDELINES. The General Accounting Office (GAO) has published IT audit standards, guidelines, and procedures for auditing IT systems and using computer-assisted audit techniques.

a. The GAS standards state that for Information Systems Controls:

6.23 “Understanding information systems controls is important when information systems are used extensively throughout the program under audit and the fundamental business processes related to the audit objectives rely on information systems. Information systems controls consist of those internal controls that are dependent on information systems processing and include general controls, application controls, and user controls.

a. Information systems general controls (entitywide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity’s information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

b. Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls.

c. User controls are portions of controls that are performed by people interacting with information system controls. A user control is an information system control if its effectiveness depends on information systems processing or the reliability (accuracy, completeness, and validity) of information processed by information systems.

6.24 “An organization’s use of information systems controls may be extensive; however, auditors are primarily interested in those information systems controls that are significant to the audit objectives. Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of information systems controls in order to obtain

sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors should then evaluate the design and operating effectiveness of such controls. This evaluation would include other information systems controls that impact the effectiveness of the significant controls or the reliability of information used in performing the significant controls. Auditors should obtain a sufficient understanding of information systems controls necessary to assess audit risk and plan the audit within the context of the audit objectives.

- 6.25** “Audit procedures to evaluate the effectiveness of significant information systems controls include (1) gaining an understanding of the system as it relates to the information and (2) identifying and evaluating the general, application, and user controls that are critical to providing assurance over the reliability of the information required for the audit.
- 6.26** “The evaluation of information systems controls may be done in conjunction with the auditors' consideration of internal control within the context of the audit objectives, or as a separate audit objective or audit procedure, depending on the objectives of the audit. Depending on the significance of information systems controls to the audit objectives, the extent of audit procedures to obtain such an understanding may be limited or extensive. In addition, the nature and extent of audit risk related to information systems controls are affected by the nature of the hardware and software used, the configuration of the entity's systems and networks, and the entity's information systems strategy.
- 6.27** “Auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. The following factors may assist auditors in making this determination:
- a. The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
 - b. The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without evaluating the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls, there may not be sufficient

supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.

c. The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer-generated information, auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.

d. Evaluating the effectiveness of information systems controls as an audit objective: When evaluating the effectiveness of information systems controls is directly a part of an audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.” See Chapter 2210 (Audit Planning, Section 2-6, Preparing the Audit Program).

- b. When assessing the reliability of computer-processed data generated or provided by Plan officials or the audited entity, see Chapter 2210 (Audit Planning, Section 2-10, Evaluating Computer Processed Data).
- c. To guide auditors in evaluating the integrity, confidentiality, and availability of computerized data, assessing internal controls, and compliance with applicable laws and regulations, GAO published the Federal Information System Controls Audit Manual (FISCAM).
- d. IT audit standards are also included in the Government Audit Standards and OPM-OIG Audit Manual, Chapter 2210, Audit Planning.

3-2. POLICY. Auditors will include an appropriate examination of the IT system when necessary to meet audit objectives. OIG must design appropriate tests to evaluate whether these systems meet internal control and compliance requirements.

- a. To assess internal controls and compliance with applicable laws and regulations, auditors will:
 - (1) Review the system's general and application controls to determine the system's reliability and whether it operates in a manner which meets applicable laws, regulations, and contractual requirements; and

- (2) conduct appropriate tests to provide reasonable assurance that the data is valid and responsive to its use (relevant, accurate, and complete), and that confidential data is maintained in a secure manner.
 - b. The audit report will cite any scope limitations such as the inability to examine the entire system due to time; cost; or invalid or inaccurate data. See Section 7 of this Chapter, “Assessing Data Reliability,” and OPM, OIG Audit Manual Chapter 2400, “Audit Report Preparation, Review, and Standards,” for additional information. If the test results indicate that the data are unreliable, auditors will:
 - (1) Limit use of the data in the audit report and describe the limitation, including an explanation of the limitations, in the scope section of the report; and
 - (2) the audit finding will disclose the results of the reliability tests; show the significance of the questionable data by explaining the problems that management may encounter by using such data; recommend that management restrict use of the data in the decision making process until the problem areas are resolved; and, if applicable, recommend a separate review of the IT system.
 - c. Audit working papers will be prepared, indexed, and reviewed in the same manner as other working papers. See OIG Audit Manual Chapter 2220, “Audit Working Papers and Files,” for additional information.
- 3-3. REIMBURSEMENT FOR IT SERVICES. While auditors should not hesitate to use IT resources at the audit entity, OIG will generally not reimburse the audit entity for any IT costs incurred. Audit is an integral part of the entity's management control system and auditors' use of IT resources represents an appropriate cost. Auditors should **not sacrifice their independence** in conducting the audit when considering ways to minimize cost or adverse impact on audit entity operations. Auditors may consider including their IT requests during regular processing operations of the entity; being reasonable in asking for information; and not presenting any undue hardship on the entity to complete the request. To the extent possible, auditors will use OIG IT resources, including technical assistance and equipment.

SECTION 4. REVIEW OF GENERAL AND APPLICATION CONTROLS

- 4-1. GENERAL. In reviewing the general and application controls, auditors will consider the effectiveness of the general controls relevant to the application system being reviewed. General controls are applicable to all applications being processed within an installation. Application controls apply on an individual basis and may vary among applications.
- 4-2. REVIEW OF GENERAL CONTROLS IN INFORMATION SYSTEMS. General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. In reviewing the general controls, auditors will:
- a. Determine whether the controls have been designed to meet management requirements and applicable laws and regulations;
 - b. assess whether controls are operating effectively to provide reliable and secure data processing; and,
 - c. consider entity-wide security controls, access controls, application development and change controls, system software controls, and service continuity when conducting their reviews.
 - (1) Entity-wide Security Controls. An entity-wide security program establishes a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Auditors will determine whether the audited entity:
 - (a) periodically assesses risk;
 - (b) documents an entity-wide security program plan;
 - (c) establishes a security management structure and clearly assigns security responsibilities;
 - (d) implements effective security-related personnel policies; and
 - (e) monitors the security program's effectiveness and make changes as needed.
 - (2) Access Controls. These controls provide reasonable assurance that computer resources (data files, application programs, and computer-related facilities and

equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Auditors will determine whether the audited entity:

- (a) classifies information resources according to their criticality and sensitivity;
 - (b) maintains a current list of authorized users and their authorized access;
 - (c) establishes physical and logical controls to prevent or detect unauthorized access; and
 - (d) monitors access, investigates apparent security violations, and takes appropriate remedial action.
- (3) Network Security. These controls help ensure that the network environment supporting relevant information systems are protected from unauthorized access, misuse, modification, or denial of accessibility. Auditors will review procedures to determine if:
- (a) sensitive data is protected in electronic and physical form;
 - (b) network activity is logged and monitored; and
 - (c) boundaries between sensitive technical resources are defined and controlled.
- (4) Configuration Management. These controls regulate system design, development, and implementation of computer applications and the operating platforms that support these applications. They also provide appropriate controls of operating platform changes. Auditors will review procedures to determine if:
- (a) Processing features and program modifications are properly authorized;
 - (b) all new and revised software is tested and approved;
 - (c) software libraries are controlled to ensure that access to libraries is restricted and movement of programs and data among libraries is controlled;
 - (d) access to system software is limited;

- (e) access to and use of system software is monitored; and
 - (f) system software changes are controlled.
- (5) Segregation of Duties - These prevent one individual from controlling all critical stages of a process. Auditors will determine whether the audited entity:
- (a) segregates incompatible duties and establishes related policies;
 - (b) establishes access controls to enforce segregation of duties; and
 - (c) controls personnel activities through formal operating procedures and supervision and review.
- (6) Business Continuity – These controls ensure that in the event of an interruption, plans and procedures are in place to protect information resources and recover critical operations. Auditors will determine whether the audited entity:
- (a) assesses the criticality and sensitivity of computerized operations and identifies supporting resources;
 - (b) takes steps to prevent and minimize potential damage and interruption;
 - (c) develops and documents a comprehensive contingency plan; and
 - (d) periodically tests the contingency plan and adjusts it as appropriate.

4-3. REVIEW OF APPLICATION CONTROLS IN INFORMATION SYSTEMS.

Application controls are designed to ensure the authority of data origination, accuracy of data input, integrity of processing, and verification and distribution of output.

Auditors will review the application controls to assess their reliability to process only authorized data in a prompt, accurate, and complete manner and to evaluate whether they are properly authorized, tested before implementation, and protect the integrity of the application software. In order to verify that an entity's application controls are proper, auditors will review the following:

- a. Input Controls. To ensure that transactions are accepted by the computer and processed only once. The controls also ensure that errors are identified, segregated, corrected, and reprocessed.
 - b. Processing Controls. To ensure that authorized transactions are (1) accepted by the application system; (2) accurately processed with valid business rules; (3) processed completely and available for authorized users in accordance with business requirements; and (4) processed effectively and efficiently.
 - c. Output Controls. To ensure that output data is (1) complete and accurate; (2) reported in the correct manner; (3) viewable/available to authorized personnel only; (3) appropriately retained or destroyed; (4) subject to necessary processing of audit trails; and (5) if erroneous, segregated from valid records, corrected, and reprocessed by the computer.
- 4-4. TESTING FOR DATA RELIABILITY. To determine whether general and application controls are reliable, the auditor must determine the degree of testing necessary to draw appropriate conclusions. See Section 7, for additional information. Appropriate testing procedures include the following:
- a. Confirming computer-processed data with independent sources, such as third parties, and knowledgeable internal sources, such as regular users of the data and suppliers of data;
 - b. reviewing management test procedures and results, and processing test transactions through the application;
 - c. comparing the data with source documents, or physical counts and inspections; and
 - d. conducting appropriate tests to evaluate whether application controls provide reasonable assurance, not absolute assurance, that the identification of fraud or other irregularities in Information Systems Controls will be detected. Should fraud or other illegal acts be identified, auditors will contact the **Assistant Inspector General for Audit (AIGA)**. The **AIGA** and the **Assistant Inspector General for Investigations (AIGI)** will determine the appropriate actions to be taken by the auditors. The **AIGI** and **Special Counsel** will determine whether these acts may be disclosed in the audit report. See Chapter 2325, Fraud, Illegal Acts, and Abuse for additional information.

SECTION 5. REVIEW OF INFORMATION SYSTEMS DESIGN AND DEVELOPMENT

- 5-1. GENERAL. If management is to have reasonable assurance that auditable and properly controlled information systems are being developed, the auditor's role in evaluating the design and development of automated systems is crucial. Recommended improvements may be accomplished more easily, at considerably less cost and effort, before the system becomes operational. Audit objectives for reviewing system design, development, and modifications will be designed to provide auditors with reasonable assurance that automated systems and applications:
- a. Carry out the policies that management has prescribed;
 - b. provide the audit trails needed for management, auditor, and operational reviews;
 - c. include the controls necessary to protect against loss or serious error;
 - d. operate effectively, efficiently, and economically;
 - e. conform with legal requirements; and
 - f. contain documentation that provides an understanding of the system sufficient for system maintenance and auditing.

Auditors and management have an interest in ensuring that system design, development, and overall operations achieve the objectives of adequate internal controls, compliance with applicable laws and regulations, and the ability to be audited. Due to the integration of applications systems, such as payroll, personnel, and labor-cost-accounting, the outputs of one subsystem now may be the inputs for another without any human review. A control weakness in one subsystem may have completely unanticipated catastrophic effects on other subsystems. Such mistakes, waste, and confusion may adversely affect the entity's viability.

Interest in computer system design and development is ever-expanding. The growing number of telecommunications links and the wide variety of new input and output devices and processing devices create challenges for the audit. IT auditors are now required to perform a wide variety of tasks that at one time did not exist or were not considered part of their role.

- 5-2. GUIDELINES. Audits generally address the ability of systems to meet management policies and legal requirements, such as examining approvals, documentation, test results, and cost studies. Audits also determine whether the systems and/or applications have the

necessary controls and audit trails.

- a. At the completion of the design and development process and during the final system testing phase, the auditors will verify that the implemented system conforms with planned functional requirements.
- b. Depending on size and system complexity, the IT system development cycle may span several years from conception to implementation. Scarce audit resources and long project life-cycles require innovative audit approaches.
- c. Auditors may want to refer to the Federal Information Resources Management Regulation (FIRMR), Federal Acquisition Regulation (FAR), and applicable OPM Office of the Chief Information Officer (OCIO) policies and procedures for guidance on Federal and agency requirements for information resources acquisition, management, and administration. See Exhibit A, for additional information on auditor responsibilities and audit approaches.

5-3. RISKS FREQUENTLY ASSOCIATED WITH INFORMATION SYSTEMS.

Computer-based information systems may not:

- a. Possess the built-in controls necessary to ensure proper and efficient operation;
- b. provide the capability to track events through the system which can impede, if not completely frustrate, audit review of the system in operation; and
- c. comply with generally accepted accounting principles or other criteria (for financial systems), resulting in qualifications of the auditor's opinion on the financial statements or their related segments.

5-4. AUDIT OBJECTIVES. The auditor's objectives for the review of system design, development, and modifications include determining if:

- a. Internal control requirements are met;
- b. controls provide reasonable assurance that systems and/or applications meet management policies and requirements by:
 - (1) Verifying proper approval of the design and modification process and access to computer systems and applications; and

- (2) reporting when management's requirements, such as deadlines, are not being met and citing appropriate corrective actions.
 - c. systems and/or applications possess the controls and necessary audit trails for management, auditor, and operational review; and
 - d. if improvements are required, the auditor will recommend appropriate corrective actions. Automated systems will provide trails for transactions from their origin, through all intermediate processing steps, to the applicable management or financial statement or report and from the statement or report to the origin of the data. Auditors will verify data output reliability by tracing the transaction processing flow and its related manual and automated controls.
- 5-5. CONTROLS. Auditors will evaluate whether the information systems controls provide reasonable assurance that systems and/or applications include the controls necessary to protect against loss or serious error.
- a. The system design and development processes include defining the processing to be done by the computer, flowcharting the processing steps, determining the data input and files that will be required, and specifying each individual program's input data and output.
 - b. Good management practice dictates that each area will be controlled properly. The auditor will evaluate whether the controls provide reasonable assurance to management that the systems and/or applications, once placed in operation, will be protected against loss or serious error.
 - c. To make the system operational, management may bypass or override controls which are built into the system. Once the system is operational, these controls may not be reactivated.
 - d. To determine the adequacy of system controls, auditors must review both manual and IT controls for input origination and output disposition.
- 5-6. ECONOMY AND EFFICIENCY. Auditors will evaluate whether the controls provide reasonable assurance that an organization is managing and using its IT resources wisely; report any problems resulting from inadequate practices; and focus on whether IT systems conduct operations and produce required outputs accurately and at a minimum cost. During the early stages of system development, auditors should review the adequacy of:

- a. Mission needs and system objectives;
 - b. the technical requirements, technical analysis, and feasibility studies to determine if the proposed system meets its objectives; and
 - c. the cost-benefit analysis which identifies applicable costs and benefits to each alternative, including maintaining the present operating system.
- 5-7. LEGAL REQUIREMENTS. Auditors will determine whether systems and/or applications conform with legal requirements. Legal requirements applicable to systems and/or applications may originate from various sources.
- a. One such requirement is compliance with Federal privacy statutes that restrict collection and use of certain types of information about individuals. Safeguards obviously are necessary in such systems. Conversely, organizations subject to the Freedom of Information Act will have systems and/or applications designed so that applicable and timely responses may be made to legitimate requests.
 - b. Auditors should consider the applicability of the Federal Information Processing Standards (required by P.L. 89-306) to the system under audit.
 - c. Auditors will also review the Federal Information Resources Management Regulation (FIRMR), Federal Acquisition Regulation (FAR), Office of Management and Budget (OMB) Circulars (A-130 Federal Information Resources; A-127, Financial Management Systems; and A-123, Internal Control Systems), General Accounting Office (GAO) Title 2, and applicable OPM regulations, policies, and procedures.
- 5-8. DOCUMENTATION. Auditors will determine if documentation produced by IT systems and/or applications provide end users with an adequate understanding of the system to facilitate its proper maintenance and auditing. To evaluate the adequacy of this documentation, auditors will:
- a. Review the documentation produced by the systems which process programs and data files, prepare production reports, and provide computer operators and user groups with instructions which prepare and control data;
 - b. conduct adequate tests, including reviews of documentation produced; and
 - c. verify that the implemented system conforms with applicable requirements.

- 5-9. AUDIT APPROACHES. Life-cycle management (LCM) provides a structured approach to establishing and administering IT systems in an effective and efficient manner. Emphasis is placed on improving early decisions that affect the system's cost and utility through periodic milestone reviews and high level management participation.
- a. Since the system development cycle, from conception to implementation, may span several years, the LCM process establishes distinct IT system development phases.
 - (1) Depending on the management direction and IT system needs, the points of specific tasks may differ somewhat within or between LCM phases. To adequately consider these factors, a flexible audit approach is required to evaluate IT system development.
 - (2) IT system audits should consider the size and relative importance of the system. Based on these factors, auditors will determine the audit scope necessary to meet audit objectives.
 - b. In the traditional systems development approach, the following activities are performed:
 - (1) **Initiation.** The need for a computerized solution to a problem is identified and validated. The decision to pursue a solution must be based upon a clear understanding of the problem, a preliminary investigation of alternative solutions, and a comparison of the expected benefits versus costs. At this stage the risk/sensitivity of the data or information processed by the system should be evaluated. The objective of this phase is to look at alternate functional solutions to the user's need.
 - (2) **Requirements Definition.** The functional requirements are defined and detailed planning for the development of an operational system is begun. The needs from the Initiation Phase are translated into a computer solution. The users specify their information resource needs and how they wish to have them addressed by the system. From this interactive process, a general preliminary design of the system may be developed and presented to user management. A project schedule is created for developing, testing, and implementing the system. Auditors during this phase determine whether adequate security requirements have been defined to address the confidentiality, integrity, and availability requirements of the system.
 - (3) **System Design.** Detailed design specifications which describe the physical solution to the requirements are developed. The system design phase takes user

needs and requirements and converts them into specifications for a computerized system. A formal change control process is established to prevent uncontrolled entry of new requirements into the development process. Auditor's involvement is focused on whether an adequate system of information systems controls is incorporated into system specifications and test plans and whether continuous online auditing functions are built into the system. Also, the auditor is interested in evaluating the effectiveness of the design process.

- (4) Development. Detailed design is implemented into executable programming code, and the program is tested to verify and validate that the system performs the functions for which it has been designed. When testing is completed, the auditor should evaluate the system to determine if it has any deficiencies that need to be corrected before being placed into production.
- (5) Implementation. The actual operation of the new information system is established and tested. Final user acceptance testing is also conducted. After the system is accepted by users, it is placed into production. Following implementation of the system, it is beneficial for auditors independent of the system development process to perform a review to verify the control integrity of the system and the control aspects of the system development and implementation process.

SECTION 6. REVIEW OF COMPUTER SECURITY

- 6-1. GENERAL. The use of automated technology has increased with the significant cost reductions in powerful micro-computers, increased emphasis on use of off-the-shelf software to process data, and increased computer literacy of end-users. Adequate security over computer programs, data files, telecommunications networks, and input and output materials is essential.
- a. The risks associated with the protection of personnel, proprietary, and other sensitive data have increased.
 - b. Risks jeopardizing computer security and information privacy are many, including disaster; unauthorized access to commit acts such as theft, sabotage, or espionage; human errors; tampering with input, programs or data files for fraudulent purposes; and use of computer resources for personal gain.
- 6-2. OMB REQUIREMENTS. OMB Circular A-130, Management of Federal Information Resources, prescribe specific responsibilities for the administration and management of IT resources.
- a. OMB Circular A-130, Appendix III establishes a minimum set of controls to be included in Federal automated information systems security programs; assigns system security responsibilities; and clarifies the relationship between system security programs and internal control systems established in accordance with OMB Circular A-123, Internal Control Systems.
 - b. Federal agencies are required to conduct management reviews and recertifications of their computer security programs every 3 years. In conducting an OMB Circular A-123 vulnerability assessment, these reviews become part of the vulnerability assessment. When internal auditors conduct general and application control audits, these reviews may satisfy OMB Circular A-130 review requirements.

SECTION 7. ASSESSING THE RELIABILITY OF COMPUTER OUTPUT FROM
INFORMATION SYSTEMS

- 7-1. GENERAL. When reviewing information systems, auditors will test the reliability of the data produced since it may be inaccurate or incomplete. Computer:
- a. Files may be altered which may not be readily apparent when reviewing a computer product;
 - b. product reliability may be affected by lack of data processing controls in agency systems; and
 - c. products are produced by a technology in which continuous changes in equipment and techniques hinder long-term credibility of a system.
- 7-2. RELIABILITY ASSESSMENTS. The reliability of information systems products will be evaluated to determine the risks in using such products.
- a. Objective. The objective of a reliability assessment is to determine the degree of risk in using computer-processed data.
 - b. Procedures. Auditors will test the data for reliability to determine the degree of risk involved in using data that may be incomplete and/or inaccurate. If data accuracy is important, auditors will:
 - (1) Identify computer-processed data that will be used;
 - (2) document and determine data sources and data flows through the system;
 - (3) consult the GAO audit guide, Assessing the Reliability of Computer-Processed Data, to obtain additional guidance on audit work needed to test data reliability and satisfy data validation requirements; and
 - (4) conduct appropriate tests to support an opinion on the data reliability. These tests include:
 - (a) Questioning a sufficient number of principal users about the reliability of computer outputs;
 - (b) obtaining views from auditors who have made detailed reviews of the computer system during the system development phase;

- (c) comparing data with sources independent of the information system that generated the data;
 - (d) identifying problems from computer-generated edit reports; and
 - (e) reviewing computer data for obvious errors and reasonableness.
- (5) If the auditor is unable to examine or analyze the generated computer-processed information due to time or cost, or the information is not critical to the audit results, then citing the source of the information and stating that it was not verified will satisfy the accuracy and completeness of the reporting standards. The following is an example of a statement for the scope section of the audit report:

In conducting the audit we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Also see Chapter 2210 (Audit Planning, Section 2-6, Preparing the Audit Program).

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2315

Review of Internal Controls

CHAPTER 2315 – REVIEW OF INTERNAL CONTROLSCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
1-3. Guidance Affecting Internal Controls.....	1
SECTION 2. INTERNAL CONTROL REVIEW FOR FINANCIAL AUDITING	
2-1. General.....	4
2-2. Audit Strategy.....	4
2-3. Understanding the Internal Control Structure.....	5
2-4. Control Risk Assessment.....	8
2-5. Tests of Controls.....	9
2-6. Substantive Testing.....	10
2-7. Reporting on Internal Controls.....	10
SECTION 3. INTERNAL CONTROL REVIEW FOR PERFORMANCE AUDITING	
3-1. General.....	13
3-2. Understanding Internal Controls.....	14
3-3. Assessing Significance of Controls to Audit Objectives.....	15
3-4. Tests of Controls.....	15
3-5. Reporting.....	16
SECTION 4. VULNERABILITY ASSESSMENTS	
4-1. General.....	17
4-2. Assessment Review.....	17

CHAPTER 2315 – REVIEW OF INTERNAL CONTROLSSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides the objectives, standards, and techniques to be used by the OIG Office of Audits to review, assess, and evaluate a program's or activity's overall system of internal control.
- 1-2. POLICY. The OIG Office of Audits will review, assess, evaluate and report on internal controls in accordance with Government Auditing Standards (GAS). All audit work performed for the internal control review will be recorded in the audit documents.
- 1-3. GUIDANCE AFFECTING INTERNAL CONTROLS. The auditor should become familiar with pertinent laws, regulations, and guidance that have been issued concerning internal controls. See Chapter 2005 (Audit Reference Materials) for additional information.
- a. Government Auditing Standards by the Comptroller General of the United States, December 2011. Establishes standards for conducting financial, performance audits, and attestation engagements including reviewing and assessing the internal control system. <http://www.gao.gov/govaud/ybk01.htm>
 - b. Public Law 97-255, The Federal Managers' Financial Integrity Act (FMFIA) of 1982, September 8, 1982. Amends the Budget and Accounting Procedures Act of 1950. Requires GAO to issue standards for internal control in government. The standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse and mismanagement. <http://www.whitehouse.gov/omb/financial/fmfia1982.html>
 - c. Public Law 101-576, The Chief Financial Officers Act of 1990, November 15, 1990. Requires the Inspectors General to audit the agencies' financial statements in accordance with generally accepted government auditing standards. Also requires financial management systems to comply with the internal control standards. <http://govinfo.library.unt.edu/npr/library/misc/cfo.html>

- d. Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control, Revised June 1995. This Circular replaces Circular No. A-123, "Internal Control Systems", revised, dated August 4, 1986, and OMB's 1982 "Internal Controls Guidelines" and associated "Questions and Answers" document, which are hereby rescinded. This Circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.
<http://www.whitehouse.gov/omb/circulars/a123/a123.html>
- e. Government Accounting Office (GAO), Standards for Internal Control in the Federal Government, (GAO/AIMO-00-21.3.1, November 1999). Provides standards for internal control in the Federal Government. Gives greater recognition to increasing use of information technology to carry out critical government operations, recognizes the importance of human capital, and incorporates, as appropriate, the relevant updated internal control guidance developed in the private sector. These standards are effective beginning with FY 2000 and the FMFIA reports covering that year. These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas at greatest risk for fraud, waste, abuse, and mismanagement.
<http://www.gao.gov/special.pubs/ai00021p.pdf>
- f. GAO, Internal Control Management Evaluation Tool, (GAO-01-1008G, August 2001). This management and evaluation tool, which is based upon GAO's *Standards for Internal Control in the Federal Government*, is used to assist agencies in maintaining or implementing effective internal control and, when needed, to help determine what, where, and how improvements can be implemented. Although this tool is not required to be used, it is intended to provide a systematic, organized, and structured approach to assessing the internal control structure.
<http://www.gao.gov/products/GAO-01-1008g>
- g. GAO, Auditing and Investigating the Internal Controls of Government Purchase Card Programs, (GAO-04-678G, November 2003). This guide focuses on audits of internal control activities - designed primarily to prevent or detect significant fraudulent, improper, and abusive purchases in a government purchase card program.
<http://www.gao.gov/products/GAO-04-87G>
- h. OMB Circular No. A-127, Financial Management Systems, Revised to include June 10, 1999 Transmittal Memorandum. This transmittal memorandum revises Circular No. A-127, "Financial Management Systems", dated July 23, 1993, by revising Sections 8d and 9b. It also will add new Sections 9a (3) and 9c. These changes are being made to reflect recommendations from the Chief Financial Officers (CFO) Council. These recommendations change the process for acquiring software to meet

core financial system requirements by eliminating the restriction to only acquire the software and related services from the FMSS Schedule, and to provide for software testing that is independent of the procurement process. These updates will become effective on September 12, 1999.

<http://www.whitehouse.gov/omb/fedreg/a127final.html>

- i. OMB Circular No. A-130, Management of Federal Information Resources, Revised to include November 30, 2000 Transmittal Memorandum No. 4. Requires agencies to establish systems of management controls for each major information system and provide for periodic review of those requirements over the life of the system in order to determine whether the requirements continue to exist and the system continues to meet the purpose for which it was developed.
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>
- j. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. Internal control is a process, effected by an audited entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
 - Effectiveness and efficiency of operations.
 - Reliability of financial reporting.
 - Compliance with applicable laws and regulations.

SECTION 2. INTERNAL CONTROL REVIEW FOR FINANCIAL AUDITING

- 2-1. GENERAL. GAGAS incorporate the AICPA generally accepted field work standards for audits and the related AICPA Statements on Auditing Standards (SAS). The AICPA generally accepted field work standards for financial audits requires a sufficient understanding of internal control¹ structure to plan the audit and to determine the nature, timing, and extent of tests to be performed. The auditor should summarize and document this understanding in the audit documentation.
- a. An audited entity's internal control structure consists of the policies and procedures that pertain to the audited entity's ability to record, process, summarize, and report financial data consistent with management's assertions embodied in the financial statements and related data.
 - b. The assertions are managements' representations that embody the account balance, transaction class, and disclosure components of financial statements. This includes:
 - (1) Existence or Occurrence. Management asserts that reported assets and liabilities actually exist as represented on the balance sheet and transactions reported on the income statement actually occurred during the period covered.
 - (2) Completeness. Management asserts that all transactions and accounts that should be included in the financial statements are included.
 - (3) Rights and Obligations. Management asserts that the organization owns and has clear title to assets and that liabilities are obligations of the organizations.
 - (4) Valuations or Allocation. Management asserts that assets and liabilities are valued properly and that revenues and expenses are measured properly.
 - (5) Presentation and Disclosure. Management asserts that the assets, liabilities, revenues, and expenses are properly classified, described, and disclosed in the financial statements.
- 2-2. AUDIT STRATEGY. The auditor should develop an audit strategy on how to obtain an understanding of the audited entity's internal control structure. This strategy should be

¹ The AICPA standards incorporate the concepts contained in "Internal Control – Integrated Framework", published by the Committee of Sponsoring Organization (COSO) of the Treadway Commission. Internal control consists of five interrelated components, which are (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The objectives of internal control relate to (1) financial reporting, (2) operations, and (3) compliance. Safeguarding of assets is a subset of these objectives. In that respect, internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of assets.

used as the basis for preparing the audit planning document and the audit program. See Chapter 2210 (Audit Planning).

- a. In developing the audit strategy, the auditor should consider:
 - (1) The degree of knowledge necessary to understand the audited entity's internal control structure; and
 - (2) the tests of the internal controls that should be performed to obtain this understanding.
- b. The specific steps the auditor should perform to develop the audit strategy include:
 - (1) Identifying the audited entity's internal control structure policies and procedures for preventing and detecting material misstatements in the financial statements;
 - (2) performing cursory tests of specific policies and procedures to determine whether they are operational; and
 - (3) assessing the relative strengths and weaknesses of the audited entity's internal control structure.
- c. Per GAGAS, auditors should specifically address their planned work and reporting related to testing internal control over financial reporting. During the planning stages of an audit, auditors should communicate their responsibilities for testing and reporting on internal control over financial reporting. Such communication should include the nature of any additional testing of internal control or otherwise requested, and whether the auditors are planning on providing opinions on internal control over financial reporting.

2-3. UNDERSTANDING THE INTERNAL CONTROL STRUCTURE. Following the development of the audit strategy, the auditor should proceed to obtain a detailed understanding of the audited entity's internal control structure.

- a. This level of understanding should assist the auditor in:
 - (1) Designing an effective audit plan and program including specific audit steps to be used to achieve the objectives of the audit;
 - (2) identifying the types of potential financial statement misstatement which affect the design of the audit steps and substantive tests; and
 - (3) formulating the cause of any potential findings.

- b. To obtain this detailed level of understanding, the auditor should depend upon prior audit experience with the audited entity and knowledge of and familiarity with the complexity, size, and sophistication of the audited entity's operations, activities, and programs.
- c. The auditor should also gain an understanding of the three elements comprising the audited entity's internal control structure, as well as how the elements relate to each other and to the audited entity as a whole.
 - (1) Control Environment. This is the audited entity's collective efforts to establish or enhance specific control policies and procedures. The control environment consists of:
 - (a) Management philosophy and operating style. This area encompasses a broad range of characteristics that include management's approach to taking and monitoring business risks; management's attitudes and actions toward financial reporting; and management's emphasis on meeting budget, profit, and other financial and operating goals.
 - (b) Organizational structure. This is management's overall framework for planning, directing, and controlling its operations. This includes consideration of the form and nature of operational units, related management functions, and reporting relationships.
 - (c) Methods of defining and/or communicating authority and responsibility. The methods that management uses to affect the understanding of authority and responsibilities established within the organization, i.e., mission statements.
 - (d) Management control objectives. The specific objectives set by management that are designed to implement the internal control structure:
 - 1) Transactions are executed in accordance with management's general or specific authorization;
 - 2) transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and to maintain accountability for assets;
 - 3) access to assets is permitted only in accordance with management's authorization; and

- 4) recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any difference.
 - (e) External influences. The reviews, follow up, and influences established and exercised by parties or conditions outside an organization that affect the audited entity's operations, practices, laws, regulations, physical environment, etc.
 - (2) Accounting System. This is the audited entity's methods and records used to identify, assemble, analyze, classify, record, and report transactions and maintain accountability for assets, liabilities and fund balances.
 - (3) Control Procedures. These are the audited entity's policies and practices which, in addition to the control environment and accounting system, provide management with reasonable assurance that the specific organization objectives will be achieved.
- d. The auditor should use the following steps as a guide to obtain a detailed understanding of the audited entity's internal control structure.
- (1) Review organizational flow charts, audit or regulatory reports and other independent evaluations, mission statements, etc.;
 - (2) review the audited entity's documented policies, procedures, systems manual, desk guides, etc.;
 - (3) review the audited entity's documentation that supports compliance with OMB Circular A-123. This includes internal control reviews, vulnerability assessments, and other self evaluations;
 - (4) review the organization and classification of transactions which affect the financial statement and the account processes from initiation of those transactions to the financial statement preparation;
 - (5) review the organization's authorization of transactions, separation of duties, record keeping documents, security over assets and liabilities, and independent checks;
 - (6) review the control procedures by comparing and analyzing data produced relative to applicable policies and procedures, reviewing computer general controls, and asking personnel about follow-up activities on deviation or error listings;

- (7) interview management officials and observe employees conducting specific functions; and
- (8) if the control environment and accounting systems of the internal control structure are automated, the auditor should test the computer generated controls to ensure proper design and function. See Chapter 2230 (Auditing Computer-Based Systems).

2-4. CONTROL RISK ASSESSMENT. After obtaining a sufficient understanding of the audited entity's internal control structure, the auditor should assess the level of control risk in auditing the audited entity's financial statements and related data. The control risk is the risk caused by weak internal control structure policies and procedures which will not prevent or detect an error on a timely basis.

- a. The ultimate purpose of assessing control risk is to determine whether the financial statements are susceptible to material misstatements. In addition, the process of assessing control risk provides evidential matter for the auditor to use as part of the reasonable basis for an opinion on the financial statements.
- b. In assessing the level of control risk, the auditor should consider:
 - (1) The relevant assertions related to each of the significant account balances and transaction classes. However, the control risk of misstatement may not be significant for each account balance and the auditor should not review every account balance or transaction class; and
 - (2) whether the control risk should be set below or at the maximum level.
 - (a) Setting the level of control risk at maximum level means the auditor believes that the internal control structure policies and procedures are unlikely to pertain to the financial statement assertion, be effective, or that evaluating their effectiveness would be inefficient.
 - (b) Setting the level of control at below the maximum level means the auditor believes the internal controls structure is effective in preventing or detecting material misstatements in the financial statements assertions.
 - (c) In order to assess the control risk at below the maximum level, the auditor must identify the specific internal control structure policies and procedures relevant to the specific assertions that are likely to prevent or detect material misstatements in those assertions and perform tests of controls to evaluate the effectiveness of such policies and procedures.

- 2-5. TESTS OF CONTROLS. During the development of the audit strategy or in conjunction with the control risk assessment, the auditor should test the effectiveness of the design or operation of the internal control structure's policy or procedure in preventing or detecting material misstatements in a financial statement assertion.
- a. The tests of controls ordinarily include procedures such as observing the application of various policies or procedures, interviewing appropriate organization personnel, and inspecting documents and reports showing the performance of the policy or procedure. This process is similar to testing performed during the OIG field work phase. See Chapter 2215 (Managing the Audit).
 - b. In some circumstances, a specific procedure may address the effectiveness of both design and operation. However, a combination of procedures may be necessary to evaluate the effectiveness of the design or operation of an internal control structure policy or procedures.
 - c. The nature, extent, and timing of these tests of controls depend upon the evidential material which exists within the organization and the audit period to which it applies.
 - (1) In testing the operations of policies or procedures, the auditor should be concerned with how the policy or procedures were applied and the consistency of this application.
 - (2) The auditor can also evaluate whether the policy or procedure is suitably designed to prevent or detect a material misstatement in specific financial statement assertions.
 - d. The auditor should, if applicable, revise any preliminary assessment of the internal control structure developed during the audit strategy process to reflect the results from the test of controls and control risk assessment.
 - e. Auditors need to be sensitive to the concerns of officials regarding previously reported internal control deficiencies of the audited entity and, accordingly, may need to test the effectiveness of internal controls that have been changed in response to reported deficiencies even if auditors do not plan to rely on the effectiveness of such internal controls.
 - f. GAGAS states that tests of internal control over financial reporting in a financial statement audit contribute to the evidence supporting the auditors' opinion on the financial statements or other conclusions regarding financial data. However, such tests generally are not sufficient in scope to provide an opinion on internal control over financial reporting. To meet certain audit report users' needs, laws and regulations sometimes prescribe testing and reporting on internal control over financial reporting to supplement coverage of these areas. Even after

auditors perform and report the results of additional tests of internal control over financial reporting, some reasonable needs of officials of the audited entity or individuals contracting for or requesting the audit still may be unmet. Auditors may meet these needs by performing further tests of internal control using the AICPA Statement on Standards for Attestation Engagements (SSAE) and additional GAGAS requirements, or the performance audit standards, to achieve these objectives.

- 2-6. SUBSTANTIVE TESTING. The objective of substantive tests is to detect material misstatement in the financial statements.
- a. When the auditor completes the control risk assessment and tests of controls, the results should be used to determine an acceptable level of detection risk for financial statement assertions. Detection risk is the risk that the audit procedures will not detect an error. The risk assessment is the basis for planning the nature, extent, and timing of substantive testing for significant account balances and transaction classes.
 - b. The auditor should design substantive testing to provide reasonable assurance that the controls are operational. In addition, the substantive tests that the auditor performs should consist of tests of details of transactions and balances and analytical procedures to detect material misstatements in the account balance, transaction class, and disclosure components of financial statements.
- 2-7. REPORTING ON INTERNAL CONTROLS. The GAGAS provides standards for reporting on internal controls and reporting any deficiencies in internal controls for financial audits.
- a. Reporting on Internal Controls – The auditor should reflect in the audit report the scope of assessment work and any significant weaknesses found during the audit. See Chapter 2400 (Audit Report Preparation and Standards).
 - (1) When providing an opinion or a disclaimer on financial statements, auditors must also report on internal control over financial reporting.
 - (2) Auditors should include either in the same or in separate report(s) a description of the scope of the auditors' testing of internal control over financial reporting and compliance with laws, regulations, and other compliance requirements. If the auditors issue separate reports, they should include a reference to the separate reports in the report on financial statements. Auditors should state in the reports whether the tests they performed provided sufficient, appropriate evidence to support an opinion on the effectiveness of internal control over financial reporting and on compliance with laws and regulations. The internal control reporting standard under GAGAS differs from the objective of an examination of internal control in accordance with the AICPA SSAE, which is to express

an opinion on the design or the design and operating effectiveness of an entity's internal control, as applicable. To form a basis for expressing such an opinion, the auditor must plan and perform the examination to obtain reasonable assurance about whether the entity maintained, in all material respects, effective internal control as of a point in time or for a specified period of time.

- (3) When auditors report separately (including separate reports bound in the same document) on internal control over financial reporting and compliance with laws and regulations, they should state in the financial statement audit report that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports on internal control over financial reporting and compliance with laws and regulations and provisions of contracts or grant agreements are an integral part of a GAGAS audit and important for assessing the results of the audit. If auditors issued or intend to issue a management letter, they should refer to that management letter in the reports.
- b. Reporting Deficiencies in Internal Controls – For further guidance see Chapter 2400 (Audit Report Preparation and Standards).
- (1) For financial audits, including audits of financial statements in which the auditor provides an opinion or disclaimer, auditors should report, as applicable to the objectives of the audit and based upon the audit work performed, significant deficiencies in internal control, identifying those considered to be material weaknesses.
 - (2) For all financial audits, auditors should report the following deficiencies in internal control (Definitions of Internal Control Deficiencies – Consistent with SAS No. 112):
 - (a) Significant deficiency: a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with GAAP such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.
 - (b) Material weakness: a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.
 - (3) Auditors should include all significant deficiencies in the auditors' report on internal control over financial reporting and indicate those that

represent material weaknesses. If (1) a significant deficiency is remediated before the auditors' report is issued and (2) the auditors obtain sufficient, appropriate evidence supporting the remediation of the significant deficiency, then the auditors should report the significant deficiency and the fact that it was remediated before the auditors' report was issued.

- (4) When auditors detect deficiencies in internal control that are not reportable conditions, they should communicate those deficiencies separately in a management letter to officials of the audited entity unless the deficiencies are clearly inconsequential considering both quantitative and qualitative factors. Auditors should refer to that management letter in the report on internal control. Auditors should use their professional judgment in deciding whether or how to communicate to officials of the audited entity deficiencies in internal control that are clearly inconsequential. Auditors should include in their audit documentation evidence of all communications to officials of the audited entity about deficiencies in internal control found during the audit.

SECTION 3. INTERNAL CONTROL REVIEW FOR PERFORMANCE AUDITING

- 3-1. GENERAL. In accordance with the GAS for performance audits, an assessment of applicable internal controls should be made when necessary to satisfy the audit objectives. The auditor should review internal controls to understand the relevant controls well enough to plan the audit. The auditor should summarize and document this understanding in the audit documentation.

In addition, understanding information systems controls is important for performance auditing when information systems are used extensively throughout the program under audit and the fundamental business processes related to the audit objectives rely on information systems. Information systems controls consist of those internal controls that are dependent on information systems processing and include general controls and application controls. Information systems general controls are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls help ensure the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning. Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions and data during application processing.

Information systems controls are significant to the audit objectives if auditors determine that it is necessary to evaluate the effectiveness of information systems controls in order to obtain sufficient, appropriate evidence. When information systems controls are determined to be significant to the audit objectives, auditors should then evaluate the design and operating effectiveness of such controls.

- a. Internal controls are the plan of organization, methods, and procedures adopted by management to ensure that:
- (1) Missions, goals, and objectives are met;
 - (2) resources are used consistent with laws, regulations, and policies;
 - (3) resources are safeguarded against waste, loss, and misuse;
 - (4) reliable data are obtained, maintained, and disclosed fairly in reports;
 - (5) security over computerized information systems will prevent or timely detect unauthorized access; and
 - (6) contingency planning for information systems provides essential back-up to prevent unwarranted disruption of activities and functions the systems support.

- b. Internal controls also encompass planning, organizing, directing, and controlling program operations. Included are management control systems for reporting and monitoring program performances. The audited entity's management is responsible for establishing an effective system of controls. Internal controls serve as the first line of defense in preventing and detecting errors, fraud, and violations of laws, regulations, and provisions of contracts and grant agreements.
- c. Auditors are encouraged to use Institute of Internal Auditors Standards in conjunction with GAGAS.

3-2. UNDERSTANDING INTERNAL CONTROLS. Auditors should obtain an understanding of internal control that is significant within the context of the audit objectives. For internal control that is significant within the context of the audit objectives, auditors should assess whether internal control has been properly designed and implemented. For those internal controls that are deemed significant within the context of the audit objectives, auditors should plan to obtain sufficient, appropriate evidence to support their assessment about the effectiveness of those controls. Auditors may modify the nature, timing, or extent of the audit procedures based on the auditors' assessment of internal control and the results of internal control testing.

Auditors may obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other auditors' reports, or direct tests. The procedures auditors perform to obtain an understanding of internal control may vary among audits based on audit objectives and audit risk. The extent of these procedures will vary based on the audit objectives, known or potential internal control risks or problems, and the auditors' knowledge about internal control gained in prior audits.

- a. The procedures the auditor will perform to obtain this understanding should depend on the type of audit and the particular aspects of the program.
- b. The auditor should also gain an understanding of the following categories of internal controls and focus on determining their significance to the planned audit objectives:
 - (1) Effectiveness and efficiency of program operations. Include those policies and procedures that management has implemented to reasonably ensure that the program meets its objectives, while considering cost-effectiveness and efficiency.
 - (2) Relevance and reliability of information. Include those policies and procedures that management has implemented to reasonably ensure that relevant and reliable information is obtained, maintained, and fairly disclosed in reports.

- (3) Compliance with applicable laws and regulations and provisions of contracts or grant agreements. Include policies and procedures that management has implemented to reasonably ensure that resources are used in compliance with laws, regulations, and policies and provisions of contracts or grant agreements.
 - (4) Safeguarding assets and resources. Include those policies and procedures that management has implemented to protect resources from waste, loss, and misuse.
 - c. In performance audits, a deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, detect, or correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations, on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.
- 3-3. ASSESSING SIGNIFICANCE OF CONTROLS TO AUDIT OBJECTIVES. After the auditor has gained a sufficient understanding of the internal controls relevant to the audit, the auditor should assess the significance of the controls to the intended audit objectives.
 - a. The auditor's assessment of significance may vary with the audit objectives. To determine whether the controls are significant and to what extent it is necessary to test those controls, the auditor should consider:
 - (1) The type of sufficient evidence needed to support audit judgment about those controls;
 - (2) the audit procedures needed to provide reasonable assurance about compliance with the significant laws and regulations and provisions of contracts or grant agreements; and
 - (3) collecting and evaluating the evidence relating to internal controls.
- 3-4. TESTS OF CONTROLS. When the auditor completes assessing the significance of controls to the objectives, the auditor should use the assessment results as a basis for planning and testing the controls for effectiveness. This process is similar to testing performed during the OIG field work phase. See Chapter 2215 (Managing the Audit).

- 3-5. REPORTING. Reporting on controls will vary depending on the significance of any weaknesses found and the relationship of those weaknesses to the audit objective. The auditor should identify in the audit report the scope of assessment work and any significant weaknesses found during the audit. See Chapter 2400 (Audit Report Preparation and Standards).
- a. Auditors should include in the audit report (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed. When auditors detect deficiencies in internal control that are not significant to the objectives of the audit, they may include those deficiencies in the report or communicate those deficiencies in writing to officials of the audited entity unless the deficiencies are inconsequential considering both qualitative and quantitative factors. Auditors should refer to that written communication in the audit report, if the written communication is separate from the audit report. Determining whether or how to communicate to officials of the audited entity deficiencies that are inconsequential within the context of the audit objectives is a matter of professional judgment. Auditors should document such communications.
 - b. In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. In reporting this type of finding, the internal control deficiency would be described as the cause.

SECTION 4. VULNERABILITY ASSESSMENTS

- 4-1. GENERAL. In compliance with OMB Circular A-123 and other OMB guidelines, the audited entity's management is responsible for performing vulnerability assessments on its programs and operations. The vulnerability assessments review the susceptibility of a program or function to waste, loss, unauthorized use, or misappropriation.
- a. The vulnerability assessments are also the mechanism with which management can determine the relative potential for loss in programs and functions, after giving consideration to such relevant factors as management priorities, resource constraints, the schedule of internal control reviews, and related actions.
 - b. The vulnerability assessments may be performed for the organization as a whole or individually for each program or administrative function as determined by size, nature, and degree of centralization of the programs or functions.
- 4-2. ASSESSMENT REVIEW. Vulnerability assessments can be a source of information for the auditor in obtaining an understanding of the audited entity's internal controls and structures during financial and performance auditing. The assessments can also aid the auditor in evaluating the applicable controls.
- a. The auditor should review the assessment results for the impact of the review of internal controls. However, the auditor's review of internal controls should not be limited to the vulnerability assessments since, by themselves, the assessments do not necessarily identify all the audited entity's weaknesses or result in improvements to the internal control systems.
 - b. The auditor should always keep in mind that vulnerability assessment results are based on management's judgment or other subjective approaches.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2325

Fraud, Illegal Acts, and Abuse

CHAPTER 2325 - FRAUD, ILLEGAL ACTS, AND ABUSECONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. DEFINING FRAUD, ILLEGAL ACTS, AND ABUSE	
2-1. Fraud.....	2
2-2. Illegal Acts.....	2
2-3. Abuse.....	2
SECTION 3. AUDITING FOR FRAUD	
3-1. Fraud Indicators.....	4
3-2. Prevention.....	4
3-3. Designing Audit Steps.....	5
SECTION 4. FRAUD INVESTIGATION	
4-1. General.....	8
4-2. Policy.....	8
4-3. Documenting Evidence.....	9
4-4. Reporting.....	9
SECTION 5. AUDIT SUPPORT	
5-1. Requests for Audit Support.....	12
5-2. Responsibilities of Audit Personnel.....	12
EXHIBITS	
A. Common Federal Statutes on Fraud and Conduct.....	14

CHAPTER 2325 - FRAUD, ILLEGAL ACTS, AND ABUSESECTION 1. GENERAL

- 1-1. PURPOSE. This chapter establishes OIG policy for detecting and reporting fraud, illegal acts, and abuse.
- 1-2. POLICY. The Office of Audits (OA) will report any evidence of fraud, illegal acts, significant violations of provisions of contracts or grant agreements, or abuse to the Office of Investigations (OI). The OA will consult with the Office of Legal Affairs (OLA) regarding the identification of fraud, illegal acts, significant violations of provisions of contracts or grant agreements, or abuse and their reporting in the audit report.

Upon identification or suspicion of fraud, auditors will report these instances directly to the Auditor-in-Charge (AIC) or Team Leader. The AIC or Team Leader will immediately notify the Senior Team Leader or, if the Senior Team leader is unavailable, the Group Chief or designee. The Group Chief or designee will report the incident to both the Assistant Inspector General for Audits (AIGA) and Deputy Assistant Inspector General for Audits (DAIGA).

The OA will remain alert to the indicators of fraud in each audit which it performs. To comply with Government Auditing Standards (GAS), audit programs will identify those audit steps which are designed to identify fraud. Auditors should refer to Section 3 of this Audit Chapter and the OIG Audit Manual Chapter 2210, Audit Planning, for additional information.

SECTION 2. DEFINING FRAUD, ILLEGAL ACTS, AND ABUSE

- 2-1. FRAUD. Fraud is an intentional misrepresentation of fact that results in the violation of a statute or implementing regulation. A common form of fraud is a false statement or false claim.
- a. Fraudulent acts may include claiming contract cost or business/employee reimbursement inappropriately; concealment or deceit to prevent identification of an activity resulting in a gain of money or other property regardless of whether personal gain results; omissions of a required action; conflict-of-interest; or unfair advantage. These acts may also include personal benefit, such as avoiding a cost.
 - b. Fraud includes, but is not limited to, the following activities: theft; embezzlement; bribery; gratuities; and violations of antitrust laws, such as price fixing and bid rigging.
- 2-2. ILLEGAL ACTS. An illegal act is any act of noncompliance that results in the violation of a statute or implementing regulation. See Exhibit A, Common Federal Statutes on Fraud and Conduct, for additional information.
- a. Criminal Acts. Offenses, usually requiring specific criminal intent and knowledge, can result in incarceration and fines after conviction under Federal or State criminal procedures. Prosecutors must prove guilt beyond a reasonable doubt.
 - b. Civil Acts. Violation of statutes providing for civil damages and penalties but not incarceration, with lesser or no requirement of knowledge. Burden of proof is based on preponderance of evidence rather than stricter criminal standard.
- 2-3. ABUSE. Abuse is distinct from fraud, illegal acts, or violations of provisions of contracts or grant agreements. When abuse occurs, no law, regulation, or provision of a contract or grant agreement is violated. Rather, abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Auditors should be alert to situations or transactions that could be indicative of abuse. When information comes to the auditors' attention (through audit procedures, allegations received through a fraud hotline, or other means) indicating that abuse may have occurred, auditors should consider whether the possible abuse affects the audit results significantly. However, because the determination of abuse is subjective, auditors are not expected to provide reasonable assurance of detecting it.

If during the course of the audit, auditors become aware of abuse that could be quantitatively or qualitatively material/significant to the financial statements or program under audit, auditors should apply audit procedures specifically directed to ascertain the potential effect on the financial statements or program under audit within the context of the audit objectives.

After performing additional work, auditors may discover that the abuse represents potential fraud or illegal acts. However, because the determination of abuse is subjective, auditors are not required to provide reasonable assurance of detecting abuse.

SECTION 3. AUDITING FOR FRAUD

3-1. FRAUD INDICATORS. Since fraud is the intentional deception or manipulation of acts resulting in an adverse effect to the benefit of an individual or entity, auditors must be aware of fraud indicators. (b) (7)(E)

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

3-2. PREVENTION. Accounting and administrative internal controls which deter fraud, illegal acts, or abuse are the primary responsibility of management. Management must maintain a system of checks and balances that will disclose any irregularities and improprieties having a material impact on operations or financial reporting; show a continuing effort to identify internal control weaknesses; and preclude the possibility of conflict of interest arrangements and conditions promoting intentional wrongdoing.

a. Auditors will:

1. Examine and evaluate the adequacy and effectiveness of management's actions and internal control systems which deter or prevent fraud and safeguard resources against waste, loss, or misuse and make appropriate recommendations;
 2. maintain sufficient knowledge of the characteristics of fraud, including common fraud types and techniques used to commit fraud; and
 3. exercise professional judgment when reviewing activities that are highly vulnerable to fraud, such as pay, procurement, cash management, property disposal, nonappropriated funds, and inventories.
- 3-3. DESIGNING AUDIT STEPS. OIG audit programs will be designed to provide the auditor with reasonable assurance of detecting significant instances of fraud, illegal acts or violations of provisions of contracts or grant agreements and abuse. When reviewing compliance with applicable laws and regulations, auditors will assess the risk that irregularities, illegal acts, and abuse could occur. See Chapter 2210, Audit Planning, for additional information. Auditors will:
- a. Evaluate the adequacy and effectiveness of the entity's internal controls for accounting and administration;
 - b. expand audit steps when there is evidence of fraud, illegal acts, significant violations of provisions of contracts or grant agreements, or abuse which could effect audit results, operations, programs, or functions; and
 - c. consult with the OI, OLA, and OA management and document the situation or transaction constituting the initial fraud, illegal act, significant violations of provisions of contracts or grant agreements, or abuse (see Section 4-2). In addition, avoiding interference with investigations or legal proceedings is important in pursuing indications of fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse. Laws, regulations, or policies might require auditors to report indications of certain types of fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse to law enforcement or investigatory authorities before performing additional procedures. When investigations or legal proceedings are initiated or in process, auditors should evaluate the impact on the current engagement. In some cases, it may be appropriate for the auditors to work with investigators and/or legal authorities, or withdraw from or defer further work on the engagement or a portion of the engagement to avoid interfering with an investigation.

- d. For financial audits and attestation engagements, auditors should design the audit to provide reasonable assurance of detecting misstatements that result from violations of provisions of contracts or grant agreements or illegal acts that could have a direct and material effect on the determination of financial statement amounts or other financial data significant to the audit objectives. If specific information comes to the auditors' attention that provides evidence concerning the existence of possible illegal acts that could have a material indirect effect on the financial statements, the auditors should apply audit procedures specifically directed to ascertaining whether an illegal act has occurred. When the auditors conclude that a violation of provisions of contracts or grant agreements or illegal acts has or is likely to have occurred, they should determine the effect on the financial statements as well as the implications for other aspects of the audit.

Under both the AICPA standards and GAGAS, auditors should plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Recognizing the possibility that a material misstatement due to fraud could be present is important for achieving this objective. However, absolute assurance is not attainable and thus even a properly planned and performed audit may not detect a material misstatement resulting from fraud.

- e. For performance audits, in planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives. Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussion with officials of the audited entity or through other means to determine the susceptibility of the program to fraud, the status of internal controls the entity has established to detect and prevent fraud, or the risk that officials of the audited entity could override internal control. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives. When auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud.

Auditors should determine which laws, regulations, and provisions of contracts or grant agreements are significant within the context of the audit objectives and

assess the risk that violations of those laws, regulations, and provisions of contracts or grant agreements could occur.

Based on that risk assessment, the auditors should design and perform procedures to provide reasonable assurance of detecting instances of violations of legal and regulatory requirements or violations of provisions of contracts or grant agreements that are significant within the context of the audit objectives.

If information comes to the auditors' attention indicating that significant fraud may have occurred within the context of the audit objectives, auditors should extend the audit steps and procedures, as necessary, to (1) determine whether fraud has likely occurred and (2) if so, determine its effect on the audit findings. If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

- f. For audits of internal OPM programs, auditors should refer to the most recent Office of Management and Budget (OMB) Circular A-123 vulnerability assessment and prior internal control reviews conducted by program officials.
- g. As reference material in designing audit steps to identify fraud, auditors may refer to the National Association of Certified Fraud Examiners (NACFE) Fraud Examiners Manual; Internal Auditors Handbook, Paul E. Heeschen and Lawrence B. Sawyer, Institute of Internal Auditors, Inc.; and Fraud Auditing and Forensic Accounting: New Tools and Techniques., G. Jack Bologna and Robert J. Lindquist.

SECTION 4. FRAUD INVESTIGATION

- 4-1. GENERAL. Areas of the OIG audit program that normally contain audit steps which identify fraud, illegal acts, or violations of provisions of contracts or grant agreements include the internal control review and computer based processing systems review; assessing compliance with applicable laws and regulations; and reviewing claimed reimbursements by contractors and employees and reconciling those claimed costs to the applicable accounting system.
- 4-2. POLICY. Auditors will exercise professional judgment and be alert to situations or transactions that could indicate evidence of fraud or illegal activity. If identified, auditors will:
- a. Immediately notify their appropriate Group Chiefs or designee and Senior Team Leaders who will immediately report these acts to the AIGA;
 - b. in consultation with the OI and OLA, determine those audit steps which are required to verify the existence and extent of the fraud or illegal activity and identify the effect on the entity's financial statements, operations, or programs;
 - c. work closely with the designated investigator by responding in a timely fashion to all requests and identify other conditions or internal control weaknesses which may be subject to fraud or illegal activity;
 - d. report the results of work performed during the audit to the designated investigator;
 - e. ensure that extended audit steps do not interfere or jeopardize potential investigations by OIG or other law enforcement investigators, such as Rule 6(e) of the Federal Rules of Criminal Procedure, as explained in Section 5-2 of this Chapter;
 - f. prepare audit documentation which document the illegal activity; demonstrate its effect; and fully comply with OIG policy on the preparation of audit documentation (See Chapter 2220, Audit Documentation and Files, for additional information) and on documenting evidence, as explained in Section 4-3; and
 - g. in consultation with the AIGA, continue to conduct the audit; the OI will advise the OA on the correct course of action from an investigative standpoint.

- 4-3. DOCUMENTING EVIDENCE. Auditors should take the following actions to document evidence when suspected fraudulent or illegal activity is revealed during audit proceedings:
- a. Photocopy suspicious documentary evidence, including all attachments. Annotate, on the bottom right corner of the back copy, their initials; the date and time the copy was made; the location of the original document; whether the document appears to be a copy; the type of markings found on the document; and the owner's name.
 - b. Place their initials after all notations they make on the document.
 - c. If there are multiple documents containing similar information, then annotate the required information on the first copy as explained in Sections 4-3.a. and 4-3.b. Indicate the date, time, and originality information on remaining copies.
 - d. When documenting testimonial evidence, the auditor should prepare a memorandum to file which identifies the source; provides a clear recitation of statements made; indicates the date, time, and place the statements were made; and identifies any witnesses to the interview.
 - e. Generate two copies of documentary evidence or memorandums to file related to testimonial evidence. One copy will be required to support investigative operations and the other copy will support audit documentation.
- 4-4. REPORTING. Auditors are required to report occurrences of fraud or illegal activity that are significant within the context of the audit objectives. Other instances of fraud are required to be communicated in writing to the attention of those charged to monitor.
- a. The OI and OA staff and the OLA will confer and decide what, if any, activities will be disclosed and the type of reporting to be used. The Group Chief or designee will be advised of this decision.
 - b. Audit reports may disclose indictments or convictions.
 - c. Auditors may identify relevant information concerning fraud, illegal acts, and significant violations of provisions of contracts or grant agreements, or abuse in a separate audit report if appropriate to the circumstances. The OA and OI staff and the OLA will confer and decide, what, if any, activities will be disclosed, and the type of reporting to be used. The Group Chief or designee will be advised of this decision.

- d. For financial audits, auditors have responsibilities for detecting fraud and illegal acts that have a material effect on the financial statements and determining whether those charged with governance are adequately informed about fraud and illegal acts. GAGAS include additional reporting standards. For financial audits and attestation engagements, when auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their audit report the relevant information about:
1. fraud and illegal acts that have an effect on the financial statements and/or the subject matter that is more than inconsequential;
 2. violations of provisions of contracts or grant agreements that have a material effect on the determination of financial statement amounts or other financial data significant to the audit and/or subject matter; and,
 3. abuse that is material to the financial statements and/or the subject matter, either quantitatively or qualitatively.
- e. For financial audits and attestation engagements, when auditors detect violations of provisions of contracts or grant agreements or abuse that have an effect on the financial statements/engagements that is less than material but more than inconsequential, they should communicate those findings in writing to officials of the audited entity. Determining whether and how to communicate to officials internal control deficiencies that have an inconsequential effect on the financial statements/engagements is a matter of professional judgment. Auditors should document such communications.
- f. For performance audits, when auditors conclude, based on sufficient, appropriate evidence, that fraud, noncompliance with provisions of laws, regulations contracts or grant agreements, or abuse either has occurred or is likely to have occurred which is significant within the context of the audit objectives, they should report the matter as a finding. Whether a particular act is, in fact, fraud or noncompliance with provisions of laws, regulations, contracts of grant agreements may have to await final determination by a court of law or other adjudicative body.
- g. For performance audits, when auditors detect fraud, violations of provisions of contracts or grant agreements, or abuse that are not significant, they should communicate those findings in writing to officials of the audited entity unless the findings are inconsequential within the context of the audit objectives, considering both qualitative and quantitative factors. For attestation agreements,

when auditors detect violations of provisions of contracts or grant agreements or abuse that have an effect on the subject matter that is less than material but more than inconsequential, they should communicate those findings in writing to entity officials.

Determining whether or how to communicate to officials of the audited entity fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse that is inconsequential is a matter of the auditors' professional judgment. Auditors should document such communications.

- h. For performance audits and attestation engagements, when fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse either have occurred or are likely to have occurred, auditors may consult with authorities or legal counsel about whether publicly reporting such information would compromise investigative or legal proceedings. Auditors may limit their public reporting to matters that would not compromise those proceedings, and for example, report only on information that is already a part of the public record.
- i. For all audits, when an audit entity's management fails to satisfy legal or regulatory requirements to report such information to external parties specified in laws or regulations, the auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the information directly to the specified external parties. When an audit entity's management fails to take timely and appropriate steps to respond to known or likely fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse that (1) is significant to the findings and conclusions and (2) involves funding received directly or indirectly from a government agency, auditors should first report management's failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors' communication with those charged with governance, then the auditors should report the entity's failure to take timely and appropriate steps directly to the funding agency. Auditors should comply with these requirements even if they have resigned or been dismissed from the engagement prior to its completion. Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by the audited entity's management that it has reported such findings in accordance with regulations and funding agreements. When auditors are unable to do so, they should report such information directly as stated above. Internal audit organizations do not have a

duty to report outside the audited entity unless required by law, rule, regulation, or policy.

SECTION 5. AUDIT SUPPORT

- 5-1. REQUESTS FOR AUDIT SUPPORT. Should the OI or the OLA request audit support for an investigation, the OA will provide full cooperation and assistance, including the assignment of auditors to a team investigating illegal activity.
- a. All audit support requests will be made in writing.
 - b. To document requests for audit support, the OIG OA will prepare a listing of these requests and revise it when necessary.
 - c. Audit programs will include those audit steps the investigator requests to detect the fraud or illegal activity.
 - d. The AIGA, AIGI, and OLA will meet to determine the nature and extent of reporting the audit results.
- 5-2. RESPONSIBILITIES OF AUDIT PERSONNEL. Audit officials will consider the following factors in selecting auditors to support investigators in the investigative process: auditor level of experience, special skill, or expertise in the particular activity or program under review; specific auditor name request; auditor level of certification (Certified Public Accountant, Certified Fraud Examiner, or Certified Internal Auditor); and the auditor's interest in participating in the investigation.
- a. The AIGA and AIGI will resolve any disagreements concerning assignment of audit staff to the investigation.
 - b. Auditors will not perform duties traditionally assigned to investigators.
 - c. Auditors and investigators will share information which is not related to a matter occurring before a grand jury, and thus covered by Rule 6(e) of the Federal Rules of Criminal Procedure. Rule 6(e) requires that matters occurring before a grand jury be kept secret. Auditors and investigators cannot discuss the grand jury proceedings with anyone, including other OIG staff and supervisory personnel. To prevent the appearance of improper disclosure of information, auditors will:
 1. Not be involved in any other audits that may potentially relate, in any manner, to the matter under investigation; and

2. cease any oversight responsibilities for the entity if the audit supervisor is a member of the investigation (these responsibilities can resume when Government criminal proceedings end).
- d. Investigators may review and copy audit working papers.
- e. If auditors obtain original documents, including contractor records, that reflect indicators of fraud, illegal acts, significant violations of provisions of contracts or grant agreements, or abuse, they will immediately notify the AIGI according to the procedure in Section 4-2 and document the evidence in accordance with procedures in Section 4-3. The AIGI will take appropriate measures to maintain custody and control of the documents for use as evidence in subsequent criminal proceedings.
- f. The AIGI and AIGA will jointly decide whether the organization being audited is the subject of an investigation, in addition to an audit. Auditors will receive appropriate guidance from both the AIGI and AIGA in responding to potential questions from the audit entity or subject.
- g. Access to records may be gained through contract clause, voluntary disclosure by the entity, Inspector General subpoena (in the case of nonfederal records), search warrant, and grand jury subpoena.
 1. Auditors will not use their position to acquire information that would not normally be available to the auditor in the conduct of an audit. The auditor will request that the investigator obtain the information through other legal means.
 2. Auditors will not use deception or false pretense to obtain documents.

COMMON FEDERAL STATUTES ON FRAUD AND CONDUCT

Following are short digests of the major civil and criminal statutes relating to fraud and conflicts of interest. The digests are designed merely to provide an introduction to the range of prohibited acts in this area. Since many of the statutes are complex, the auditor should not rely on these summaries alone but, where necessary, refer to the United States Code provision cited or consult with the OLA.

1. Sherman Antitrust Act, 15 U.S.C. § 1. This act prohibits competitors from entering into any agreement to restrain trade in interstate commerce, including price fixing and bid rigging schemes. <http://www.justice.gov/atr/public/divisionmanual/chapter2.pdf>
2. Bribery, Graft, and Conflicts of Interest, 18 U.S.C. §§ 201-209. These statutes prohibit a broad range of activities, such as giving or receiving a bribe or gratuity and engaging in a conflict of interest by a federal government employee.
<http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/11/toc.html>
 - a. Bribery includes giving a government employee something of value for the purpose of influencing any official act.
 - b. Gratuities are gifts of value to a government employee because of the employee's official position. The Government does not have to prove that the gratuity was provided to influence any official act.
 - c. Conflicts of interest are those situations where a Government employee engages in activities that create an actual or appearance of conflict between the employee's personal interests and official duties and responsibilities, such as acting as an agent or attorney for anyone before an agency or taking part in decisions in which he or a relative has a financial interest. Certain restrictions apply to activities of former Government employees such as appearing before Government agencies within a specified period after employment.

3. Voiding Contracts, 18 U.S.C. § 218. Federal agencies may terminate contracts obtained through bribery, graft, or conflicts of interest.
http://caselaw.lp.findlaw.com/cascode/uscodes/18/parts/i/chapters/11/sections/section_218.html
4. Conspiracy - Claims, 18 U.S.C. § 286. This statute provides that any person who enters into an agreement or conspiracy to defraud the United States by obtaining, or aiding obtaining, the payment for any false or fraudulent claim should be fined not more than \$10,000 or imprisoned not more than 10 years, or both.
http://caselaw.lp.findlaw.com/cascode/uscodes/18/parts/i/chapters/15/sections/section_286.html
5. False Claims, 18 U.S.C. § 287. This statute punishes the making of any false, fictitious, or fraudulent claim against any department or agency of the United States. Payment of the claim need not be an element of the offense or proven in order to obtain a conviction.
<http://trac.syr.edu/laws/18USC287.html>
http://caselaw.lp.findlaw.com/cascode/uscodes/18/parts/i/chapters/15/sections/section_287.html
6. Conspiracy, 18 U.S.C. § 371. This statute prohibits any agreement between two or more persons or entities to defraud the United States or violate any federal law or regulation when at least one person commits an act in furtherance of the agreement.
<http://www4.law.cornell.edu/uscode/18/371.html>
<http://trac.syr.edu/laws/18USC371.html>
7. Theft, Embezzlement, or Destruction of Public Money, Property, or Records, 18 U.S.C. § 641. This statute prohibits intentional and unauthorized taking, destruction, receipt, concealment, embezzlement, conversion or use of federal government property, records, vouchers, including property being made under contract for the government.
<http://trac.syr.edu/laws/18USC0641.html>
http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=641

8. Mail Fraud, 18 U.S.C. § 1341, and Wire Fraud, 18 U.S.C. § 1343. It is illegal to engage in any scheme which uses delivery by the Postal Service or interstate wire, radio, or television to defraud. Use of the mail or wire communications includes sending or receiving any matter through these mediums.
<http://www4.law.cornell.edu/uscode/18/1341.html>
<http://trac.syr.edu/laws/18USC1341.html> <http://trac.syr.edu/laws/18USC1343.html>
http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=1343
9. False Statements, 18 U.S.C. § 1001. This statute makes the following acts illegal when they relate to any matter within the jurisdiction of any Federal agency or department:
 - a. Falsify, conceal, or cover up a material fact by any trick, scheme, or device;
 - b. knowingly make false, fictitious, or fraudulent statements, certifications, or representations; or
 - c. knowingly make or use any false documents or writing.
<http://trac.syr.edu/laws/18USC1001.html>
http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=1001
10. Obstruction of Federal Audit, 18 U.S.C. § 1516. This section prohibits the influencing, obstructing, or impeding of a federal audit through the destruction or fabrication of documents or intimidation of witness and contractor employees. It is illegal to intentionally deceive or defraud any federal official conducting contract audits of persons or entities receiving \$100,000 or more in one year. Convicted persons are subject to fines or imprisonment of not more than five years, or both. This statute specifically covers quality assurance in addition to audits. <http://www4.law.cornell.edu/uscode/18/1516.html>
11. Trade Secrets Act, 18 U.S.C. § 1905. This statute prohibits unauthorized release of any information relating to trade secrets or confidential business data by a federal employee who receives such information in conducting official duties. This information includes, but is not limited to, advance procurement information, pricing or income information, technical proposals, and proprietary information.
<http://www4.law.cornell.edu/uscode/18/1905.html>

12. Racketeer-Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961-1968. While aimed at organized crime, this statute may be applicable in situations involving frauds in Federal agencies. "Racketeering" is defined as any number of offenses under federal law, including those discussed above. The statute is applicable to "enterprises," including an individual, partnership, corporation, association, or other legal entity.
<http://www4.law.cornell.edu/uscode/18/p1ch96.html>
13. Anti-kickback Act, 41 U.S.C. §§ 53-55. It is illegal to provide or attempt to provide or offer any fee, commission, compensation, gift, or gratuity to a prime contractor, higher tier subcontractor, or employee of one of these firms, for the purpose of improperly obtaining favorable treatment under a government contract.
http://idcontent.bellevue.edu/content/CORPORATE/kiewit/antikickback/Anti-Kickback_Act.pdf
14. Forfeiture of Fraud Claims, 28, U.S.C. § 2514. Any claim against the United States shall be forfeited to the United States by any person who corruptly practices or attempts to practice any fraud against the United States. Activities included are the proof, statement, establishment, or allowance of the claim.
<http://www4.law.cornell.edu/uscode/28/2514.html>
15. Federal Procurement Act, 41 U.S.C. § 423. Prohibits government officials, employees, consultants and advisors, and those of competing contractors from conducting certain activities relating to promises of future employment to procurement officials during federal agency procurements of property or services. Federal procurement officials must certify that they are familiar with certain provisions of the law and will not violate these provisions and immediately report to the contracting officer any information concerning a violation or potential violation. Administrative, civil, and criminal penalties are available under the Act.
<http://www.gpo.gov/fdsys/pkg/USCODE-1998-title41/html/USCODE-1998-title41-chap7-sec423.htm>
16. False Claims Act, 31 U.S.C. §§ 3729-3733. This Act provides civil penalties of between \$5,000 and \$10,000, plus up to three times the amount of the damages (double damages are allowed if a person comes forward prior to investigation of civil or criminal action or within 30 days of his discovery of a false claim) the government sustains when a person knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval. Among other offenses covered by the Act are:

- a. Knowingly making or using, or causing to be made or used, a false record or statement to get a false or fraudulent claim paid or approved;
- b. conspiring to defraud the government by getting a false or fraudulent claim paid or approved;
- c. knowingly making or using, or causing to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the government.

Corporations and partnerships are liable for the acts of their employees. A claim against the government is specifically defined as including a demand for money made upon a contractor or grantee if the United States provides any portion of the money demanded or will reimburse any portion thereof. Types of claims include: bid rigging, defective pricing, discount and marketing data, items billed but not delivered, product substitution, or mischarging. Statute of limitations: Six years from when a false claim submitted or three years from when a responsible government official first learned of the false claim but no more than 10 years after the false claim was submitted.

<http://www.law.cornell.edu/uscode/text/31/3729>

http://www.justice.gov/civil/docs_forms/C-FRAUDS_FCA_Primer.pdf

17. Program Fraud Civil Remedies Act, 31 U.S.C. § 3801. (b) (7)(E) [REDACTED]
- [REDACTED]
- [REDACTED]
- <http://www4.law.cornell.edu/uscode/31/3801.html>
18. Contract Disputes Act, 41 U.S.C. § 604. Provides for the recovery of the amount of a claim or portion thereof, whether or not paid, which is presented to contracting officers for payment and which is based upon fraud or misrepresentation. The contractor is liable for the amount of false and unsupported portion of the claim whether or not it has been paid by the Government. Claim must be in writing and certified and the contractor must know that the claim is false. Government may also recover the cost of investigation.
- <http://www.cohenseglia.com/federal-contracting-database/the-contract-disputes-act>

19. Federal Employees Health Benefits Act Debarment, 5 U.S.C. § 8902a. This Act empowers OPM to suspend or debar health insurance carriers or providers of health care services upon conviction of a state or federal criminal offense relating to fraud or financial misconduct, neglect or abuse of patients, or interference with or obstruction of investigation or prosecution of a criminal offense, or of a criminal offense relating to unlawful manufacture, distribution, prescription, or dispensing of a controlled substance. Other grounds for debarment include: revocation, restriction or nonrenewal of a license to provide health care services or supplies, or determination by OPM of fraudulent activity with regard to submission of claims or the knowing failure of a provider to provide information required by a carrier to determine whether payment or reimbursement can be made or the amount of such payment. Civil monetary penalties provided. Six years statute of limitations.
- <http://www.opm.gov/oig/html/debar.asp>
<http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2004/pdf/04-4730.pdf>

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2330

**Ethical Principles in
Government Auditing**

CHAPTER 2330 – ETHICAL PRINCIPLES IN GOVERNMENT AUDITING

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. ETHICAL PRINCIPLES	
2-1. Management and Ethical Principles.....	2
2-2. Types of Principles Under GAGAS.....	2
2-3. Ethics Training.....	4

CHAPTER 2330 – ETHICAL PRINCIPLES IN GOVERNMENT AUDITINGSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides the ethical principles' foundation, discipline, and structure as well as the climate which influences the application of GAGAS. This chapter deals with the fundamental principles rather than specific requirements.
- 1-2. POLICY. The OIG Office of Audits will use the ethical principles found in the Government Auditing Standards as guidelines for conducting financial and performance audits. The ethical principles contained in the following sections provide the overall framework for application of GAGAS, including general standards, field work standards, and reporting standards. Each principle is described, rather than set forth as a series of requirements, so that auditors can consider the facts and circumstances of each situation within the framework of these ethical principles.

SECTION 2. ETHICAL PRINCIPLES

- 2-1. MANAGEMENT AND ETHICAL PRINCIPLES. Management of the audit organization sets the tone for ethical behavior throughout the organization by maintaining an ethical culture, clearly communicating acceptable behavior and expectations to each employee, and creating an environment that reinforces and encourages ethical behavior throughout all levels of the organization. The ethical tone maintained and demonstrated by management and staff is an essential element of a positive ethical environment for the audit organization.

Conducting audit work in accordance with ethical principles is a matter of personal and organizational responsibility. Ethical principles apply in preserving auditor independence, taking on only work that the auditor is competent to perform, performing high-quality work, and following the applicable standards cited in the audit report.

- 2-2. TYPES OF PRINCIPLES UNDER GAGAS. The ethical principles that guide the work of auditors who conduct audits in accordance with GAGAS are:

- The Public Interest;
 - Integrity;
 - Objectivity;
 - Proper Use of Government Information, Resources, and Position; and
 - Professional Behavior.
- a. The Public Interest. The public interest is defined as the collective well-being of the community of people and entities the auditors serve. Observing integrity, objectivity, and independence in discharging their professional responsibilities assists auditors in meeting the principle of serving the public interest and honoring the public trust. These principles are fundamental to the responsibilities of auditors and critical in the government environment. A distinguishing mark of an auditor is acceptance of responsibility to serve the public interest. This responsibility is critical when auditing in the government environment. GAGAS embody the concept of accountability for public resources, which is fundamental to serving the public interest.

- b. Integrity. Public confidence in government is maintained and strengthened by auditors' performing their professional responsibilities with integrity. Integrity includes auditors' conducting their work with an attitude that is objective, fact-based, nonpartisan, and nonideological with regard to audited entities and users of the auditors' reports. Within the constraints of applicable confidentiality laws, rules, or policies, communications with the audited entity, those charged with governance, and the individuals contracting for or requesting the audit are expected to be honest, candid, and constructive.

Making decisions consistent with the public interest of the program or activity under audit is an important part of the principle of integrity. In discharging their professional responsibilities, auditors may encounter conflicting pressures from management of the audited entity, various levels of government, and other likely users. Auditors may also encounter pressures to violate ethical principles to inappropriately achieve personal or organizational gain. In resolving those conflicts and pressures, acting with integrity means that auditors place priority on their responsibilities to the public interest.

- c. Objectivity. The credibility of auditing in the government sector is based on auditors' objectivity in discharging their professional responsibilities. Objectivity includes being independent in fact and appearance when providing audit and attestation engagements, maintaining an attitude of impartiality, having intellectual honesty, and being free of conflicts of interest. Avoiding conflicts that may, in fact or appearance, impair auditors' objectivity in performing the audit or attestation engagement is essential to retaining credibility. Maintaining objectivity includes a continuing assessment of relationships with audited entities and other stakeholders in the context of the auditors' responsibility to the public.
- d. Proper use of Government Information, Resources, and Position. Government information, resources, or positions are to be used for official purposes and not inappropriately for the auditor's personal gain or in a manner contrary to law or detrimental to the legitimate interests of the audited entity or the audit organization. This concept includes the proper handling of sensitive or classified information or resources.

In the government environment, the public's right to the transparency of government information has to be balanced with the proper use of that information. In addition, many government programs are subject to laws and regulations dealing with the disclosure of information. To accomplish this balance, exercising discretion in the use of information acquired in the course of

auditors' duties is an important part in achieving this goal. Improperly disclosing any such information to third parties is not an acceptable practice.

As accountability professionals, accountability to the public for the proper use and prudent management of government resources is an essential part of auditors' responsibilities. Protecting and conserving government resources and using them appropriately for authorized activities is an important element in the public's expectations for auditors.

Misusing the position of an auditor for personal gain violates an auditor's fundamental responsibilities. An auditor's credibility can be damaged by actions that could be perceived by an objective third party with knowledge of the relevant information as improperly benefiting an auditor's personal financial interests or those of an immediate or close family member; a general partner; an organization for which the auditor serves as an officer, director, trustee, or employee; or an organization with which the auditor is negotiating concerning future employment.

- e. Professional Behavior. High expectations for the auditing profession include compliance with laws and regulations and avoidance of any conduct that might bring discredit to auditors' work, including actions that would cause an objective third party with knowledge of the relevant information to conclude that the auditors' work was professionally deficient. Professional behavior includes auditors' putting forth an honest effort in performance of their duties and professional services in accordance with the relevant technical and professional standards.
- 2-3. ETHICS TRAINING. OIG management and audit staff are required to review and complete an annual one-hour ethics briefing. The briefing is a computer web-based training program developed by the U.S. Office of Government Ethics. OIG staff and auditors are required to spend at least one hour on the training program. The program has various ethic topics for review. Once the individual is finished with a topic, he or she answers questions pertaining to each topic. Upon completion of the training, a certificate is completed and submitted to OPM's Office of General Counsel. The auditor also keeps a copy of the certificate for CPE training purposes.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2335

**Independence in
Government Auditing**

CHAPTER 2335 – INDEPENDENCE IN GOVERNMENT AUDITING

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. DEFINING INDEPENDENCE	
2-1. Independence of Mind.....	2
2-2. Independence in Appearance.....	2
SECTION 3. INDEPENDENCE THREATS AND SAFEGUARDS	
3-1. Threats to Independence	3
3-2. Safeguards to Identified Threats.....	3
SECTION 4. ADDRESSING THREATS TO INDEPENDENCE	
4-1. Applying GAGAS Conceptual Framework Approach to Independence	5
SECTION 5. GOVERNMENT AUDITORS AND AUDIT ORGANIZATION STRUCTURE	
5-1. External Auditor Independence	7
5-2. Internal Auditor Independence	8

CHAPTER 2335 – INDEPENDENCE IN GOVERNMENT AUDITINGSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter establishes the OIG policy for Independence. It also provides a conceptual framework to implement this policy.
- 1-2. POLICY. The Office of Audits (OA) will be independent in mind and appearance when performing audits and professional engagements. The OIG Office of Audits will use the independence standards found in the Generally Accepted Government Auditing Standards (GAGAS) as guidelines for conducting financial and performance audits.

SECTION 2. DEFINING INDEPENDENCE2-1. INDEPENDENCE OF MIND

The Office of Audits auditor's state of mind as it relates to financial statements or subject matter audits or professional engagements must enable the auditor to perform an audit without being affected by influences that could compromise professional judgment during the time period covered. This allows the auditor to act with integrity and exercise objectivity and professional skepticism.

2-2. INDEPENDENCE IN APPEARANCE

The Office of Audits must demonstrate to a reasonable and informed third party that the integrity, objectivity, or professional skepticism as it relates to audits or professional engagements has not been compromised.

SECTION 3. INDEPENDENCE THREATS AND SAFEGUARDS

- 3-1. THREATS TO INDEPENDENCE. Auditors should evaluate the following broad categories of threats to independence when threats are being identified and evaluated:
- a. Self-interest threat - the threat that a financial or other interest will inappropriately influence an auditor's judgment or behavior;
 - b. Self-review threat - the threat that an auditor or audit organization that has provided non-audit services will not appropriately evaluate the results of previous judgments made or services performed as part of the non-audit services when forming a judgment significant to an audit;
 - c. Bias threat - the threat that an auditor will, as a result of political, ideological, social, or other convictions, take a position that is not objective;
 - d. Familiarity threat - the threat that aspects of a relationship with management or personnel of an audited entity, such as a close or long relationship, or that of an immediate or close family member, will lead an auditor to take a position that is not objective;
 - e. Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments;
 - f. Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit; and
 - g. Structural threat - the threat that an audit organization's placement within a government entity, in combination with the structure of the government entity being audited, will impact the audit organization's ability to perform work and report results objectively.
- 3-2. SAFEGUARDS TO IDENTIFIED THREATS.

Safeguards are controls designed to eliminate or reduce to an acceptable level threats to independence. Under the conceptual framework, the auditor applies safeguards that address the specific facts and circumstances under which threats to independence exist. In some cases, multiple safeguards may be necessary to address a threat. The list of safeguards in this section provides examples that may be effective under certain

circumstances. The list cannot provide safeguards for all circumstances. It may, however, provide a starting point for auditors who have identified threats to independence and are considering what safeguards could eliminate those threats or reduce them to an acceptable level. Examples of safeguards include:

- a. Consultation with professional organizations, regulatory bodies, or another auditor;
- b. Involving another audit organization to perform or re-perform part of the audit;
- c. Having a professional staff member who was not a member of the audit team review the work performed;
- d. Removing an individual from an audit team when that individual's financial or other interests or relationships pose a threat to independence;
- e. An entity requirement that persons other than management ratify or approve the appointment of an audit organization to perform an audit;

To ensure Independence the Office of Audits requires the following documented safeguards:

- a. Independence Declaration. To provide evidence that audit work is free from personal and external impairments, all audit team members who prepared, worked on or reviewed an audit report or set of work papers (this includes the Group Chief, Senior Team Leader, Team Leader/AIC, audit staff, and the independent referencer) must complete the "Audit Staff Declaration of Personal and Financial Independence" statement for each audit in which they are involved. This statement is retained with the audit documentation and should be properly signed and dated by all staff involved with the audit. In addition, each auditor should immediately notify his/her immediate supervisor when something occurs that may impair their independence.
- b. Financial Disclosure Form. GS-13's or above must complete and file a financial disclosure statement annually with the Assistant IG for Legal Affairs and OPM's Designated Ethics Officer (see Chapter 2210). If OIG employees engage in outside work, a formal statement is submitted to their supervisor (see Chapter 2210).

SECTION 4. ADDRESSING THREATS TO INDEPENDENCE4-1. APPLYING GAGAS CONCEPTUAL FRAMEWORK APPROACH TO INDEPENDENCE

The conceptual framework assists auditors in maintaining both independence of mind and independence in appearance. It can be applied to many variations in circumstances that create threats to independence and allows auditors to address threats to independence that result from activities that are not specifically prohibited by GAGAS. Auditors should apply the conceptual framework at the audit organization, audit, and individual auditor levels to:

- a. identify threats to independence;
- b. evaluate the significance of the threats identified, both individually and in the aggregate; and
- c. apply safeguards as necessary to eliminate the threats or reduce them to an acceptable level.

If no safeguards are available to eliminate an unacceptable threat or reduce it to an acceptable level, independence would be considered impaired.

Auditors should evaluate threats to independence using the conceptual framework when the facts and circumstances under which the auditors perform their work may create or augment threats to independence. Auditors should evaluate threats both individually and in the aggregate because threats can have a cumulative effect on an auditor's independence.

Facts and circumstances that create threats to independence can result from events such as the start of a new audit; assignment of new staff to an ongoing audit; and acceptance of a non-audit service at an audited entity. Many other events can result in threats to independence. Auditors use professional judgment to determine whether the facts and circumstances created by an event warrant use of the conceptual framework. Whenever relevant new information about a threat to independence comes to the attention of the auditor during the audit, the auditor should evaluate the significance of the threat in accordance with the conceptual framework.

Auditors should determine whether identified threats to independence are at an acceptable level or have been eliminated or reduced to an acceptable level. A threat to

independence is not acceptable if it either (a) could impact the auditor's ability to perform an audit without being affected by influences that compromise professional judgment or (b) could expose the auditor or audit organization to circumstances that would cause a reasonable and informed third party to conclude that the integrity, objectivity, or professional skepticism of the audit organization, or a member of the audit team, had been compromised.

When an auditor identifies threats to independence and, based on an evaluation of those threats, determines that they are not at an acceptable level, the auditor should determine whether appropriate safeguards are available and can be applied to eliminate the threats or reduce them to an acceptable level. The auditor should exercise professional judgment in making that determination, and should take into account whether both independence of mind and independence in appearance are maintained. The auditor should evaluate both qualitative and quantitative factors when determining the significance of a threat.

In cases where threats to independence are not at an acceptable level, thereby requiring the application of safeguards, the auditors should document the threats identified and the safeguards applied to eliminate the threats or reduce them to an acceptable level.

Certain conditions may lead to threats that are so significant that they cannot be eliminated or reduced to an acceptable level through the application of safeguards, resulting in impaired independence. Under such conditions, auditors should decline to perform a prospective audit or terminate an audit in progress.

If a threat to independence is initially identified after the auditors' report is issued, the auditor should evaluate the threat's impact on the audit and on GAGAS compliance. If the auditors determine that the newly identified threat had an impact on the audit that would have resulted in the auditors' report being different from the report issued had the auditors been aware of it, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. If the report was previously posted to the auditors' publicly accessible website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

SECTION 5. GOVERNMENT AUDITORS AND AUDIT ORGANIZATION STRUCTURE

The ability of audit organizations in government entities to perform work and report the results objectively can be affected by placement within government and the structure of the government entity being audited. The independence standard applies to auditors in government entities whether they report to third parties externally (external auditors), to senior management within the audited entity (internal auditors), or to both.

5-1 EXTERNAL AUDITOR INDEPENDENCE.

Audit organizations that are structurally located within government entities are often subject to constitutional or statutory safeguards that mitigate the effects of structural threats to independence. For external audit organizations, such safeguards may include governmental structures under which a government audit organization is:

- a. at a level of government other than the one of which the audited entity is part (federal, state, or local); for example, federal auditors auditing a state government program; or
- b. placed within a different branch of government from that of the audited entity; for example, legislative auditors auditing an executive branch program.

Safeguards other than those described above may mitigate threats resulting from governmental structures. For external auditors or auditors who report both externally and internally, structural threats may be mitigated if the head of an audit organization meets any of the following criteria in accordance with constitutional or statutory requirements:

- a. directly elected by voters of the jurisdiction being audited;
- b. elected or appointed by a legislative body, subject to removal by a legislative body, and reports the results of audits to and is accountable to a legislative body;
- c. appointed by someone other than a legislative body, so long as the appointment is confirmed by a legislative body and removal from the position is subject to oversight or approval by a legislative body, and reports the results of audits to and is accountable to a legislative body; or
- d. appointed by, accountable to, reports to, and can only be removed by a statutorily created governing body, the majority of whose members are independently elected or appointed and are outside the organization being audited.

The following safeguards may also be used to augment those previously listed, including:

- a. statutory protections that prevent the audited entity from abolishing the audit organization;
- b. statutory protections that require that if the head of the audit organization is removed from office, the head of the agency reports this fact and the reasons for the removal to the legislative body;
- c. statutory protections that prevent the audited entity from interfering with the initiation, scope, timing, and completion of any audit;
- d. statutory protections that prevent the audited entity from interfering with audit reporting, including the findings and conclusions or the manner, means, or timing of the audit organization's reports;
- e. statutory protections that require the audit organization to report to a legislative body or other independent governing body on a recurring basis;
- f. statutory protections that give the audit organization sole authority over the selection, retention, advancement, and dismissal of its staff; and
- g. statutory access to records and documents related to the agency, program, or function being audited and access to government officials or other individuals as needed to conduct the audit.

5-2 INTERNAL AUDITOR INDEPENDENCE.

Internal auditors who work under the direction of the audited entity's management are considered independent for the purposes of reporting internally if the head of the audit organization meets all of the following criteria:

- a. is accountable to the head or deputy head of the government entity or to those charged with governance;
- b. reports the audit results both to the head or deputy head of the government entity and to those charged with governance;

- c. is located organizationally outside the staff or line-management function of the unit under audit;
- d. has access to those charged with governance; and
- e. is sufficiently removed from political pressures to conduct audits and report findings, opinions, and conclusions objectively without fear of political reprisal.

When internal audit organizations perform audits of external parties such as auditing contractors or outside party agreements, and no impairments to independence exist, the audit organization can be considered independent as an external audit organization of those external parties.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2400

Audit Report Preparation and Standards

CHAPTER 2400 - AUDIT REPORT PREPARATION AND STANDARDS

CONTENTS

	<u>Page</u>
 SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy and Standards.....	1
 SECTION 2. REPORTING STANDARDS	
2-1. General.....	2
2-2. Financial Reporting Standards.....	6
2-3. Performance Audit Reporting Standards.....	15
2-4. Reporting Standards for Special Audit Requests.....	19
2-5. Reporting Standards for Attestations.....	19
2-6. Federal Financial Statement Audit Reporting Standards.....	27
2-7. Flash Audit Report.....	30
 EXHIBITS	
A. Examples of Audit Report Opinions	
B. Examples of Compliance for Financial Audits	
C. Examples of Internal Controls for Financial Audits	
D. Examples of Compliance for Performance Audits	
E. Examples of Internal Controls for Performance Audits	
F. Examples of Attestation Reports	
G. Examples of Federal Financial Statement Audit Reports	
H. Example of the OIG Transmittal Memorandum pertaining to the Consolidated Financial Statement Report	

CHAPTER 2400 - AUDIT REPORT PREPARATION AND STANDARDSSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides the standards that the OIG Office of Audits (OA) will follow regarding audit report purpose, timeliness, distribution, and reporting. See Chapter 2410 (Report Organization and Processing), Chapter 2415 (Indexing and Independent Referencing), and Chapter 2420 (Non-Standard Audit Reports) for additional guidance on audit reports.
- 1-2. POLICY AND STANDARDS. The OA will prepare and issue audit reports in compliance with:
- a. Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States:
 - Chapter 4 (Reporting Standards for Financial Audits)
 - Chapter 5 (Reporting Standards for Attestation Engagements)
 - Chapter 7 (Reporting Standards for Performance Audits)
 - b. Office of Management and Budget (OMB) Bulletins, and
 - c. American Institute of Certified Public Accountants (AICPA) Statements on Auditing Standards.

SECTION 2. REPORTING STANDARDS

2-1. GENERAL. This section details the reporting standards to be followed and adhered to by the OIG Office of Audits.

- a. Purpose. Audit reports communicate audit results to appropriate officials.
- (1) To be effective, audit reports must be timely and available for use by all involved parties. Reports must be complete, accurate, objective, convincing, clear, and concise, in order to make audit results less susceptible to misunderstanding and available for public inspection.
 - (2) To be completely objective and fair, audit reports must include responsible official views and OIG evaluation of those views; noteworthy accomplishments; and actions requiring further study.
 - (3) When audits are terminated prior to completion, the audited entity and all other appropriate officials will be notified by memorandum. The memorandum will describe the reason for terminating the audit and any audit results. This memorandum should be documented in TeamMate.

b. Report Timeliness.

Final reports should be received by the Quality Assurance Group (QAG) no later than **10** months after the audit's entrance conference for the report to be considered timely. Once received by QAG, the report should be reviewed, edited by the preparing group, and signed by the AIGA within **1** month for the review process to be considered timely. Exceptions to the 10 month standard are highlighted below.

Any final report exceeding the time frames outlined in this policy will be considered untimely. It is critical that the audit staff clearly document all reasons for variances of actual time versus budgeted time and for instances of untimely reporting in the "time phased audit plan" work paper.

A. Timeliness of Report Preparation

- (1) In order to issue a timely final report, the suggested target for the issuance of the draft report is within four months of the entrance conference. This will allow sufficient time for a comprehensive auditee response, our evaluation of this response, and the preparation of the final report.

B. Timeliness of Report Review

(1) Once a report is delivered to QAG and the review process begins, there are several steps that the report typically goes through, as follows:

1. QAG review, then forwarded to AIGA or DAIGA.
2. AIGA/DAIGA review, then back to Group Chief with comments.
3. Group Chief addresses comments, then back to QAG.
4. QAG review, then to AIGA/DAIGA.
5. AIGA signs, or back to step 2 with additional comments.

(2) In order to meet the 1 month timeliness standard for the review phase, the following are the targets for total time for each party’s role in the process:

- QAG 14 days
- AIGA/DAIGA 10 days
- Preparing Group 7 days
- Total 31 days

c. Exceptions

The following are exceptions to the 10-month timeframe for timely report issuance:

A. Standard Exceptions

10-Month Standard Exceptions				
Audit Type	Months from Audit Entrance Conference			
	Draft to Carrier Target	Final Report to QAG	QAG/AIGA /DAIGA Review	Final Report Issued
BCBS Plan Claims only (ERAG)	3	9	1	10
System Specific FISMA (ISAG)	3	7	1	8
Special Limited Scope (ISAG)	3	7	1	8
RRAs (CRAG)	---	2	10 Business Days	2.5
CFC Audits (SAG)	3	8	1	9
Final Only (no Draft Issued) (All Groups)	---	6	1	7

Special/Multi-Plan/High-Risk Audits/Increased Scope (All Groups)	Audit/Reporting timeframe to be determined at the planning stage. Reporting timeframes that differ (+/-) from the standard 10 months must be discussed with and approved by the DAIGA and AIGA. A formal agreement must be prepared.
--	--

B. Draft Report Response Delays

If the auditee requests an extension of the time to respond to the draft report, the group chief may grant up to 30 additional days for the auditee to respond. If such an extension is granted, the due date for the final report may be extended up to 1 month, to 11 months from the entrance conference. However, any extension to when the final report will be submitted to QAG must be discussed with the DAIGA and documented. Documentation supporting the extension request and approval must be included in the work papers and submitted to QAG with the report.

C. Special Exceptions

In **rare** cases, an extended reporting period will be allowed if there is sufficient documentation to conclude that there are complexities or other unique circumstances that will require fieldwork and/or the reporting process to be more time-consuming than normal. To the extent that it will take longer than 10 months to prepare a final report, the group chief should document these reasons and the expected time required and submit this to the DAIGA for review and approval. **The expectation is that this will be necessary in very limited situations.**

d. Report Distribution. In general, each audit will result in the issuance of two reports: the draft audit report and the final audit report. For general distribution guidance see below. For specific reporting standards on financial reports see Section 2-2 and for performance audits see Section 2-3 of this chapter.

(1) Draft Audit Report. The audited entity and appropriate program agency official will be provided the draft audit report for written comment. For internal and CFC audits, the OIG will request written comments be provided within 30 days after issuing the CFC draft reports and internal draft reports. For insurance audits, the OIG will request written comments be provided within 90 days for comprehensive medical plan insurance audits, 60 days for limited scope audits (i.e., health benefit claims only) and 90 days for full scale audits for BlueCross BlueShield, Employee

Organizations, or other complex insurance audits, after issuing the draft report. Authority is delegated to the Group Chiefs to modify these requirements at their discretion.

- (2) Final Audit Report. The appropriate agency officials and those responsible for conducting follow up activity on audit report recommendations receive the final audit report. For all final reports, the OIG will request that the appropriate agency officials resolve all audit findings, including reaching agreement on actions to be taken on reported findings and recommendations, or, for findings with which the agency officials do not agree, the agency follow up official determines that the matter is resolved, within six months of the date of the report. In addition, the OIG should request that the follow up official provides a report describing the corrective action(s) taken, and the rationale for any findings in which the corrective action differs from the recommendation.
- (a) If the audited entity does not provide comments in a timely manner, or within any allotted extension of time, the final audit report may be issued without them. The final audit report must state that comments were requested and why they were not provided.
- (b) Final audit reports will generally be available to the public in accordance with the Freedom of Information Act (FOIA). However, auditors will not release any reports. All requests for audit reports will be handled in accordance with the policy and procedures in Chapter 2905 (Release of Official Information).
- (c) Distribution of reports depends on:
- the relationship of the auditors to the audited organization, and
 - the nature of the information contained in the report.

Audit organizations in government entities should distribute audit reports to:

- those charged with governance,
- to the appropriate officials of the audited entity, and
- to the appropriate oversight bodies or organizations requiring or arranging for the audits.

As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on audit findings and recommendations, and to others authorized to receive such reports.

Internal audit organizations in government entities may follow the Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing. Under GAGAS and IIA standards, the head of the internal audit organization should communicate results to parties who can ensure that the results are given due consideration. Public accounting firms contracted to perform an audit under GAGAS should clarify report distribution responsibilities with the engaging organization.

- 2-2. FINANCIAL REPORTING STANDARDS: The OIG will prepare audit reports in compliance with the AICPA reporting standards and the standards contained in GAGAS Chapter 4. In addition, the American Institute of Certified Public Accountants (AICPA) has established professional standards that apply to financial audit engagements for non-issuers performed by certified public accountants (CPA). For financial audits, GAGAS incorporate the AICPA field work and reporting standards and the related Statements on Auditing Standards (SAS) unless specifically excluded or modified by GAGAS. Also, the Public Company Accounting Oversight Board (PCAOB) has established professional standards that apply to financial audit engagements for issuers. Auditors may use GAGAS in conjunction with the PCAOB standards. Auditors must state in the auditor's report whether the financial statements are presented in accordance with generally accepted accounting principles (GAAP). Auditors must identify in the auditor's report those circumstances in which such principles have not been consistently observed in the current period in relation to the preceding period. When auditors determine that informative disclosures are not reasonably adequate, they must so state in the auditor's report. Auditors must either express an opinion regarding the financial statements, taken as a whole, or state that an opinion cannot be expressed, in the auditor's report. When the auditors cannot express an overall opinion, they should state the reasons therefore in the auditor's report. In all cases where the auditor's name is associated with financial statements, the auditors should clearly indicate the character of the auditors' work, if any, and the degree of responsibility the auditor is taking in the auditor's report.

The financial audit report is required to express a conclusion or opinion, or if circumstances require, disclaim an opinion on the data audited. There are four types of opinions. The opinion paragraph should be placed in the scope section of the report and

this section should also define any limitations on the scope of the audit. See Exhibit A of this Chapter for additional information.

- a. Unqualified Opinion. An unqualified opinion states that the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with generally accepted accounting principles (GAAP). Certain circumstances, while not affecting the auditors' unqualified opinion on the financial statements, may require that the auditors add an explanatory paragraph to the audit reports.
- b. Qualified Opinion. A qualified opinion states that, "except for", or "with the exception of" the effects of the matter(s) to which the qualification relates, the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP. When expressing a qualified opinion, substantive reasons must be disclosed in one or more separate explanatory paragraph(s) preceding the opinion. The opinion paragraph must include the appropriate qualifying language and a reference to the explanatory paragraph.
- c. Adverse Opinion. An adverse opinion states that the financial statements "do not present fairly" the financial position, results of operations, or cash flows of the entity in conformity with GAAP. Adverse opinions require a separate explanatory paragraph(s) preceding the opinion paragraph.
 - (1) All substantive reasons for the adverse opinion must be disclosed.
 - (2) The principal effects of the subject matter of the adverse opinion on the financial position, results of operations, and cash flows, if practicable, must be disclosed. The opinion will state whether these effects are not reasonably determinable.
 - (3) The opinion paragraph must include a direct reference to separate paragraph(s) that disclose the basis for the adverse opinion.
- d. Disclaimer of Opinion. A disclaimer of opinion states that the auditors "do not express" an opinion regarding the financial statements. This may be due to a scope limitation or because generally accepted auditing standards (GAAS) were not followed.
 - (1) If so, the audit report will disclose the reasons why the audit scope was limited or which GAAS were not followed and why.

- (2) Audit reports must disclose those circumstances that impact upon the fair presentation in conformity with GAAP. The specific procedures that were performed need not be identified.
- e. Statement on Compliance with Auditing Standards: Financial audits should include a statement that the audit was conducted in accordance with GAGAS. When auditors do not follow an applicable standard, this statement should be qualified.
 - f. Report on Compliance: A written report will include the results of audit tests of compliance with applicable laws, regulations, and provisions of contracts or grant agreements; or a reference to a separate report will be included as a separate section in the audit report. The report will identify those specific laws and regulations tested. The report should include all material instances of noncompliance. See Exhibit B of this Chapter for additional information.
 - (1) All material instances of noncompliance related to the entity's financial statements or the program, award, claim, fund, or group of accounts being audited should be reported. Other nonmaterial instances of noncompliance or abuse that have an effect on the financial statements or other financial data significant to the audit objectives need not be disclosed in the compliance report but should be reported in a separate written communication to the audited entity officials.
 - (2) The OA will promptly report all illegal acts to the Office of Investigations (OI). The OA and OI staff will consult with Special Counsel regarding the identification of illegal acts and their reporting in the audit report. See Chapter 2325 (Fraud, Illegal Acts, and Abuse), for further information.
 - g. Report on Internal Controls. The auditors should prepare a written report (or a separate section in the audit report) on their understanding of the entity's internal control structure and the assessment of control risk made as part of a financial statement audit. See Exhibit C of this Chapter and Chapter 2315 (Review of Internal Controls) for additional information.
 - (1) The internal control report should include:
 - (a) The scope of the auditor's testing in obtaining an understanding of the internal control structure and in assessing the control risk;

- (b) a description of the entity's significant internal controls established to ensure compliance with laws and regulations that have a material impact on the financial statements; and
 - (c) reportable conditions, including the identification of material weaknesses, resulting from audit work in understanding and assessing risk.
 - (2) The auditor may limit the consideration of the entity's internal control structure for a number of reasons, including, i) the entity's small size; ii) the auditors assessment that it would be inefficient to evaluate the internal control structure and that the audit would be more efficient by expanding substantive audit testing, and iii) the audit objectives did not require an understanding of the entity's internal control structure. The audit documentation will document these limiting conditions.
 - (3) An auditor may classify the internal control structure according to the entity's cycle of activity; financial statement captions; accounting applications; controls used in administering compliance with laws and regulations; or other appropriate classifications.
- h. Reporting and Findings: Written audit reports will provide the results. Auditors should plan and perform procedures to develop the elements of a finding. Findings are complete to the extent that the audit objectives are satisfied. Findings should contain the elements of criteria, condition, cause and effect (potential effect), when problems are found.
- (1) Criteria: The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.
 - (2) Condition: Condition is a situation that exists. The condition is determined and documented during the audit.
 - (3) Cause: The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions.

Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference.

- (4) Effect or potential effect: The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, “effect” is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

The report should contain conclusions when called for by the objectives. The audit work is complete when audit objectives are satisfied and the report clearly relates those objectives to the finding elements. When auditors detect deficiencies in internal control that are not significant, they should communicate those deficiencies separately in a management letter to officials of the audited entity unless the deficiencies are clearly inconsequential considering both quantitative and qualitative factors.

Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. To give the reader a basis for judging the prevalence and consequences of these findings, auditors should, as applicable, relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures, as appropriate. If the results cannot be projected, auditors should limit their conclusions appropriately.

In presenting findings such as deficiencies in internal control, fraud, illegal acts, violations of provisions of contracts or grant agreements, and abuse, auditors should develop the elements of the findings to the extent necessary to achieve the audit objectives. Clearly developed audit findings assist management or oversight officials of the audited entity in understanding the need for taking corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

Under AICPA standards, auditors may emphasize in the auditors' report significant matters regarding the financial statements. Due to the public interest in the operations of government entities and entities that receive or administer government awards, there may be situations in GAGAS audits in which certain types of information would help facilitate the readers' understanding of the financial statements and the auditors' report. These situations may be in addition to the examples presented in AICPA standards. Examples of matters that auditors may communicate in a GAGAS audit include the following:

- (1) Significant concerns or uncertainties about the fiscal sustainability of a government program or other matters that could have a significant impact on the financial condition or operations of the government entity beyond 1 year of the financial statement date. However, auditors are not responsible for designing audit procedures to detect such concerns or uncertainties, and any judgment about the future is based on information that is available at the time the judgment is made.
- (2) Unusual or catastrophic events that will likely have a significant ongoing or future impact on the entity's financial condition or operations.
- (3) Significant uncertainties surrounding projections or estimations in the financial statements.
- (4) Any other matter that the auditors consider significant for communication to users and oversight bodies in the auditors' report.

Determining whether to communicate such information in the auditors' report is a matter of professional judgment. The communication may be presented in a separate paragraph or separate section of the auditors' report and may include information that is not disclosed in the financial statements.

AICPA Professional Standards, AU Section 561, Subsequent Discovery of Facts Existing at the Date of the Auditor's Report, establish standards and provide guidance for situations when auditors become aware of new information that could have affected their report on previously-issued financial statements. Under AU Section 561, if auditors become aware of new information that might have affected their opinion on previously-issued financial statement(s), then the auditors should advise entity management to determine the potential effect(s) of the new information on the previously-issued financial statement(s) as soon as reasonably possible. Such new information may lead management to conclude that previously-issued financial statements were materially misstated and to

restate and reissue the misstated financial statements. In such circumstances, auditors should advise management to make appropriate disclosure of the newly discovered facts and their impact on the financial statements to those who are likely to rely on the financial statements.

Under GAGAS, auditors should advise management to make appropriate disclosures when the auditors believe that the following conditions exist:

- (1) it is likely that previously-issued financial statements are misstated and
- (2) the misstatement is or reasonably could be material.

Under GAGAS, auditors also should perform the following procedures related to restated financial statements:

- (1) evaluate the timeliness and appropriateness of management's disclosure and actions to determine and correct misstatements in previously-issued financial statements;
 - (2) report on restated financial statements; and
 - (3) report directly to appropriate officials when the audited entity does not take the necessary steps.
- i. Reporting Views of Responsible Officials: If the auditors' report discloses deficiencies in internal control, fraud, illegal acts, violations of provisions of contracts or grant agreements, or abuse, auditors should obtain and report the views of responsible officials concerning the findings, conclusions, and recommendations, as well as planned corrective actions.

Providing a draft report with findings for review and comment by responsible officials of the audited entity and others helps the auditors develop a report that is fair, complete, and objective. Including the views of responsible officials results in a report that presents not only the auditors' findings, conclusions, and recommendations, but also the perspectives of the responsible officials of the audited entity and the corrective actions they plan to take. Obtaining the comments in writing is preferred, but oral comments are acceptable.

When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and

provide a copy of the summary to the responsible officials to verify that the comments are accurately stated.

Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.

Obtaining oral comments may be appropriate when, for example, there is a reporting date critical to meeting a user's needs; auditors have worked closely with the responsible officials throughout the conduct of the work and the parties are familiar with the findings and issues addressed in the draft report; or the auditors do not expect major disagreements with findings, conclusions, and recommendations in the draft report, or major controversies with regard to the issues discussed in the draft report.

When the audited entity's comments are inconsistent or in conflict with findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence. If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.

- j. Privileged and Confidential Information: Auditors will consult with the Assistant Inspector General for Audits or Deputy Assistant Inspector General for Audits (**DAIGA**) and the **Office of Legal Affairs (OLA)** regarding material which is omitted from financial or performance audit reports due to its privileged or confidential nature. If auditors omit material, the audit report will cite the nature of the omission and reason for the omission. The auditors may issue a separate report and distribute it to only persons authorized to receive it. Evidence or indications of illegal acts shall not be reported in the audit report unless they are a matter of public record. The OA and OI staff will consult with OLA regarding questions of disclosure in audit reports. See 2905 (Release of Official Information) for additional guidance.

Considering the broad public interest in the program or activity under review assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate.

- k. Previously-Issued Financial Statements: Auditors should evaluate the timeliness and appropriateness of management's disclosure to those who are likely to rely on the financial statements and management's actions to determine and correct misstatements in previously-issued financial statements.

When management restates financial statements, auditors should perform audit procedures sufficient to reissue or update the auditors' report on the restated financial statements regardless of whether the restated financial statements are separately issued or presented on a comparative basis with those of a subsequent period. Auditors should include the following in an explanatory paragraph in the reissued or updated auditors' report:

- a. a statement disclosing that the previously-issued financial statements have been restated;
- b. a statement that the previously-issued auditors' report is not to be relied on because the previously-issued financial statements were materially misstated and the previously-issued auditors' report is replaced by the auditors' report on the restated financial statements; and,
- c. a reference to the note(s) to the restated financial statements that discusses the restatement.

Management's failure to include appropriate disclosures, in restated financial statements may have implications for the audit. In addition, auditors should include the omitted disclosures in the auditors' report, if practicable.

Auditors should notify those charged with governance if management (1) does not act in an appropriate time frame after new information was available to determine the financial statement effects of the new information and take the necessary steps

to timely inform those who are likely to rely on the financial statements and the related auditors' reports of the situation or (2) does not restate with reasonable timeliness the financial statements under circumstances in which auditors believe they need to be restated. Auditors should inform those charged with governance that the auditors will take steps to prevent further reliance on the auditors' report and advise them to notify oversight bodies and funding agencies that rely on the financial statements. If those charged with governance do not notify appropriate oversight bodies and funding agencies, then the auditors should do so.

2-3. PERFORMANCE AUDIT REPORTING STANDARDS: Written audit reports will be prepared to communicate the results of each performance audit. The reports shall be timely, complete, accurate, objective, and convincing. Audit reports will be as clear and concise as the subject matter permits.

a. OIG performance audit reports will ensure:

- (1) Proper reporting of audit results to appropriate officials;
- (2) clear understanding of the subject matter;
- (3) public availability of audit results; and
- (4) ease of follow-up action.

b. Findings and Conclusions: Performance audit reports will fully discuss findings and, where applicable, the auditor's conclusions.

- (1) Sufficient, competent, and relevant information about findings will be included to promote adequate understanding of the matters reported and provide convincing, but fair presentations in the proper perspective. The report should include the appropriate information, background, objectives, scope, and methodology needed by readers to understand the findings.
- (2) Auditors should plan and perform procedures to develop the elements of a finding. Findings are complete to the extent that the audit objectives are satisfied. Findings should contain the elements of criteria, condition, cause and effect (potential effect), when problems are found.

Criteria represent the laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated.

Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings, conclusions, and recommendations included in the report. Auditors should use criteria that are relevant to the audit objectives and permit consistent assessment of the subject matter.

Condition is a situation that exists. The condition is determined and documented during the audit.

The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference.

The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or consequences of the condition. When the audit objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the audit, “effect” is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

The report should contain conclusions when called for by the objectives. The audit work is complete when audit objectives are satisfied and the report clearly relates those objectives to the finding elements.

- c. Cause and Recommendations: Audit reports should include the cause of problem areas noted in the audit and recommendations for corrective actions which respond to the cause and improve operations.
 - (1) Audit reports should clearly discuss and identify the cause of problem areas and explain with applicable evidence the link between the problem and the factors identified as the cause.

- (2) The report should include constructive recommendations that are responsive to the problem, cost effective, and encourage adherence to applicable laws and regulations.
- d. Statement of Compliance with GAGAS: The scope section of the audit report will include the following statement, which represents an unmodified GAGAS compliance that the audit was made in accordance with Generally Accepted Government Auditing Standards:

“We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.”

An unmodified GAGAS compliance statement states that the auditor performed the audit engagement in accordance with GAGAS. Auditors should include an unmodified GAGAS compliance statement in the audit report when they have (1) followed all applicable unconditional and presumptively mandatory GAGAS requirements, or (2) have followed all unconditional requirements and documented justification for any departures from applicable presumptively mandatory requirements, and have achieved the objectives of those requirements through other means.

When auditors do not comply with all applicable GAGAS requirements, they should include a modified GAGAS compliance statement in the audit report. For performance audits, auditors should use a statement that includes either (1) the language in GAS 7.30, modified to indicate the standards that were not followed or (2) language that the auditor did not follow GAGAS.

A modified GAGAS compliance statement states that either (1) the auditor performed the audit engagement in accordance with GAGAS, except for specific applicable requirements that were not followed, or (2) because of the significance of the departure(s) from the requirements, the auditor was unable to and did not perform the audit or attestation engagement in accordance with GAGAS. Situations when auditors use modified compliance statements include scope limitations, such as restrictions on access to records, government officials, or other individuals needed to conduct the audit. When auditors use a modified GAGAS statement, they should disclose in the report the applicable requirement(s) not followed, the reasons for not following the

requirement(s), and how not following the requirements affected, or could have affected, the audit and the assurance provided.

- e. Compliance with Laws and Regulations: The audit report will disclose all significant instances of noncompliance. See Exhibit D of this chapter for additional information. Evidence or indications of illegal acts shall not be reported in the audit report unless they are a matter of public record. The OA should immediately report indications of illegal acts to the OI. The **OA** and **OI** staff will consult with **the OLA** regarding questions of disclosure in audit reports. See Chapter 2325 (Fraud, Illegal Acts, and Abuse) for additional information.
- f. Internal Controls: The audit report will identify the significant internal controls that were assessed. The report will identify the scope of the auditor's work and any significant weaknesses found during the audit. See Exhibit E of this chapter for additional information. When auditors detect deficiencies in internal controls that are not significant, they should communicate those deficiencies in a separate letter to officials of the audited entity unless the deficiencies are clearly inconsequential considering both qualitative and quantitative factors. Information systems controls are often an integral part of an entity's internal control. When obtaining an understanding of internal controls significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.
- g. Follow-Up Issues. The report should contain a statement on audit follow-up on significant findings and recommendations from previous audits that could have an effect on the current audit objectives or scope.
- h. Responsible Official Views: Pertinent views of audit officials should be obtained regarding audit report findings, conclusions, recommendations, and responsive corrective actions. The views should be reflected in the body of the report with verbatim comments attached as a separate addendum or appendix. Also, the report should include an evaluation of the comments, as appropriate. When the responsible official provides oral comments, they should be summarized and a copy provided to the official for verification of the facts. Oral comments may be appropriate due to time constraints or when the auditors do not expect major disagreements. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report if they find the comments valid and supported with sufficient evidence. If the audited entity refuses to provide comments or is unable to comment, the auditor may issue the report without receiving the comments from

the audited entity. This should be noted in the report. As appropriate, auditors will also seek the views of OPM and other interested officials. See Chapter 2215 (Managing the Audit) for additional information.

- i. Noteworthy Accomplishments: Any noteworthy accomplishments should be presented in the report.
- j. Issues Needing Further Study: Issues requiring further study and consideration should be discussed in the report.
- k. Privileged and Confidential Information: Omission of pertinent privileged or confidential information should be disclosed in the report. The nature of such information and the basis for its omission should be stated in the report. Omission of information should be discussed with the DAIGA and the OLA.

Considering the broad public interest in the program or activity under review assists auditors when deciding whether to exclude certain information from publicly available reports. When circumstances call for omission of certain information, auditors should evaluate whether this omission could distort the audit results or conceal improper or illegal practices.

When audit organizations are subject to public records laws, auditors should determine whether public records laws could impact the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate.

- 2-4. REPORTING STANDARDS FOR SPECIAL AUDIT REQUESTS: Special audit reports will address the specific objectives of the requestor. The scope will be limited to those audit tests which are necessary to meet the audit objectives and those limitations will be disclosed in the report. Audit results will be presented clearly and concisely and relate solely to the audit objectives and requestor's needs. The audit report format may be either a written memorandum or audit report depending upon the audit results and requestor's needs. Distribution will be limited to the requestor. Additional guidance on distribution should be sought from the DAIGA.
- 2-5. REPORTING STANDARDS FOR ATTESTATIONS: Attestations are written communications expressing a conclusion about the reliability of a written assertion that is the responsibility of another party. Examples of such written assertions are the Federal Employees' Health Benefits Program (FEHBP) Annual Accounting Statements filed by insurance carriers and contract proposals submitted in response to Requests for Proposals. There are two types of attestations: those in which OIG conducts an examination in accordance with GAGAS and those where the scope is limited to

agreed-upon procedures with another responsible party. See Exhibit F of this Chapter for additional information.

- a. For instances where the audit is conducted in conformity with GAGAS, OIG audit reports containing attestations will state:
 - (1) The assertion being reported and its character;
 - (2) OIG's conclusion about whether the assertion is presented in conformity with the stated criteria against which it was measured;
 - (3) OIG's reservations about the engagement and the presentation of the assertion; and intended use by specific parties under certain circumstances;
 - (a) When the criteria used to evaluate the subject matter are determined by the auditor to be appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria.
 - (b) When the criteria used to evaluate the subject matter are available only to specified parties.
 - (c) When reporting on subject matter and a written assertion has not been provided by the responsible party.
 - (d) When the report is on an attest engagement to apply agreed-upon procedures to the subject matter.
 - (4) For financial reports,
 - (a) identify the financial statements presented;
 - (b) state that the examination was made in accordance with GAS and provide a brief description of the nature of the examination;
 - (c) render an opinion that the financial statements were presented in conformity with the principles, standards, or criteria which govern the financial statements under review, such as the contract (for contract audits), GAAP, or Treasury guidelines **and** that any

- underlying assumptions provide a reasonable basis for the forecast or, if applicable, hypothetical assumptions projected;
- (d) if applicable, state that the prospective results may not be achieved, such as in a pre-award audit; and
 - (e) indicate that the OIG assumes no responsibility to update the report for events and circumstances after the date of the report.
- b. For agreed-upon procedure reports, the OIG will state:
- (1) If applicable, the prospective financial statements covered;
 - (2) the report is limited in use, intended solely for the specified users, and should not be used by others;
 - (3) the procedures performed;
 - (4) any reductions in the scope relative to GAGAS;
 - (5) a disclaimer on whether the presentation of prospective financial statements conform to GAGAS or AICPA presentation guidelines and on whether the underlying assumptions provide a reasonable basis for the forecast or projection;
 - (6) OIG's findings;
 - (7) the prospective results may not be achieved; and
 - (8) the OIG assumes no responsibility to update the report for events and circumstances after the date of the report.
- c. Compliance with American Institute of Certified Public Accountants (AICPA) Standards: Auditors performing attestation engagements in accordance with GAGAS should comply with the American Institute of Certified Public Accountants (AICPA) general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding statements on standards for attestation engagements (SSAEs).

- d. Use of AICPA and GAGAS Requirements: An attestation engagement can provide one of three levels of service as defined by the AICPA, namely an examination engagement, a review engagement, or an agreed-upon procedures engagement. Auditors performing an attestation engagement should determine which of the three levels of service apply to that engagement and refer to the appropriate AICPA standards and GAGAS requirements and considerations. (5.2)
- e. Citing Compliance with GAGAS in Attestation Reports: When auditors comply with all applicable GAGAS requirements for examination, review, or agreed upon procedures engagements, they should include a statement in the report that they performed the engagement in accordance with GAGAS. Because GAGAS incorporates by reference the AICPA's general attestation standard on criteria, the field work and reporting attestation standards, and the corresponding SSAEs, GAGAS does not require auditors to cite compliance with the AICPA standards when citing compliance with GAGAS. GAGAS does not prohibit auditors from issuing a separate report conforming only to the requirements of AICPA or other standards.
- f. Classified, Confidential, and Sensitive Information: Auditors will consult with the Assistant Inspector General for Audits or Deputy Assistant Inspector General for Audits (DAIGA) and the Office of Legal Affairs (OLA) regarding material which is omitted from financial or performance audit reports due to its privileged or confidential nature. If auditors omit material, the audit report will cite the nature of the omission and reason for the omission. The auditors may issue a separate report and distribute it to only persons authorized to receive it. Evidence or indications of illegal acts shall not be reported in the audit report unless they are a matter of public record. The OA and OI staff will consult with OLA regarding questions of disclosure in audit reports. See Chapter 2905 (Release of Official Information) for additional guidance.
- g. Distributing Attestation Reports: Auditors should document any limitation on report distribution. For GAGAS review engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. Auditors should document any limitation on report distribution. For GAGAS agreed-upon procedures engagements, if the subject matter or the assertion involves material that is classified for security purposes or contains confidential or sensitive information, auditors should limit the report distribution. See Chapter 2905 (Release of Official Information) for additional guidance.

- h. Additional Examination Reporting Standards: When performing GAGAS examination engagements, auditors should report, based upon the work performed, (1) significant deficiencies and material weaknesses in internal control; (2) instances of fraud and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance; (3) noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement; and (4) abuse that has a material effect on the subject matter or an assertion about the subject matter of the examination engagement. Auditors should include this information either in the same or in separate report(s). If auditors report separately (including separate reports bound in the same document) on the aforementioned items, they should state in the examination report that they are issuing those additional reports. They should include a reference to the separate reports and also state that the reports are an integral part of a GAGAS examination engagement.

In addition to the AICPA requirements concerning internal control, when performing GAGAS examination engagements, including attestation engagements related to internal control, auditors should include in the examination report all deficiencies, even those communicated early, that are considered to be significant deficiencies or material weaknesses.

When performing a GAGAS examination engagement, and auditors conclude, based on sufficient, appropriate evidence, that any of the following either has occurred or is likely to have occurred, they should include in their examination report the relevant information about:

- a) fraud and noncompliance with provisions of laws or regulations that have a material effect on the subject matter or an assertion about the subject matter and any other instances that warrant the attention of those charged with governance,
- b) noncompliance with provisions of contracts or grant agreements that has a material effect on the subject matter or an assertion about the subject matter, or
- c) abuse that is material to the subject matter or an assertion about the subject matter, either quantitatively or qualitatively.

- i. Presenting the Elements of a Finding: When performing a GAGAS examination engagement and presenting findings such as deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should develop the elements of the findings to the extent necessary. Clearly developed findings assist management or oversight officials of the audited entity in understanding the need for taking corrective action, and assist auditors in making recommendations for corrective action. If auditors sufficiently develop the elements of a finding, they may provide recommendations for corrective action.

Auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. Auditors should plan and perform procedures to develop the elements of a finding. Findings are complete to the extent that the audit objectives are satisfied. Findings should contain the elements of criteria, condition, cause and effect (potential effect), when problems are found.

- a) **Criteria:** The laws, regulations, contracts, grant agreements, standards, measures, expected performance, defined business practices, and benchmarks against which performance is compared or evaluated. Criteria identify the required or desired state or expectation with respect to the program or operation. Criteria provide a context for evaluating evidence and understanding the findings.
- b) **Condition:** Condition is a situation that exists. The condition is determined and documented during the engagement.
- c) **Cause:** The cause identifies the reason or explanation for the condition or the factor or factors responsible for the difference between the situation that exists (condition) and the required or desired state (criteria), which may also serve as a basis for recommendations for corrective actions. Common factors include poorly designed policies, procedures, or criteria; inconsistent, incomplete, or incorrect implementation; or factors beyond the control of program management. Auditors may assess whether the evidence provides a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference between the condition and the criteria.
- d) **Effect or potential effect:** The effect is a clear, logical link to establish the impact or potential impact of the difference between the situation that exists (condition) and the required or desired state (criteria). The effect or potential effect identifies the outcomes or consequences of the condition. When the

engagement objectives include identifying the actual or potential consequences of a condition that varies (either positively or negatively) from the criteria identified in the engagement, “effect” is a measure of those consequences. Effect or potential effect may be used to demonstrate the need for corrective action in response to identified problems or relevant risks.

- j. Reporting Fraud, Noncompliance with Provisions of Laws, Regulations, Contracts, or Grant Agreements, or Abuse to Parties Outside the Audited Entity: Auditors should report known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse directly to parties outside the audited entity in the following two circumstances:
- a) When entity management fails to satisfy legal or regulatory requirements to report such information to external parties specified in law or regulation, auditors should first communicate the failure to report such information to those charged with governance. If the audited entity still does not report this information to the specified external parties as soon as practicable after the auditors’ communication with those charged with governance, then the auditors should report the information directly to the specified external parties.
 - b) When entity management fails to take timely and appropriate steps to respond to known or likely fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse that (1) is likely to have a material effect on the subject matter or an assertion about the subject matter and (2) involves funding received directly or indirectly from a government agency, auditors should first report management’s failure to take timely and appropriate steps to those charged with governance. If the audited entity still does not take timely and appropriate steps as soon as practicable after the auditors’ communication with those charged with governance, then the auditors should report the entity’s failure to take timely and appropriate steps directly to the funding agency.

Auditors should comply with these requirements even if they have resigned or been dismissed from the engagement prior to its completion. Auditors should obtain sufficient, appropriate evidence, such as confirmation from outside parties, to corroborate assertions by management of the audited entity that it has reported such findings in accordance with laws, regulations, or funding agreements. When auditors are unable to do so, they should report such information directly.

- k. Reporting Views of Responsible Officials: When performing a GAGAS examination engagement, if the examination report discloses deficiencies in internal control, fraud, noncompliance with provisions of laws, regulations, contracts, or grant agreements, or abuse, auditors should obtain and report the views of responsible officials of the audited entity concerning the findings, conclusions, and recommendations, as well as any planned corrective actions. If the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors may issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.
- l. Responsible Officials' Comments: When auditors receive written comments from the responsible officials, they should include in their report a copy of the officials' written comments, or a summary of the comments received. When the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments and provide a copy of the summary to the responsible officials to verify that the comments are accurately stated. Auditors should also include in the report an evaluation of the comments, as appropriate. In cases in which the audited entity provides technical comments in addition to its written or oral comments on the report, auditors may disclose in the report that such comments were received.
- m. Evaluating the Validity of Comments: When the audited entity's comments are inconsistent or in conflict with the findings, conclusions, or recommendations in the draft report, or when planned corrective actions do not adequately address the auditors' recommendations, the auditors should evaluate the validity of the audited entity's comments. If the auditors disagree with the comments, they should explain in the report their reasons for disagreement. Conversely, the auditors should modify their report as necessary if they find the comments valid and supported with sufficient, appropriate evidence.
- n. Review Reports: The AICPA standards require that the auditors' review report be in the form of a conclusion expressed in the form of negative assurance.
- o. Agreed Upon Procedures Reports: The AICPA standards require that the auditors' report on agreed-upon procedures engagements be in the form of procedures and findings and specifies the required elements to be contained in the report.
- p. Statement on Limitations: Because reviews and GAGAS agreed-upon procedures engagements are substantially less in scope than audits and examination

engagements, it is important to include all required reporting elements contained in the SSAEs. For example, a required element of the review report is a statement that a review engagement is substantially less in scope than an examination, the objective of which is an expression of opinion on the subject matter, and accordingly, review reports express no such opinion. Furthermore, a required element of the report on agreed-upon procedures is a statement that the auditors were not engaged to and did not conduct an examination or a review of the subject matter, the objectives of which would be the expression of an opinion or limited assurance and that if the auditors had performed additional procedures, other matters might have come to their attention that would have been reported. Another required element is a statement that the sufficiency of the procedures is solely the responsibility of the specified parties and a disclaimer of responsibility for the sufficiency of those procedures. Including only those elements that the AICPA reporting standards for review or agreed-upon procedure engagements require or permit ensures that auditors comply with the AICPA standards and that users of GAGAS reports have an understanding of the nature of the work performed and the results of the review or agreed-upon procedures engagement.

- q. Departures from GAGAS: Any departures from the GAGAS requirements and the impact on the engagement and on the auditors' conclusions when the examination engagement is not in compliance with applicable GAGAS requirements due to law, regulation, scope limitations, restrictions on access to records, or other issues impacting the audit should be documented. This applies to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirement.

2-6. FEDERAL FINANCIAL STATEMENT AUDIT REPORTING STANDARDS. If the OIG conducts the financial statement audit, the OIG will prepare written audit reports to communicate the results of federal financial statement audits in compliance with Generally Accepted Accounting Standards (GAAS), GAS, and the supplemental provisions in OMB Bulletins. See Exhibit G of this chapter for additional information.

- a. The audit report shall be submitted to the agency head by the statutory due date for which the financial statements were prepared unless an earlier date is prescribed by the OMB.
- b. The audit report shall consist of at least the following three elements:

- (1) An opinion paragraph as to whether the entity's Principal Statements, including the Notes to the Principal Statements, and Combining Statements are fairly presented in all material respects.
 - (2) A report on internal controls which states that the auditor assessed and tested the entity's internal controls. The report shall provide the auditor's assurance on the internal control objectives and identify any reportable conditions and material weaknesses. See Exhibit G-2 of this chapter for an example of a report on internal controls.
 - a. Reportable conditions are matters coming to the auditor's attention that, in the auditor's judgment, should be communicated because they represent significant deficiencies in the design or operation of the internal control structure.
 - b. A material weakness in the internal control structure is a reportable condition in which the design or operation of one or more of the internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.
 - (3) A report on the reporting entity's compliance with applicable laws and regulations. See Exhibit G-3 of this chapter for an example of a report on compliance.
- c. In preparing the audit reports, the auditor should:
- 1) Determine materiality at the Combining Statements level.
 - 2) Report any other matters coming to his or her attention which meet the OMB criteria for materiality.
 - 3) Disclose the status of known but uncorrected significant findings and recommendations from prior audits that affect the current audit objectives.
 - 4) Disclose inconsistencies among the Overview of the Reporting Entity, the Principal Statements, the Combining Statements and the Supplemental Financial and Management Information.

- d. The reporting entity shall provide comments on the findings and recommendations in the audit report, including the plans for corrective action taken or planned, and comments on the status of corrective actions taken on prior findings
- e. Management Letter - If, in the auditor's judgment, it is necessary to communicate other conditions not included in the required audit reports, they should be separately communicated to the audited entity in a management letter.
- (1) A management letter is a formal letter prepared by the auditor which discusses findings and recommendations and suggestions for improvements in internal controls and other management issues that were identified during an audit and were not required to be included in the audit report.
 - (2) The letter may also expand on recommendations included in the audit report, but it cannot be used as a substitute for reporting matters in the audit report.
- f. Reports Prepared by Others. When federal financial statement audit reports are prepared by other auditors (i.e., Independent Public Accountants (IPA), KPMG, etc.), the Office of Audits will:
- (1) Ensure that all GAAS, GAS and supplemental provisions in OMB Bulletins are met. See Exhibit H of Chapter 2205 for the Consolidated Financial Statement Audit Report Checklist; and,
 - (2) Prepare the OIG transmittal letter. See Exhibit H of this chapter.
- g. Report Distribution. Copies of the audit report shall be distributed to the head of the department or agency reviewed and subsequently included in the Chief Financial Officer's (CFO) annual report. Audit organizations in government entities should distribute audit reports
- to those charged with governance,
 - to the appropriate officials of the audited entity, and
 - to the appropriate oversight bodies or organizations requiring or arranging for the audits.

As appropriate, auditors should also distribute copies of the reports to other officials who have legal oversight authority or who may be responsible for acting on audit findings and recommendations, and to others authorized to receive such

reports. Public accounting firms contracted to perform an audit under GAGAS should clarify report distribution responsibilities with the engaging organization.

- 2-7. FLASH AUDIT REPORT. If there are audit issues requiring immediate action they will be brought to the attention of the responsible official by use of a Flash Audit Alert (FAA). The FAA will be processed expeditiously and will be developed in accordance with Chapter 2420 (Non-Standard Audit Reports) of the OIG Audit Manual. This will permit corrective action to be taken before the draft or final audit reports are issued. Issuance of a FAA will be disclosed in the draft and final audit report.

EXHIBIT A-1

EXAMPLES OF AUDIT REPORT OPINIONSEXAMPLE OF AN UNQUALIFIED OPINION

We have audited the balance sheet of *(name of entity)* as of *(date)*, and the related statements of income, retained earnings, and cash flow for the year then ended. These financial statements are the responsibility of *(name of entity)* management. Our responsibility is to express an opinion on these financial statements based on our audit.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosure in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of *(name of entity)* as of *(date)*, and the results of its operations and cash flows for the year then ended in conformity with generally accepted government accounting principles.

EXHIBIT A-2

EXAMPLES OF AUDIT REPORT OPINIONSEXAMPLE OF A QUALIFIED OPINION

We have audited the balance sheet of *(name of entity)* as of *(date)*, and the related statements of income, retained earnings, and cash flow for the year then ended. These financial statements are the responsibility of *(name of entity)* management. Our responsibility is to express an opinion on these financial statements based on our audit.

Except as discussed in the following paragraph, we conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosure in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

We were not able to *(statement on the specific qualification to the opinion)*. In addition, we were unable to determine the validity of the accounts through alternative procedures.

In our opinion, except for the effects of the above adjustment, if any, as might have been determined to be necessary had we been able to determine the *(statement on the qualification)*, the financial statements referred to in the first paragraph above present fairly, in all material respects, the financial position of *(name of entity)* as of *(date)*, and the results of its operations and cash flows for the year then ended in conformity with generally accepted government accounting principles.

EXHIBIT A-3

EXAMPLES OF AUDIT REPORT OPINIONSEXAMPLE OF AN ADVERSE OPINION

We have audited the balance sheet of *(name of entity)* as of *(date)*, and the related statements of income, retained earnings, and cash flow for the year then ended. These financial statements are the responsibility of *(name of entity)* management. Our responsibility is to express an opinion on these financial statements based on our audit.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosure in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

As disclosed in Note **XXX** to the financial statements, management reports *(OIG will state the condition which results in the adverse opinion)*. In our opinion, generally accepted government accounting principles require *(OIG will state the applicable criteria)*. As a result of these departures from generally accepted government accounting principles, *(OIG will state the dollar effect on the item and total dollar effect on the financial statements)*.

In our opinion, because of the effects of the matters discussed in the preceding paragraph, the financial statements referred to above do not present fairly, in conformity with generally accepted government accounting principles, the financial position of *(name of entity)* as of *(date)* or the results of its operations and cash flows for the year then ended.

EXHIBIT A-4

EXAMPLES OF AUDIT REPORT OPINIONSEXAMPLE OF A DISCLAIMER

We were engaged to audit the accompanying balance sheet of *(name of entity)* as of *(date)*, and the related statements of income, retained earnings, and cash flow for the year then ended. These financial statements are the responsibility of *(name of entity)* management.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosure in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

(Explanatory paragraph - In this paragraph the reason(s) for disclaiming an opinion should be fully described. The paragraph should not describe any audit procedures performed.)

(Opinion paragraph - will refer to the scope limitation described in the explanatory paragraph and state explicitly that no opinion is expressed.) The accompanying balance sheet of *(name of entity)* as of *(date)*, and the related statements of income, retained earnings, and cash flows for the year then ended were not audited by us and, accordingly, we do not express an opinion on them.

EXHIBIT B-1

EXAMPLES OF COMPLIANCE FOR FINANCIAL AUDITS

As described in GAAS (AU § 801.25 & .28), the report on compliance should generally read as follows (as adapted for our environment):

EXAMPLE OF REPORT ON COMPLIANCE FOR FINANCIAL AUDITS WITH NO MATERIAL INSTANCES OF NONCOMPLIANCE

We have audited the (*description of what was audited*) of (*name of entity*) for the period (*dates covered by the audit*) and the results of our audit are presented in Section (*section where results of audit are reported*) herein. We conducted our audit in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States.

Compliance with the (*laws, regulations, and/or contracts*) applicable to (*name of entity audited*) is the responsibility of (*name of entity's management*). As part of our audit of the (*description of what was audited*), we performed tests of (*name of entity's*) compliance with certain provisions of (*identify the pertinent laws, regulations and/or contracts*). However, the objective of our audit of (*description of what was audited*) was not to provide an opinion on overall compliance with such provisions. Accordingly, we do not express such an opinion.

The results of our tests indicate that, with respect to the items tested, (*name of entity*) complied in all material respects, with the provisions referred to in the preceding paragraph.

EXHIBIT B-2

EXAMPLES OF COMPLIANCE FOR FINANCIAL AUDITSCOMPLIANCE REPORT FOR FINANCIAL AUDITS WITH MATERIAL INSTANCES OF NONCOMPLIANCE

We have audited the *(description of what was audited)* of *(name of entity)* for the period *(dates covered by the audit)* and the results of our audit are presented in Section *(section where results of audit are reported)* herein. We conducted our audit in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States.

Compliance with the *(laws, regulations, and (or contracts))* applicable to *(name of entity audited)* is the responsibility of *(name of entity)'s* management. As part of our audit of the *(description of what was audited)*, we performed tests of *(name of entity)'s* compliance with certain provisions of *(identify the pertinent laws, regulations and/or contracts)*. However, the objective of our audit of *(description of what was audited)* was not to provide an opinion on overall compliance with such provisions. Accordingly, we do not express such an opinion.

Material instances of noncompliance are failures to follow requirements, or violations of prohibitions, contained in *(statutes, regulations, or contracts)* that cause us to conclude that the aggregation of the misstatements resulting from those failures or violations is material to the *(description of what was audited)*. The result of our tests of compliance disclosed the following material instances of noncompliance, the effects of which have been reported in Section *(section where results of audit are reported)* herein.

(Describe the material instances of noncompliance noted.)

EXAMPLES OF INTERNAL CONTROLS FOR FINANCIAL AUDITS

FINANCIAL AUDIT - No reportable internal control conditions:

We have audited the (*description of what was audited e.g. financial statements, annual accounting statements, etc.*) of (*name of entity that was audited*) for the period (*dates covered by the audit*) and the results of our audit are presented in Section (*section where the results of audit are reported*) herein. We conducted our audit in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States.

In planning and performing our audit of (*description of what was audited*) of (*name of entity*) for the period (*dates covered by the audit*), we considered its internal control structure in order to determine our auditing procedures for the purpose of (*describe the purpose, e.g., evaluating the allowance, allocability, and reasonableness of charges or expressing an opinion on the financial statements, etc.*) and not to provide assurance on the internal control structure.

The management of (*name of entity*) is responsible for establishing and maintaining an internal control structure. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control structure policies and procedures. The objectives of an internal control structure are to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition and that transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of financial reports in accordance with (*state the appropriate criteria for maintaining financial reports for the audit subject e.g., generally accepted accounting principles or contract terms*). Because of inherent limitation in any internal control structure, errors or irregularities may nevertheless occur and not be detected. Also, projection of any evaluation of the structure to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or that the effectiveness of the design and operation of policies and procedures may deteriorate.

EXAMPLES OF INTERNAL CONTROLS FOR FINANCIAL AUDITS

For the purpose of this report, we have classified the significant internal control structure policies and procedures in the following categories (*identify internal control structure categories*).

For all of the internal control structure categories listed above, we obtained an understanding of the design of relevant policies and procedures and whether they have been placed in operation, and we assessed control risk. (*Note: This paragraph should be consistent with the work performed and be supported in the audit working papers.*)

Our consideration of the internal control structure would not necessarily disclose all matters in the internal control structure that might be material weaknesses. A material weakness is a condition in which the design or operation of one or more of the internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the (*describe what was audited*) being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving the internal control structure and its operation that we consider to be material weaknesses as defined above.

However, we noted certain other matters involving the internal control structure and its operation that we have reported to the management of (*name of entity*) in a separated letter dated (*date*). (*Include this paragraph when nonreportable, weaknesses are reported separately to the auditee.*)

EXAMPLES OF INTERNAL CONTROLS FOR FINANCIAL AUDITSFINANCIAL AUDIT - Internal control structure not relied on for Planning Purposes

We audited the (*description of what was audited e.g. financial statements, annual accounting statements, etc.*) of (*name of entity that was audited*) for the period (*dates covered by the audit*). The (*type of audit*) audit was conducted in accordance with generally accepted government auditing standards, issued by the Comptroller General of the United States.

To gain an understanding of the internal controls inherent in the (*description of what was audited*) of (*name of entity*) for the period (*dates covered by the audit*), we audited (*describe what was audited*) and we interviewed (*name of entity*) officials regarding the internal control structure. However, we did not consider the (*name of entity*) internal control structure in planning our auditing procedures. We determined that the audit could be accomplished more efficiently by performing substantive tests of the (*name of entity and description of what was audited*). We performed auditing procedures necessary to meet our audit objectives of verifying that the (*name of entity and description of what was verified*).

For the purpose of this report, we classified the significant internal controls in the following categories:

- (*Identify internal control structure categories*).

(*Name of entity*) management is responsible for establishing and maintaining internal controls and procedures which ensure compliance with applicable statutory and regulatory requirements. In addition, (*name of entity*) is responsible for ensuring accurate reporting to OPM. Because of inherent limitations in any internal control structure, errors or irregularities may nevertheless occur and not be detected. Also, projections of any evaluation of the structure to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or that the degree of compliance with the procedures may deteriorate.

Our audit, made for the limited purpose described above, would not necessarily disclose all material weaknesses in the system.

Accordingly, we do not express an opinion on the internal controls structure of the (*name of entity*), taken as whole. However, our audit showed that the (*name of entity*) did not have adequate controls to assure compliance with (*laws, regulations, and/or contracts*). The resulting deficiency and detrimental impact upon the (*describe program audited*) is described in detail in the "Audit Findings and Recommendations" section of this report.

EXHIBIT D-1

EXAMPLES OF COMPLIANCE FOR PERFORMANCE AUDITS

(Placed in the scope section of the audit report)

Example #1: For Experience-Rated Audits, Combined Federal Campaign Audits

We also conducted tests to determine whether the Plan had complied with the contract, the applicable procurement regulations (i.e., Federal Acquisition Regulations and Federal Employees Health Benefits Acquisition Regulations, as appropriate), and the laws and regulations governing the FEHBP. The results of our tests indicate that, with respect to the items tested, the Plan did not comply with all provisions of the contract and federal procurement regulations. Exceptions noted in the areas reviewed are set forth in detail in the "Audit Findings and Recommendations" section of this audit report. With respect to the items not tested, nothing came to our attention that caused us to believe that the Plan had not complied, in all material respects, with those provisions.

Example #2: For Community-Rated Audits

Our audits of community-rated carriers are designed to test carrier compliance with the FEHBP contract, applicable laws and regulations, and OPM rate instructions, and to provide reasonable assurance of detecting errors, irregularities, and illegal acts.

Example # 3: For Information Systems Audits

In conducting the audit, we performed tests to determine whether (*Name of audited entity*) practices were consistent with applicable standards. While generally compliant, with respect to the items tested, (*Name of audited entity*) was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

EXAMPLES OF INTERNAL CONTROLS FOR PERFORMANCE AUDITS
(Placed in the scope section of the audit report)

PERFORMANCE AUDIT: Where assessment was not made.

Example #1: For Experience-Rated Audits, Combined Federal Campaign Audits

In planning and conducting our audit, we obtained an understanding of the Plan's internal control structure to help determine the nature, timing, and extent of our auditing procedures. This was determined to be the most effective approach to select areas of audit. For those areas selected, we primarily relied on substantive tests of transactions and not tests of controls. Based on our testing, we did not identify any significant matters involving the Plan's internal control structure and its operation. However, since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the Plan's system of internal controls taken as a whole.

Example # 2: For Community-Rated Audits

We obtained an understanding of the Plan's internal control structure, but we did not use this information to determine the nature, timing, and extent of our review procedures. However, the audit included such tests of the Plan's rating systems and such other auditing procedures considered necessary under the circumstances. Our review of internal controls was limited to the procedures the Plan has in place to ensure that:

- The appropriate similarly sized subscriber groups (SSSGs) are selected;
- the rates charged the FEHBP are the market price rates (i.e., equivalent to the best rate offered to SSSGs); and
- the loadings to the FEHBP rates are reasonable and equitable.

EXAMPLES OF INTERNAL CONTROLS FOR PERFORMANCE AUDITS

(Placed in the scope section of the audit report)

Example # 3: For Information Systems Audits

Our performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of the *(Name of audited entity)* internal controls through interviews, observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of *(Name of audited entity)* internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective. We audited the confidentiality, integrity, and availability of *(Name of audited entity)* computer-based information systems used to process FEHBP claims and found that there are opportunities for improvement in the information systems' internal controls. These areas are detailed in the "Audit Findings and Recommendations" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the *(Name of audited entity)*'s system of internal controls taken as a whole.

EXAMPLES OF INTERNAL CONTROLS FOR PERFORMANCE AUDITS

PERFORMANCE AUDIT: Where assessment was made.

We have assessed selected internal controls used by *(name of entity audited and description of what was audited)*. We conducted this audit in accordance with generally accepted government auditing standards for performance audits issued by the Comptroller General of the United States. These standards require that we assess internal controls when necessary to satisfy the audit objectives.

(Name of entity audited) is responsible for establishing and maintaining an internal control structure for administering *(describe program)*. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control structure policies and procedures. The objectives of an internal control structure are to provide management with reasonable, but not absolute, assurance that transactions are executed in accordance with management's authorization and applicable laws, regulations, policies, and procedures. Because of inherent limitations in any internal control structure, errors or irregularities may nevertheless occur and not be detected.

For the purpose of this audit, our review of internal controls focused on those controls designed to deter and/or detect fraud, errors, and irregularities in the *(description of what was audited)*.

We noted certain matters involving the internal controls and their operation that we consider to be conditions we must report under our auditing standards. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal controls that, in our judgment, could adversely affect *(name of entity audited and description of what was audited)*. We have reported these matters in Section *(section where results of audit are reported)* of this audit report.

EXAMPLES OF INTERNAL CONTROLS FOR PERFORMANCE AUDITS

A material weakness is a reportable condition in which the design or operation of one or more internal control structure elements does not reduce to a relatively low level the risk that errors or of irregularities that would be material in relation to the area being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of the internal controls would not necessarily disclose all matters in the internal control structure that might be reportable and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses as defined above. However, we believe none of the reportable conditions described in Section (*section where results of audit are reported*) of this report are material weaknesses.

EXHIBIT F-1

EXAMPLES OF ATTESTATION REPORTS

As described in the AICPA Attestation Standards (AT § 100.58), the below wording should generally be used when reporting on an attestation engagement.

ATTESTATION REPORT - When work is not sufficient to express an opinion:

We have reviewed the accompanying *(identify what was reviewed, e.g. the annual accounting statement for the years ended December 31, 20XX, 20XX, and 20XX)* for *(name of entity)*. Our review was conducted in accordance with the generally accepted government auditing standards issued by the Comptroller General of the United States. Our review was made during the period *(dates)* at *(location)*.

A review is substantially less in scope than an audit. Accordingly, we do not express an opinion on the accompanying *(identify what was reviewed)* taken as a whole. The purpose of our review was to determine whether the *(identify what was reviewed)* were prepared in accordance with the requirements of *[identify the presentation criteria, e.g. the contract number XXX between the U. S. Office of Personnel Management and (name of entity)]*.

(Additional paragraph(s) may be added to emphasize certain matters related to the attest engagement or the presentation of assertions.)

Based on our review, we conclude that the *(identify what was audited)* differs materially *(if appropriate, otherwise delete the word "materially")* from that which would have been presented if the criteria specified in *(e.g. contract number XXX)* had been followed. Our review findings are detailed in Section **XX** of this report.

EXHIBIT F-2

EXAMPLES OF ATTESTATION REPORTSEXAMPLE OF AGREED-UPON PROCEDURES REPORT

We have applied the procedures enumerated below to the accompanying **XXX** for the year ended 20**XX**. These procedures, which were agreed to by **XXX**, were performed solely to assist you in determining.... This report is intended solely for your information and should not be used by those who did not participate in determining the procedures. Our procedures were as follows:

(OIG auditors will write a paragraph on the specific procedures which were used during the review.)

Because the above procedures do not constitute an audit conducted in accordance with generally accepted government auditing standards, we do not express an opinion on **XXX** referred to above.

Based on the application of the procedures referred to above, nothing came to our attention that caused us to believe that the accompanying **XXX** is not presented in conformity with the measurement criteria as required by **XXX**. Had we performed additional procedures or had we conducted an audit of the **XXX** in accordance with generally accepted Government Auditing Standards, other matters might have come to our attention that would have been reported to you. This report relates only to **XXX** specified above and does not extend to any financial statements of XYZ Company taken as a whole.

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTSReport on Principal Statements and Combining Statements

We have audited the Principal Statements, the Notes to the Principal Statements, and Combining Statements contained in the Annual Financial Statements of the XYZ Revolving Fund of the ABC Agency as of and for the year ended September 30, 20XX. These Statements are the responsibility of the Agency's management. Our responsibility is to express an opinion on these Statements based on our audit.

We conducted our audit in accordance with generally accepted auditing standards, generally accepted government auditing standards, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 9X-XX, Audit Requirements for Federal Financial Statements. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the Principal Statements, including the Notes to the Principal Statements, and Combining Statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in these Statements, including the Notes thereto. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall Statement presentation. We believe that our audit provides a reasonable basis for our opinion.

Accounting principles are currently being studied by the Federal Accounting Standards Advisory Board. Generally accepted accounting principles for Federal entities are to be promulgated by the Comptroller General and the Director of the Office of Management and Budget, based on advice from the Board. In the interim, Federal agencies are to follow the applicable accounting standards contained in agency accounting policy, procedures, manuals, and/or related guidance. The summary of significant accounting policies included in the Notes to Principal Statements describes the accounting standards prescribed by the ABC Agency Financial manual and used to prepare the financial statements. Note X discloses the differences between these accounting

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTS

standards and Title 2 of GAO Policy and Procedures Manual for Guidance of Federal Agencies.

In our opinion, the Principal Statements, including the Notes to the Principal Statements, referred to above present fairly, in all material respects, the assets, liabilities and net financial position of the XYZ Revolving Fund of the ABC Agency as of September 30, 20XX, and the results of its operations, cash flows (or changes in financial position) and reconciliation to budget for the year then ended, in accordance with the accounting standards described in Note X. Also, in our opinion, the Combining Statements present fairly the assets, liabilities, and equity of the individual funds comprising the XYZ Revolving fund, and the results of operations, cash flow, and the reconciliation to budget, as of and for the year ended September 30, 20XX.¹

Our audit was conducted for the purpose of forming an opinion on the Principal and Combining statements described above. We have reviewed the financial information presented in management's Overview of XYZ Revolving Fund and in the Supplemental Financial and Management Information section. The information presented in the Overview and Supplemental Financial and Management Information sections are presented for the purposes of additional analysis. Such information has not been audited by us and, accordingly, we do not express our opinion on this information. This information is addressed, however, in our auditor report on compliance in accordance with Section 6.a. (3), (4) and (5) of OMB Bulletin No. 9X-XX.

¹ If the auditor does not apply procedures to the combining Statements as extensive as would be necessary to express an opinion on the information taken by itself, this sentence should be deleted. The Combining Statements would then be considered information accompanying the Principal Statements and the audit would report on them as follows:

"The Combining Statements are presented for purposes of additional analysis and are not a required part of the Principal Statements. Such information has been subjected to the auditing procedures applied in the audit of the Principal Statements and, in our opinion, is fairly stated in all material respects in relation to the Principal Statements taken as a whole."

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTSReport on Internal Control

We have audited the Principal and Combining Statements of the XYZ Revolving Fund of the ABC Agency as of and for the year ended September 30, 20XX, and have issued our report thereon dated (*month, day, and year*).

We conducted our audit in accordance with generally accepted auditing standards, generally accepted government auditing standards, issued by the Comptroller General of the United States, and the Office of Management and Budget (OMB) Bulletin No. 9X-XX, Audit Requirements for Federal Financial Statements. Those standards require that we plan and perform the audit to obtain reasonable assurance that the Principal and Combining Statements are free of material misstatements.

In planning and performing our audit of the Principal and Combining Statements of the XYZ Revolving Fund of the ABC Agency for the year ended September 30, 20XX, we considered its internal control structure. The purposes of this consideration were to: (i) determine our auditing procedures for the purpose of expressing our opinion on the Principal and Combining Statements; and (ii) to determine whether the internal control structure meets the objectives identified in the preceding paragraph. This included obtaining an understanding of the internal control policies and procedures and assessing the level of control risk relevant to all significant cycles, classes of transactions, or account balances; and for those significant control policies and procedures that have been properly designed and placed in operation, performing sufficient tests to provide reasonable assurance that the controls are effective and working as designed.

Management of the XYZ Revolving Fund is responsible for establishing and maintaining an internal control structure. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control structure policies and procedures. The objective of an internal control structure are to provide management with reasonable but not absolute assurance that obligations and costs are in compliance with applicable laws; funds, property, and other assets are safeguarded against

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTS

waste, loss, unauthorized use, or misappropriation; and revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports to maintain accountability over assets.

For the purpose of this report, we have classified the significant internal control structure policies and procedures into the following categories: *(identify internal control structure categories)*.

Our consideration of the internal control structure included all of the categories listed above except that we did not consider the accounting over *(identify any category not evaluated)* because *(state reason for excluding any category from the evaluation)*.

We noted certain matters involving the internal control structure and its operations that we consider to be reportable conditions under standards established by the American Institute of Certified Public Accountants and OMB Bulletin No. 9X-XX. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the organization's ability to ensure that obligations and costs are in compliance with applicable law; funds, property and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports in accordance with applicable accounting standards and to maintain accountability over the assets. *(Include paragraphs describing reportable conditions noted).*²

2 After describing the reportable conditions add the following statement. "Except for the matters noted above, we believe there is reasonable assurance that the control structure meets the internal control objectives." When the reportable conditions or material weaknesses are of sufficient magnitude to preclude the auditor from providing reasonable assurance this sentence should be deleted.

If there are no reportable conditions, replace the previous paragraph that defines reportable conditions and subsequent three paragraphs with the following two paragraphs:

"Our consideration of the internal control structure would not necessarily disclose all matters in the internal control structure that might be material weaknesses under standards established by the American Institute of Certified Public Accountants and OMB Bulletin No. 9 X-XX. A material weakness is a reportable condition in which the design or operation of one or more of the specific internal control structure elements does not reduce to a relatively low level the risk that error or irregularities in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving the internal control structure and its operation that we consider to be material weaknesses as defined above. Therefore, we believe there is reasonable assurance that the internal control objectives were achieved."

If a management letter is issued when there were no reportable conditions, the following paragraph should be added.

"However, we noted certain matters involving the internal control structure and its operation that we have reported to the management of XYZ Revolving Fund of the ABC Entity in a separate letter dated *(month, day, and year)*."

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTS

- (1) A material weakness is a reportable condition in which the design or operation of the specific internal control structure elements does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the Statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of the internal control structure would not necessarily disclose all matters in the internal control structure that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses as defined above. However, we believe none of the reportable conditions described above is a material weakness.³

We also noted other matters involving the internal control structure and its operation that we have reported to the management of the XYZ Revolving Fund of the ABC Entity in a separate letter dated (*month, day, and year*).

³ If any of the reportable conditions are considered material weaknesses, this sentence would be replaced with the following:

"We believe the conditions reported in the (*list which paragraphs*) previous paragraphs are material weaknesses as defined in the immediately previous paragraphs."

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTSReport on Compliance

We have audited the Principal and Combining Statements of the XYZ Revolving Fund of the ABC Agency as of and for the year ended September 30, 20XX, and have issued our report thereon dated (*month, day, and year*).

We conducted our audit in accordance with generally accepted auditing standards issued by the Comptroller General of the United States, and the Office of Management and Budget (OMB) Bulletin No. 9X-XX, Audit Requirements for Federal Financial Statements. Those standards require that we plan and perform the audit to obtain reasonable assurance that the Principal and Combining Statements are free of material misstatements.

Compliance with laws and regulations applicable to the XYZ Revolving Fund is the responsibility of ABC Agency's management. As part of obtaining reasonable assurance about whether the Principal and Combining Statements are free of material misstatement, we tested compliance with laws and regulations that may directly affect the financial statements and certain other laws and regulations designated by OMB and ABC Agency (*list the laws and regulations tested*). As part of our audit, we reviewed management's process for evaluating and reporting on internal control and accounting systems as required by the Federal Managers' Financial Integrity Act (FMFIA) and compared the agency's most recent FMFIA reports with the evaluation we conducted of the entity's internal control system. We also reviewed and tested the entity's policies, procedures, and systems for documenting and supporting financial, statistical, and other information presented in the Overview of the Reporting Entity and Supplemental Financial and Management Information. However, our objective was not to provide an opinion on overall compliance with such provisions.

EXAMPLES OF FEDERAL FINANCIAL STATEMENT AUDIT REPORTS

The results of our tests indicate that with respect to the items tested, XYZ Revolving Fund complied in all material respects with the provisions referred to in the preceding paragraph.⁴

-
- 4 If the auditor's testing of compliance with laws and regulations identifies material instances of noncompliance with laws and regulations, the following paragraph should be included:

"Material instances of noncompliance are failures to follow requirements, or violations of prohibitions, contained in law or regulations that cause us to conclude that the aggregation of the misstatements resulting from those failures or violations is material to the Principal and Combining Statements or the sensitivity of the matter would cause it to be perceived as significant by others. The results of our tests of compliance disclosed the following instances of noncompliance, the effects of which have been corrected in the XYZ Revolving Fund's **20XX** Principal and Combining Statements."

(Include paragraphs describing the material instances of noncompliance noted).

"We considered these material instances of noncompliance in forming our opinion on whether the Principal and Combining Statements are presented fairly, in all material respects, in conformity with the applicable accounting standards now in affect for the preparation of the entity's financial statements and this report does not effect our report dated (*month, day, and year*) on the Principal and Combining Statements."

"Except as described above, the results of our tests of compliance indicate that, with respect to the items tested, the XYZ Revolving Fund of the ABC Agency complied, in all material respects, with the provisions referred to in the third paragraph of this report."

EXHIBIT H

Consolidated Financial Statement Audit Report Checklist

Instructions: This checklist is a tool for evaluating audit reports for the consolidated financial statement audit. The checklist is largely based on FAM 650. Each question should be marked N/A, Yes, or No. The Ref./Comment can be used to provide an explanation or a workpaper reference. The checklist is meant to be an aid to the auditor in considering FAM and other requirements.

N/A Yes No Ref./Comment

1. Was the report dated at the end of fieldwork? (FAM 650.48)
2. Is the audit report addressed to the proper official?
3. Did

Report No. XX-XX-XX-XX-XXX

MEMORANDUM FOR XXXXXX XXXXXXXXX

Deputy Director

FROM: PATRICK E. McFARLAND

Inspector General

SUBJECT: Audit of the Office of Personnel Management's Fiscal Year
20XX Consolidated Financial Statements

This memorandum transmits KPMG LLP's (KPMG) report on its financial statement audit of the Office of Personnel Management's (OPM) Fiscal Year 20XX Consolidated Financial Statements and the results of the Office of the Inspector General's (OIG) oversight of the audit and review of that report. OPM's consolidated financial statements include the Retirement Program, Health Benefits Program, Life Insurance Program, Revolving Fund Programs (RF) and Salaries & Expenses funds (S&E).

Audit Reports on Financial Statements, Internal Controls and Compliance with Laws and Regulations

The Chief Financial Officers (CFO) Act of 1990 (P.L. 101-576) requires OPM's Inspector General or an independent external auditor, as determined by the Inspector General, to audit the agency's financial statements in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States. We contracted with the independent certified public accounting firm KPMG LLP to audit OPM's consolidated financial statements as of September 30, 20XX and for the fiscal year then ended. The contract requires that the audit be performed in accordance with generally accepted government auditing standards and the Office of Management and Budget (OMB) bulletin number 07-04, *Audit Requirements for Federal Financial Statements*. KPMG's audit report for Fiscal Year 20XX includes: (1) opinions on the consolidated financial statements and the individual statements for the three benefit programs, (2) a

Report No. XX-XX-XX-XX-XXX

MEMORANDUM FOR XXXXXX XXXXXXXXX

Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Audit of the Office of Personnel Management's Fiscal Year
20XX Consolidated Financial Statements

This memorandum transmits KPMG LLP's (KPMG) report on its financial statement audit of the Office of Personnel Management's (OPM) Fiscal Year 20XX Consolidated Financial Statements and the results of the Office of the Inspector General's (OIG) oversight of the audit and review of that report. OPM's consolidated financial statements include the Retirement Program, Health Benefits Program, Life Insurance Program, Revolving Fund Programs (RF) and Salaries & Expenses funds (S&E).

Audit Reports on Financial Statements, Internal Controls and Compliance with Laws and Regulations

The Chief Financial Officers (CFO) Act of 1990 (P.L. 101-576) requires OPM's Inspector General or an independent external auditor, as determined by the Inspector General, to audit the agency's financial statements in accordance with Government Auditing Standards (GAS) issued by the Comptroller General of the United States. We contracted with the independent certified public accounting firm KPMG LLP to audit OPM's consolidated financial statements as of September 30, 20XX and for the fiscal year then ended. The contract requires that the audit be performed in accordance with generally accepted government auditing standards and the Office of Management and Budget (OMB) bulletin number 07-04, *Audit Requirements for Federal Financial Statements*.

KPMG's audit report for Fiscal Year 20XX includes: (1) opinions on the consolidated financial statements and the individual statements for the three benefit programs, (2) a

XXXXX XXXXXXXXX

report on internal controls, and (3) a report on compliance with laws and regulations. In its audit of OPM, KPMG found:

- The consolidated financial statements were fairly presented, in all material respects, in conformity with generally accepted accounting principles.
- There were no material weaknesses identified in the internal controls. A material weakness is a condition in which the design or operation of an internal control does not reduce to a relatively low level the risk that misstatements, in amounts that would be material in relation to the financial statements being audited, may occur and not be detected within a timely period.

However, KPMG's report did identify two significant deficiencies:

- Information systems general control environment, and
- Financial management and reporting processes of the Office of the Chief Financial Officer (OCFO). (Revolving Fund Program (RF Program) and Salaries and Expenses (S&E) Fund)

A significant deficiency represents a deficiency in the design or operation of internal controls that could adversely affect OPM's ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements.

- KPMG's report on compliance with certain provisions of laws and regulations disclosed one other matter related to the Federal Financial Management Improvement Act of 1996 (FFMIA) (RF and S&E only).

OIG Evaluation of KPMG's Audit Performance

In connection with the audit contract, we reviewed KPMG's report and related documentation and made inquiries of its representatives regarding the audit. To fulfill our audit responsibilities under the CFO Act for ensuring the quality of the audit work performed, we conducted a review of KPMG's audit of OPM's Fiscal Year 20XX Consolidated Financial Statements in accordance with GAS. Specifically, we:

- reviewed KPMG's approach and planning of the audit;
- evaluated the qualifications and independence of its auditors;
- monitored the progress of the audit at key points;
- examined its working papers related to planning the audit and assessing internal controls over the financial reporting process;

XXXXX XXXXXXXXX

- reviewed KPMG’s audit reports to ensure compliance with Government Auditing Standards;
- coordinated issuance of the audit report; and
- performed other procedures we deemed necessary.

Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, opinions on OPM’s financial statements or internal controls or on whether OPM’s financial management systems substantially complied with FFMIA or conclusions on compliance with laws and regulations. KPMG is responsible for the attached auditor’s report dated November 14, 20XX, and the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply, in all material respects, with the generally accepted GAS.

In accordance with the OMB Circular A-50 and Public Law 103-355, all audit findings must be resolved within six months of the date of this report. In order to ensure audit findings are resolved within the required six-month period, we are asking that the OCFO respond directly to the OIG within 90 days of the date of this report advising us whether they agree or disagree with the audit findings and recommendations. As stated in OMB Circular A-50, where agreement is indicated, the OCFO should describe planned corrective action. If the OCFO disagrees with any of the audit findings and recommendations, they need to explain the reason for the disagreement and provide any additional documentation that would support their opinion.

In closing, we would like to congratulate OPM’s financial management staff for once again issuing the consolidated financial statements by the November 15 due date. Their professionalism, courtesy, and cooperation allowed us to overcome the many challenges encountered during OPM’s preparation, KPMG’s audit, and the OIG’s oversight of the financial statement audit this year. If you have any questions about KPMG’s audit or our oversight, please contact me or have a member of your staff contact Michael R. Esser, Assistant Inspector General for Audits, at 606-XXXX.

cc: Dennis Coleman
Chief Financial Officer

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2410

Report Organization and Processing

CHAPTER 2410 - REPORT ORGANIZATION AND PROCESSING

CONTENTS

	<u>Page</u>
 SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy and Standards.....	1
 SECTION 2. REPORT ORGANIZATION AND FORMAT	
2-1. General.....	2
2-2. Organization and Format	2
2-3. Transmittal Memorandum Accompanying Draft Reports for Internal Audits	2
2-4. Transmittal Letter Accompanying Draft Reports for External Audits	3
2-5. Transmittal Memorandum Accompanying Final Reports	4
2-6. Report Cover.....	5
2-7. Executive Summary	6
2-8. Abbreviations.....	6
2-9. Contents	7
 SECTION 3. REPORT PROCESSING	
3-1. General.....	13
3-2. Records Management Requirements	13
3-3. Document Flow and Processing.....	13
3-4. Policies and Procedures for Placing the Final Audit Reports on the OIG Webpage.....	14

SECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides guidelines concerning audit report organization, format, and processing. Exhibits of suggested audit report contents are also provided. See Chapter 2400, Audit Report Preparation and Standards; Chapter 2415, Indexing and Independent Referencing; and Chapter 2420, Non-Standard Audit Reports, for additional information.
- 1-2. POLICY AND STANDARDS. The OIG Office of Audits (OA) will issue audit reports in accordance with the Government Auditing Standards (GAS) issued by the Comptroller General of the United States and other regulatory or statutory reporting requirements.

SECTION 2. REPORT ORGANIZATION AND FORMAT

- 2-1. GENERAL. This section details the organization and format to be followed by the OIG Office of Audits for standard, long form draft and final audit reports. These guidelines generally follow GAS requirements and should be adapted as the circumstances may dictate, to type of audit, the particular audit objectives, or the particular auditing standards that pertain to the subject audit objectives. Audit report formats for several non-standard type audit reports, such as letter reports, appear in Chapter 2420 (Non-Standard Audit Reports) of the OPM OIG Audit Manual.
- 2-2. ORGANIZATION AND FORMAT. Report organization and format will generally change slightly from the draft audit report to the final audit report. For internal audits, a transmittal memorandum will accompany the draft audit report and final audit report. For external audits, a transmittal letter will accompany the draft audit report, and a transmittal memorandum will accompany the final audit report. Each page of the draft audit report, including the cover, exhibits, and appendices, will be marked “**THIS DRAFT IS RESTRICTED FOR OFFICIAL USE ONLY,**” or if this marking is not practical, a “draft” stamp may be used. Some modifications to the formats discussed below may be required to accommodate unusual conditions.
- 2-3. TRANSMITTAL MEMORANDUM ACCOMPANYING DRAFT REPORTS FOR INTERNAL AUDITS. A transmittal memorandum on official letterhead will be sent to the appropriate OPM program official, if applicable to the group. The primary purpose of the transmittal memorandum is to provide a summarized overview of the audit performed and to solicit comments regarding the audit findings and recommendations. The memorandum may also disclose information not included in the draft audit report such as confidential information or potential illegal acts, etc. See Exhibit A of this chapter for an example of a transmittal memorandum. The information required in the transmittal memorandum will vary depending on the type of audit and its objective. Care should be taken to modify the suggested format when necessary for a particular audit situation.
- (1) The opening paragraph(s) will contain the audited entity’s name and location and/or subject, years under audit, and reference that a report is attached.
 - (2) The middle paragraphs will concisely state the audit results, including any dollars questioned and any privileged information. This paragraph may also convey confidential information to OPM program officials on external audits.
 - (3) The next to last paragraph should discuss the Freedom of Information Act and the necessity for an accurate audit report. The paragraph should also state that in our opinion, draft audit reports are not available to the public under terms of the Freedom

of Information Act.

- (4) The closing paragraph(s) will indicate that comments must be received no later than 30 days for internal draft audit reports or a date determined at the discretion of the Group Chief. Also, the last paragraph should indicate that either the Group Chief or an alternatively named knowledgeable individual is available to discuss the report further (applicable telephone numbers should be included).

2-4. TRANSMITTAL LETTER ACCOMPANYING DRAFT REPORTS FOR EXTERNAL AUDITS. A transmittal letter on official letterhead will be sent with draft audit reports to the appropriate officials of the audited entity for external audits. The transmittal letter will contain summarized information regarding the audit performed and audit findings made. Additional information specific to the reporting and administrative process will also be included. See Exhibit B of this chapter for an example of a transmittal letter.

- (1) The first paragraph(s) will identify the audited entity, location(s) audited and years under audit, and offer the opportunity for responsible views and comments.
- (2) The second paragraph indicates that we will include recognition of any actions the audited entity indicates have been or will be taken to implement our recommendations and any other information that comes to our attention. We also request that the audited entity provide comments in hard copy format and electronic copy on a CD in Microsoft Word format.
- (3) In the third paragraph, the transmittal letter for draft audit reports should indicate that, draft audit reports are not available for public viewing under the terms of the Freedom of Information Act by including the following statement:

“Please be advised that final reports of [FEHBP] or [CFC] audits must be made available to any requestor under the provisions of the Freedom of Information Act (FOIA), and will also be available on OPM’s website. It is especially important, therefore, *(to both OPM and its contractors, [if appropriate])* that such final reports are complete, accurate, fair, and as free from errors of fact or omission as our combined efforts can make them. Since we consider draft reports part of the fact finding process, they are filed with other audit documents. In our opinion, they are not releasable under the terms of the FOIA.”

- (4) In the fourth paragraph, the transmittal letter for draft reports should indicate that the Inspector General Reform Act of 2008 requires all final audit reports be made available to the public on the OIG webpage. Furthermore, objections to posting of final audit reports should be made within 21 days of issuance. The following

statement should be included:

“Also, we are required by the Inspector General Reform Act of 2008 to make all final audit reports available to the public on the Office of the Inspector General (OIG) webpage. While posting the final audit report is not considered a release under the FOIA, the OIG will use the general standards of the FOIA to determine if any portion of the report should be redacted. If you believe that anything in the report should not be posted, the OIG must receive notice of your objections in writing within 21 days of the date of receiving the final audit report. If you have any questions related to this process, please contact Timothy C. Watkins, Counsel to the Inspector General, on (202) 606-2030.”

- (5) In the closing paragraph, the transmittal letter for draft audit reports should state the due date to provide comments and any additional supporting documentation to the OIG (30 days for CFC draft audit reports, 30 to 60 days for Community Rated reports, 90 days for Global Audit reports, 90 days for Comprehensive Medical Plan reports, 60 days for limited scope audits [i.e., health benefit claims only], 90 days for full scale audits of BlueCross BlueShield Plans, Employee Organizations, or other complex insurance audits, or a date determined at the discretion of the Group Chief). Also, this paragraph will indicate that the Group Chief, Senior Team Leader or an alternatively named knowledgeable individual is available to further discuss the report (applicable telephone numbers should be included).

2-5. TRANSMITTAL MEMORANDUM ACCOMPANYING FINAL REPORTS. The final audit report will have a transmittal memorandum addressed to the Director on official letterhead. See Exhibit A of this chapter for an example of a transmittal memorandum.

- (1) The opening paragraph should indicate that a final audit report is attached and should identify the audited entity’s name and location and/or the subject of the audit, the years under audit, and provide a brief statement as to the overall findings.
- (2) The next paragraph should indicate that a draft report was issued to the audited entity and their comments are attached. The following statement can be used:
We (issued, provided, or submitted) a draft report to (the audited entity), in order to elicit their comments on the findings, conclusions, and recommendations. (Insert the audited entity’s name’s) comments on the draft report were considered in preparing the final report and are attached as an Appendix to the report. (For specific details on all audit findings, please refer to the “Audit Findings and Recommendations” section of the attached report. [if appropriate]).
- (2) The transmittal memorandum will indicate that the final audit report is available for

public release or viewing under the terms of the Freedom of Information Act. The following statement should be used:

This report has been issued by the Office of the Inspector General (OIG) to Office of Personnel Management (OPM) officials for resolution of the findings and recommendations contained herein. As part of this process, OPM may release the report to authorized representatives of the audited party. Further release outside of OPM requires the advance approval of the OIG. Under section 8M of the Inspector General Act, the OIG makes redacted versions of its final reports available to the public on its webpage.

- (3) Final audit report findings must be resolved within six months of the date of the report. The following statement should be used:

In accordance with Office of Management and Budget (OMB) Circular A-50 and Public Law 103-355, all audit findings must be resolved (agreement reached on actions to be taken on reported findings and recommendations; or, in the event of disagreement, determination by the agency follow-up official that the matter is resolved) within six months of the date of this report. Since the OIG exercises oversight concerning the progress of corrective actions, we request that (*insert the name of the designated agency representative*) provide us with a report describing the corrective action taken, and in instances where the corrective action differs from the recommendation, include the rationale for the resolution. If the corrective action has not been completed, we also ask that (*insert the name of the designated agency representative*) provide us with a report on the status every March and September thereafter until the corrective action has been completed.

- (4) The last paragraph of the transmittal memorandum will indicate that the Director can contact the IG (*on 606-1200*) or someone from the Director's staff can contact the AIGA (*include telephone number*) or Group Chief (*include telephone number*) if there are any questions.

2-6. REPORT COVER. Report covers will identify the report subject/title, the report number, and the issue date.

- (1) Many of our audits involve contractors, and as a consequence, the audit reports frequently contain proprietary data. Contractor proprietary data is protected from disclosure by law. Consequently, we must take every reasonable action to protect such data.

- (2) For most historical cost audits, place a notice on the final audit report cover informing

recipients that such reports may contain proprietary data which is protected by law.

Draft audit report covers (See Exhibit C for report cover examples) will include “**Draft Audit Report**” on the cover, as well as the following statements:

NOTICE - - THIS DRAFT RESTRICTED TO OFFICIAL USE ONLY

This document is a draft of a proposed report by the Office of the Inspector General, Office of Personnel Management. It is subject to revision and is being made available solely to those having responsibilities concerning the subjects discussed for their review and comment to the Office of the Inspector General.

Recipients of this draft must not show or release its contents for purposes other than official review and comment under any circumstances. At all times it must be safeguarded to prevent premature publication or similar improper disclosure of the information contained herein.

Final audit report covers (See Exhibit D for report cover examples) will include “Final Audit Report” on covers. The following statements will be used:

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

- 2-7. EXECUTIVE SUMMARY. This section will include summaries of why we conducted the audit, what we audited, and what we found including a brief discussion of the overall conclusions of the audit report and the most significant audit findings. The Executive Summary will also include a signature line for the Assistant Inspector General for Audits. Samples of Executive Summaries are provided in Exhibits E through I of this chapter.
- 2-8. ABBREVIATIONS. The abbreviations page will spell out each abbreviation used in the report. Samples of the Abbreviations page are provided in Exhibits E through I of this chapter.

- 2-9. CONTENTS. The contents page will reflect the following organization: executive summary; background; objectives, scope, and methodology; audit findings and recommendations (results); major contributors; exhibits; and appendices, including a section identifying abbreviations, when appropriate. (At the discretion of the group chief, the introduction, background, objectives, scope, and methodology sections may be excluded from the draft reports).
- (1) Background. This section will provide basic information on the review and nature of the program under review. It will concisely state the review type (i.e., an audit, a limited scope audit, survey, inspection, attestation, compilation, etc.) and authority (e.g., IG Act, specific statutory requirement, contract clause, request, etc.) to conduct the audit. It will include the name of the audited entity and its location. Furthermore, it will describe the program under review, the audited entity's operation, and prior audits, including recommendations and applicable follow-up activities. In addition, it will include types of communication with the audited entity (i.e., written inquiries, exit conference, etc.). See Exhibits E through I of this chapter for examples.
- (2) Objectives, Scope, and Methodology. Auditors will state the intent of the audit and the depth and coverage of the review, including any limitations, in this section. Separate headings will be used for each section. See Exhibits E through I of this chapter for examples. The requirements for each section follow.
- (a) Objectives. Objectives set the tone of the audit report. This section will provide distinct, concise statements on the intent and reason for the audit. To preclude misunderstandings, it may be necessary to identify objectives which were not covered.
- (b) Scope. Scope will describe the depth and coverage of audit work conducted to meet the audit's objectives. Any constraints (time, resources, or other) encountered during the audit will be identified in this section. The scope will identify:
- 1) Organizations and geographic locations where audit work was conducted, the time period covered, and the time period during which the audit took place;
 - 2) the type of audit performed, i.e., financial (statement), or performance (economy and efficiency, program effectiveness, internal control; and compliance with legal or other requirements);
 - 3) quality or other problems with the evidence; and

- 4) whether or not the audit was made in accordance with generally accepted government auditing standards. A statement will be made to disclose all applicable standards that were not followed. See Chapter 2400, Audit Report Preparation and Standards, for additional information.
- 5) The scope section of the audit report must consider the audited entity's internal controls as follows:
 - i) In planning and conducting the audit, did the auditors obtain an understanding of the audited entity's internal control structure?
 - ii) For areas selected, a description of the scope of testing of the audited entity's internal control structure.
 - iii) Based on the testing, did the auditors identify any significant matters involving the audited entity's internal control structure?
 - iv) A statement about whether the scope of the internal control testing provides sufficient evidence to support or not support an opinion on the audited entity's internal control structure.
 - v) The test results of the audited entity's internal control structure.
- 6) The scope section of the audit report must consider the audited entity's compliance with laws and regulations as follows:
 - i) Did the auditors conduct tests to determine whether the audited entity was in compliance with contracts, laws, and regulations?
 - ii) The test results of the audited entity's compliance with laws and regulations.
 - iii) With respect to the items not tested, was the audited entity in compliance with laws and regulations?
- 7) The scope section of the audit report must consider when reliance is placed upon the work of others as follows:
 - i) If the auditors rely on the work of others, but do not take full responsibility for that work, the scope section must indicate the division of

responsibility between the work they conducted and the work performed by others.

- ii) If the work relied upon is not significant and used for background or informational purposes, the auditors need only cite the information and its source in the audit report.
- 8) Audit planning should include a determination of the relevancy and reliability of the computer-processed data. This includes the reliance on any unverified computer data. When using unverified data, the auditors will disclose in the scope section that they did not verify the reliability of computer generated data (i.e., computer billings, claims data, etc.) and indicate whether the data was sufficient to meet the audit objective(s).
- 9) Situations Where Applicable Standards are Not Followed. The auditor and audit supervisors are responsible for using sound professional judgment in applying applicable auditing standards. Audit reports will state the nature and reason for any situations where auditors were not able to follow applicable standards. The audit report will disclose this situation in the scope section of the report. The scope section should describe the circumstances under which the standard was not followed, provide the rationale for not following the standard, and the impact these actions had on the audit results. When auditors determine that specific standards do not apply to an audit, this decision must be documented in the working papers.
- (c) Methodology. This section should explain the evidence gathering and analytical techniques used in conducting the audit, including any assumptions made in performing the audit; and comparative techniques applied and measures and criteria used to assess performance. When sampling significantly supports the auditors' findings, describe the sample type and design, including whether the results can be projected to the intended population and an explanation of the population compared to what was audited.
- (3) Audit Findings. Generally, each audit objective should be addressed in the audit report. Both positive and negative findings should be reported. Auditors should use logical structuring and the deductive approach to presenting findings. The audit findings should be reported with supporting evidence that is sufficient, competent, and relevant and should be presented in a convincing and fair manner. See Exhibits E through I for examples.
- (a) To assist readers, audit findings should be presented in order of significance or

some other logical sequence such as in the same order that the audit objectives are listed. The audit findings should also be numbered and or lettered sequentially.

- (b) Each finding should be introduced with a summary sentence or paragraph, as appropriate. Elements needed for a complete finding depend on the audit objectives but, in accordance with Government Auditing Standards, will normally include: criteria, condition, cause, and effect in addition to a discussion of evidence that supports the audit conclusions.
 - 1) Criteria establishes the standards, measures, or expectations used in evaluating audit results (what should be);
 - 2) Condition presents the factual evidence; (what the auditors found);
 - 3) Cause shows the underlying reason for the condition (why the condition occurred, Section 2-3.c. of Chapter 2400, Audit Report Preparation and Standards, provides guidance on identifying the cause); and
 - 4) Effect demonstrates the risk or exposure management faces (when the operation under audit does not operate properly).
- (c) Final audit reports should not contain discussions of findings which have been negated as a result of the audited entity's response to the draft audit report.
- (d) Where fraud or illegal acts have been identified during the course of an audit, Office of Audits staff will consult with the OIG staff from the Office of Investigations and the Office of Legal Affairs to determine what, if any, activities will be disclosed in the audit report. See Chapter 2325, Fraud, Illegal Acts, and Abuse for further information.
- (4) Recommendations. Audit reports will contain specific recommendations for corrective actions which are responsive to the problem identified. Recommendations should be clear, concise, and cost effective, citing the relationship between the corrective action and the cause. See Exhibits E through I for examples.
 - (a) When significant instances of noncompliance and weaknesses in internal controls exist, audit reports will recommend actions which can enhance compliance with applicable laws and regulations and/or result in appropriate internal control improvements.
 - (b) In final reports, comments by responsible auditee officials will be presented after

each finding and recommendation. This section should summarize the significant and relevant points. Exact quotations of the written comments is generally not necessary, but may be accepted at the discretion of the Group Chief and other reviewers. The auditee's entire response should appear as an appendix to the report.

- (5) Internal Controls. The audit report should include any significant³ deficiencies found in internal controls during the audit. The report should include all instances of fraud and illegal acts unless they are inconsequential, significant violations of provisions of contracts or grant agreements, and significant abuse. If internal control findings are insignificant, they should be communicated to the audited entity in a separate letter unless the deficiencies are clearly inconsequential considering both qualitative and quantitative factors. Instances of significant violations of provisions of contracts or grant agreements, and significant abuse should be discussed with the DAIGA before including them in the report.

The office may want to refer the fraud/abuse to the Office of Investigations and not place it in the report if further investigation work is needed. The audit report should discuss the results of an internal controls review if the sole objective is to audit the internal controls. (See Chapter 2400, Audit Report Preparation and Standards and Chapter 2205, Quality Control and Quality Assurance for additional information). Information systems controls are often an integral part of an entity's internal control. When obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.

- (6) Compliance. The audit report will disclose all significant instances of noncompliance. (See Chapter 2400, Audit Report Preparation and Standards and Chapter 2205, Quality Control and Quality Assurance for additional information).
- (7) Issues Needing Further Study. If applicable, audit reports will disclose whether the auditors identified any significant issues outside the audit objectives which need further study.
- (8) Major Contributors. List the names of the staff members who participated in the audit work. This information may be listed within a separate section of the body of

³ Significant deficiencies are those matters coming to the auditor's attention that, in the auditor's judgment, affect the results of the auditors' work and the auditors' conclusions and recommendations about those results.

- the report, in an appendix, or on the back, inside cover of the report. See Exhibits E through I for examples.
- (9) Exhibits and Appendices. Exhibits further illustrate, support, and summarize the auditors' work in developing audit findings and reaching conclusions. Appendices are supplementary materials, usually developed or provided by someone other than the auditor. They are materials which will enhance the reader's understanding of the report or present another perspective. Frequently, final reports will have appendices which include responsible official views.
- (a) Exhibits and appendices should be identified (in capital letters) "EXHIBIT" and "APPENDIX", respectively, and sequentially numbered/lettered.
- (b) For appropriate insurance audit reports, Exhibit A will be the Schedule of Contract Charges or Premiums Paid and Exhibit B will be the Schedule of Questioned Costs.
- (10) Report Fraud, Waste, and Mismanagement. The last page of the final report provides contact information to report fraud, waste, and mismanagement related to OPM programs and operations. It also includes a caution statement that is also included on the final report cover (see section 2-6 of this chapter). See Exhibits E, F, G, H, and I for examples.

SECTION 3. REPORT PROCESSING

3-1. GENERAL. OIG Office of Audits audit reports will be processed according to the following OIG guidelines.

3-2. RECORDS MANAGEMENT REQUIREMENTS.

The scanned IG's hand signed transmittal memo and the AIGA's electronically signed report are combined into a PDF file and placed in "Final Report, Transmittal Versions to Issue" folder located on the OIG LAN drive. The OIG Front Office electronically distributes this PDF file according to the distribution list on the transmittal memo, as well as certain OIG personnel. If necessary, paper versions of the report are produced in limited supplies.

3-3. DOCUMENT FLOW AND PROCESSING.

(1) Draft and Final Audit Report Review and Distribution

Draft and final audit reports will be reviewed and distributed according to the Draft and Final Audit Report Review and Distribution Work Flow Policy (see Chapter 2205, Quality Control and Quality Assurance, Exhibit I)

(2) Report Re-Issuance

If, after the report is issued, the auditors discover that they did not have sufficient, appropriate evidence to support the reported findings or conclusions, they should communicate in the same manner as that used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on the findings or conclusions that were not supported. If the report was previously posted to the OIG website, the auditors should remove the report and post a public notification that the report was removed. The auditors should then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original report if the additional audit work does not result in a change in findings or conclusions.

3-4. POLICIES AND PROCEDURES FOR PLACING THE FINAL AUDIT REPORTS ON THE OIG WEBPAGE.

- (1) All signed final reports and transmittal letters are required to be posted on the OIG webpage in accordance with the Inspector General Reform Act of 2008.
- For insurance audits, the OPM Contracting Officer notifies the OIG Counsel of the issuance of a final report. For non-insurance audits (including Combined Federal Campaign audits), the OIG issues a final report to the appropriate program offices, and the Group Chief notifies the OIG Counsel of the issuance of the final report.
 - The Group Chief converts the report, transmittal letter, and any attachments into Adobe software and then passes the documents to the OIG Counsel.
 - The OIG Counsel uses the general standards of the Freedom of Information Act to determine if any portion of the report should be redacted. If the audited entity believes anything in the report should not be posted, they have 21 days from the date of receiving the final audit report to notify the OIG Counsel in writing of their objections per FEHB Program Carrier Letter No. 2009-10. (Due to the sensitive nature of our reports, the OIG has implemented a redaction process similar to the one used to release reports to the public under the Freedom of Information Act.)
 - The OIG Counsel then forwards the redacted report to the OIG's Office of Management.
 - The Office of Management ensures that all reports posted to the OIG website meet the OPM Section 508 compliance requirements. (Section 508 compliance requires that all federal agencies' electronic and information technology be accessible to people with disabilities.)
 - Once the redaction and 508 compliance process is completed, the report goes to the OPM's Office of Chief Information Officer's (OCIO) web team. Once the OCIO web team determines that the documents are compliant, the Office of Management posts the report to the OIG webpage (www.opm.gov/oig).

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2415

Indexing and Independent Referencing

CHAPTER 2415 - INDEXING AND INDEPENDENT REFERENCINGCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy and Standards.....	1
SECTION 2. INDEXING AND INDEPENDENT REFERENCING OF REPORTS	
2-1. General.....	2
2-2. Indexing.....	2
2-3. Independent Referencing.....	5
EXHIBIT	
A. Pre-Independent Referencing Checklist	

CHAPTER 2415 - INDEXING AND INDEPENDENT REFERENCINGSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides guidelines that staff members will follow concerning indexing and independent referencing of reports. This chapter expands on the guidelines contained in Chapter 2205 (Quality Control and Quality Assurance); Chapter 2400 (Audit Report Preparation and Standards); Chapter 2410 (Report Organization and Processing); and Chapter 2420 (Non-Standard Audit Reports).
- 1-2. POLICY AND STANDARDS. The OIG Office of Audits will issue audit reports and if appropriate, attestation reports in accordance with the government auditing standards (GAS) issued by the Comptroller General of the United States.

SECTION 2. INDEXING AND INDEPENDENT REFERENCING OF REPORTS

- 2-1. GENERAL. The signer of a draft audit report has the option of having the cross-referenced copy of the draft report independently referenced before issuance. However, all final audit reports will be indexed (cross-referenced to the supporting documentation) and independently referenced before issuance. This process ensures (1) accuracy of all facts stated in the audit report; (2) fairness in the audit report presentation; and (3) adherence of audit reports and supporting audit documentation to GAS and OIG policy.
- 2-2. INDEXING. All information presented in the report must be supported. Each line in the report, including each title, statistic, fact, amount, abbreviation, regulatory or legal citation, policy, procedure, conclusion, recommendation, etc., must be indexed to supporting evidence in the audit documentation. More than one index may be required. Also, if the supporting documentation contains multiple pages, the index should take the independent referencer to the exact page(s) where the support is found. In addition, for final reports, the referenced draft report is not an appropriate supporting document and should not be indexed as support. All references/indexes must be to the actual supporting work papers.

A reference to “standard language” as support is not acceptable and the Group Chief or designee cannot pass on an independent referencer’s comment regarding the lack of support in such cases.

a. Process Overview. Indexing may be performed by any member of the audit team but ideally should be done by the team member preparing the audit document at the time the work is performed. The Auditor-in-Charge (AIC) or Team Leader is responsible for ensuring that the indexing process is complete and that the supporting documentation is properly prepared and ready for independent referencing. To help fulfill this responsibility, the AIC or Team Leader must complete and sign the Pre-Independent Referencing Check List (See Exhibit A). The check list includes a number of items that, when completed, ensure that:

- the report is fully and appropriately indexed to supporting documentation;
- supporting documentation is appropriately prepared, reviewed, and cross-referenced to other supporting documentation when appropriate; and
- totals, figures, formulas, etc. in the supporting documentation are correct and accurate and, if appropriate for the Group, the @ round function was used.

If the AIC or Team Leader is not available to complete the Pre-Independent Referencing Check List, the assigned Senior Team Leader or designee may complete the form. Whoever signs the form takes responsibility for the completion of the check list items.

- (1) All hard copy documentation indexes for non-numerical data should be made in the margin of the audit report. All automated or TeamMate indexes for non-numerical data should be made at the end of a title, a paragraph, or a sentence. All hard copy, automated or TeamMate indexes for numerical data, will be placed directly above the number to which they apply.
- (2) For hard copy audit documentation, when material is indexed to a document, the audit documentation summary must be indexed to the specific document providing evidence/support for the fact, amount, statistic, abbreviation, or regulatory citation. For automated or TeamMate audit documentation, when material is indexed to a document or the procedure summary within TeamMate, the TeamMate summary must be indexed to the specific document providing evidence/support for the fact, amount, statistic, abbreviation, or regulatory citation.

Team members will annotate audit documentation indexes in the margin for hard copy documentation; will annotate TeamMate indexes at the end of a title, a paragraph, or a sentence for TeamMate documents; and, for statistics above the number cited.

- b. Supervisory reviews, conducted by senior staff, determine whether the audit report and documentation is complete and conform to GAS and OIG policy. The Group Chief, Senior Team Leader, or designee may assign the AIC/Team Leader or designate another experienced staff member to review the audit report and documentation. The Group Chief, Senior Team Leader, or designee will ensure the completion of the review process.
- c. When indexing/cross-referencing is complete and the check list is completed and signed, the indexed report is provided to an independent referencer. The check list must be included in the report folder given to the independent referencer. The referencer should not accept the report folder unless the signed check list is included.
- d. Draft reports must be indexed and all relevant supporting documentation reviewed, initialed, and dated by a supervisor (shown as a “blue” status in TeamMate) before issuance. However, the signer of the draft report has the

option of having or not having a draft report independently referenced before it is issued.

- e. Final reports must be independently referenced before issuance. Also, all audit documentation, except for obvious administrative work papers, must be reviewed, initialed, and dated by a supervisor (shown as a “blue” status in TeamMate) before the final report is issued.

- 2-3. INDEPENDENT REFERENCING. It is the OIG’s policy to ensure that all audit reports are of the highest possible quality and that the products accurately and objectively communicate the results of our work.

Independent referencing is an important part of the quality control process that helps ensure all audit reports are of the highest possible quality and accurately and objectively communicate the results of our work. Independent referencing is the process whereby a professionally competent and independent party verifies that all information included in an audit report is adequately supported and documented. In addition to verifying every fact, figure, date, conclusion, recommendation, etc., the independent referencer also assures that the report complies with GAS and OIG requirements.

The referencer must ensure that the conclusions and recommendations logically flow from the information presented in the report. Also, a crucial part of the referencer’s responsibility is to look beyond what is presented in the report and, when appropriate, make a point on any additional facts, conclusions, or recommendations that appear to be warranted for inclusion in the report.

Referencers are to sign off on a referencing point only when they agree that the action taken fully satisfies the comment or point made. Although referencers should be reasonable in their approach to resolving identified problems, they should not compromise on points they believe have not been adequately addressed. As discussed later in this chapter, when the referencer does not agree that a point has been resolved, the point should be reviewed by the Group Chief or designee who will determine whether to “pass” the point or to revise the report to satisfy the referencer’s comment. If the Group Chief decides to “pass” on the point, he/she should type or write “pass” on the coaching note or hard copy referencing note, and initial and date it. Final audit reports will not be cleared for signature unless independent referencing has been completed and all points raised by the independent referencer have been resolved.

Under no circumstances is an independent referencer to be intimidated or feel threatened by reprisal for comments/points raised during the referencing process. If an independent referencer believes that he/she has been unduly pressured into initialing or signing off on referencing comments or is treated unfairly as a result of the referencing assignment, he/she should so inform the Deputy AIGA.

- a. Referencer's Qualifications and Responsibilities. Independent referencing will be completed by a staff member who has not been involved in performing the audit fieldwork. A staff member doing independent referencing will possess a minimum of three years of auditing experience. If a staff member is not available within the group, the Group Chief or designee shall request assistance from the DAIGA in obtaining a referencer from another audit group.

- b. Before starting the referencing process, the independent referencer must determine the extent to which the audit documentation has been reviewed and approved. For final reports, all audit documentation, except obvious administrative work papers, must be reviewed and approved (shown as a “blue” status in TeamMate). If not, the referencer should inform the Group Chief or designee that he/she cannot proceed until the audit documentation has been approved.

For draft audit reports, the referencer can proceed if a substantial portion of the audit documentation has been approved. However, when reviewing the indexed supporting documentation, the independent referencer should make a referencing comment for each supporting work paper that has not been reviewed and approved.

- c. Procedures. Referencers shall:

- (1) Verify the information on every line of the report, including each fact, figure, statistic, title, abbreviation, legal or regulatory citation, other comments, conclusions and recommendation. Also, verify information such as contract numbers, quotations, paraphrasing of policy, law, or regulations.
- (2) Perform mathematical or clerical checks to determine if every figure and statement is correctly reported.
- (3) Verify that reported findings are documented with sufficient, competent, and reliable evidence.
- (4) Verify that all conclusions and recommendations are supported by audit documentation and logically flow from the information presented in the report.
- (5) Make a point on any additional facts, conclusions, or recommendations that appear to be warranted for inclusion in the report.
- (6) Verify that supporting documentation was prepared in accordance with GAS and OIG policy.
- (7) For hard copy documentation, document that the indexed audit report has been referenced by placing tick marks (✓) over the referenced items such as numbers and figures and a tick mark at the end of each line in the report. Use a reviewer comment sheet to record instances where the independent referencer disagrees with the accuracy, consistency, fairness, etc. in the

material presented in the report. See Chapter 2220 (Audit Documentation and Files) for a copy of the comment sheet. The referencer should also note any items, which should have been indexed but were not.

- (8) For automated or TeamMate reports and documentation, the independent referencer documents that the indexed report has been referenced by placing a tick mark (√) over the numbers and figures and a tick mark after the index or cross-reference that is placed at the end of the relevant sentence. Independent referencing comments regarding the accuracy, consistency, fairness, etc. of the report information are placed in “coaching notes”. The independent referencer should also note any items which should have been indexed but were not. All coaching notes should be kept for review. See Chapter 2220 (Audit Documentation and Files).
 - (9) The resolution of each independent referencer comment shall be documented on the reviewer comment sheet for hard copy reports and on each individual coaching note for TeamMate prepared reports.
 - (10) Upon completion of the referencing assignment, the independent referencer must complete his/her section of the Pre-Independent Referencing Check List and place it in the report folder. See Exhibit A.
- d. Resolution and Disposition of Comments. When the independent referencer has completed the review of the audit report, he/she will notify the Senior Team Leader or designee and inform him/her of any comments that need to be resolved. The Senior Team Leader or designee may delegate the staff work necessary to resolve the comments, but he/she is ultimately responsible for the final disposition.
- (1) When documenting the disposition of a referencing comment, the designated responder shall clearly indicate, on the reviewer comment sheet or coaching note, whether the referencing point is accepted, modified, or rejected and note any changes made to the report. If there is disagreement as to what change should be made or if the point is rejected, the reason should be clearly stated.
 - (2) The independent referencer will review the disposition of each comment. For hard copy documentation, when the referencer agrees with the disposition, the referencer will initial and date the “Disposition Approved” column on the reviewer comment sheet and place a tick mark (√) next to the relevant material in the report. For automated or TeamMate documentation, the referencer will electronically initial and date the

coaching note and place a tick mark (√) next to the relevant material.

- (3) The independent referencer will work with the designated responder to resolve disagreements on unresolved referencing points. If the independent referencer cannot reach agreement on the resolution of a reference point, the designated responder shall refer the issue to the Senior Team Leader or other designated person for review. If the issue still cannot be resolved, it will be referred to the Group Chief for resolution.
- (4) If the independent referencer cannot agree with a disposition comment approved by the Group Chief, the Group Chief will write “pass” (accepts responsibility), initial and date the disposition for either the hard copy or TeamMate coaching note.
- (5) For all comments resolved or “passed” at the Group Chief level, a copy of the referencing comment and its disposition should be included in the report package forwarded to Quality Assurance Group (QAG).
- (6) If additional source material is provided in response to the referencing comments, the designated responder will add the appropriate indexes to the referenced copy of the report. If necessary, the designated responder will also modify existing documentation or place any new documentation in TeamMate or hard copy documentation. If the disposition of a comment involved changes to the audit report, the referencer must reference the changes and, if acceptable, place a tick mark (√) next to the new material in the report.
- (7) If oral explanations are required to resolve referencer comments, the referencer needs to consider whether the audit report and/or audit documentation needs revision in light of the explanation and if new undocumented facts are presented. Changes must be documented in the audit documentation, including the independently referenced copy of the audit report or the report control folder.
- (8) For hard copy documentation, when final resolution and disposition of comments is complete, the Senior Team Leader or designee will sign and date the reviewer comment sheets at the lower right-hand corner. See Chapter 2220, Exhibit D (Audit Documentation and Files). For automated or TeamMate audit documentation, final resolution and disposition of comments is complete when all of the coaching notes are initialed and dated.

- (9) Any substantive changes or changes of fact made to the audit report after independent referencing is complete must be referenced by the independent referencer. Once the changed areas have been highlighted and the new material indexed, the audit report is resubmitted for review of the changes by the independent referencer.
- (10) For hard copy audit documentation, all versions of the independently referenced report and accompanying reviewer comment sheets must be annotated with the date (month, day, and year) and version number of the revision. All referenced audit reports will be filed with the audit documentation or the report control folder. All reviewer comment sheets, including those relating to prior audit report versions, will be filed with the audit documentation.

For automated or TeamMate audit documentation, all versions of the independently referenced audit reports and accompanying coaching notes must be annotated with the date (month, day, and year) and version number of the revision. All referenced audit reports will be filed with TeamMate or the report control folder. All coaching notes, including those relating to prior audit report versions, will be filed with TeamMate.

- (11) The referenced copy of the report must be clearly identified as the “independently referenced copy” and must be signed/initialed and dated (month, day, and year) by the referencer. A copy of the independently referenced report will be provided to QAG. Also, all reviewer comment sheets and/or all coaching notes will be provided to QAG. If no comments or notes were made, note this on the report before passing it onto QAG.
- (12) The Group Chief will verify that the audit documentation is complete and that the independent referencer and Senior Team Leader or designee has completed their responsibilities, reviews, etc. regarding the report and that all necessary changes have been completed. See Chapter 2410 (Report Organization and Processing) for additional information on report processing. The Group Chief will also ensure that the completed Pre-Independent Referencing Check List is placed in the report package and forwarded to QAG.

Pre-Independent Referencing Check List

Audit Name: _____ **Report Number:** _____

It is an objective of the Office of Audits to produce audit reports that are of the highest possible quality and accurately and objectively communicate the results of the audit work performed. To help ensure that this objective is achieved, each audit report must be referenced by an independent and professionally competent individual. See Chapter 2415 for specific information on independent referencing. Chapter 2415 also provides additional information on this form, including the role of Quality Assurance Group in tracking AIC/Team Leader performance in regard to the form.

AICs/Team Leaders are responsible for ensuring that the reports they prepare are ready to be referenced by the independent referencer. This check list is designed to help them fulfill this responsibility. Completion of the check list will, among other things, ensure that the report is adequately indexed to appropriately prepared supporting documentation. The checklist should help expedite the referencing process by reducing the number of referencing comments and the amount of time the referencer spends looking for supporting documentation.

Upon completion of the check list, the AIC/Team Leader must sign and date the form and include it in the report package given to the independent referencer. The Senior Team Leader may complete the check list if the AIC/Team Leader is not available. After referencing is completed, the independent referencer will complete his/her section of the form and place it in the report folder. Quality Assurance Group will not accept the report package for review unless the completed form is in the folder.

Before a report is given to the independent referencer for referencing, the AIC/Team Leader must ensure that the following steps have been completed.

Completed

- _____ 1. **Each line in the report**, including each fact, figure, date, policy, procedure etc. is indexed to credible supporting data contained in a work paper(s). If the work paper includes several pages, the specific supporting page should be included with the index or the link should go to the specific page. In addition, the reference or index should be to the primary work paper supporting the data and to any summary work paper, if applicable.
- _____ 2. All conclusions and recommendations are supported by a work paper and logically flow from the data presented in the report.

Completed

- _____ 3. All supporting summary work papers are clear and convincing and have been cross-referenced to the underlying support documentation.
- _____ 4. Each supporting work paper includes the source for the data and is complete, accurate, and understandable without additional explanation.
- _____ 5. Each interview write-up includes interview date, participants, email address, telephone number, purpose, and clearly indicates who made the interview statements.
- _____ 6. Each supporting work paper has been initialed and dated by the preparer and reviewer.
- _____ 7. All totals and percentages in the report and accompanying schedules have been checked for accuracy.
- _____ 8. All formulas used in worksheet computations have been checked for accuracy and, if appropriate for your Group, the @round function was used.

I certify that the check list items have been satisfactorily completed.

Preparer Signature
Date

The following section is to be completed by the Independent Referencer upon completion of the referencing assignment.

Signature
Date

Please check the appropriate box to indicate the extent to which the cross indexed report complied with the check list items. Please note the check list items not in substantial compliance and provide comments as appropriate.

Fully Complied Substantially Complied Significant Deviations

Place any comments below.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2420

Non-Standard Audit Reports

CHAPTER 2420 - NON-STANDARD AUDIT REPORTS

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy and Standards.....	1
SECTION 2. TYPES OF NON-STANDARD AUDIT REPORTS	
2-1. General.....	2
2-2. Memorandum Report for Internal Audits.....	2
2-3. Flash Audit Alert.....	2
2-4. Supplemental Audit Report.....	3
2-5. Interim Report.....	5
2-6. Rate Reconciliation Audit Report.....	5

CHAPTER 2420 - NON-STANDARD AUDIT REPORTSSECTION 1. GENERAL

- 1-1. PURPOSE. In addition to the standard audit reports discussed in Chapters 2400 (Audit Report Preparation and Standards) and 2410 (Report Organization and Processing) of the OPM-OIG Audit Manual, the OIG Office of Audits also issues several types of non-standard audit reports. Guidance concerning these non-standard audit reports is contained within this chapter.
- 1-2. POLICY and STANDARDS. The OIG Office of Audits will issue audit reports that fully comply with Government Auditing Standards (GAS) for reporting set forth by the Comptroller General of the United States.

SECTION 2. TYPES OF NON-STANDARD AUDIT REPORTS

2-1. GENERAL. Some of the various types of non-standard audit reports issued by the OIG Office of Audits appear in this section. All non-standard audit reports, except rate reconciliation audits (RRA), are prepared for the signature of the Assistant Inspector General for Audits. All RRA reports are prepared for the signature of the Group Chief or designee of the Community-Rated Audits Group.

2-2. MEMORANDUM REPORT FOR INTERNAL AUDITS. A memorandum report on official letterhead for internal OPM audits is distributed only to officials of the audited entity. This report provides a means to quickly inform OPM officials of the audit results and eliminates the need for general information that is of no value to report recipients.

The report should include the report number; memorandum headings (from: and subject:); background of the audited subject; objectives, scope, and methodology; and the results of the audit. The report must include a reference to compliance with generally accepted government auditing standards. The report must be cross-indexed and independently referenced.

The Assistant Inspector General for Audits (AIGA) or Group Chief should be identified as the contact for additional information or concern.

2-3. FLASH AUDIT ALERT. Flash Audit Alert (FAA) reports are used to bring individual issues, or items requiring immediate action, to the attention of the audited entity and responsible OPM program official in a timely manner.

- a. The use of a Flash Audit Alert does not negate the requirement for in-depth audit reporting as detailed in Chapters 2400 and 2410 of the OPM OIG Audit Manual.
- b. The issues or items to be reported in the FAA will be fully discussed with the audited entity's management and any comments or corrective actions they are planning to take will be noted in the FAA report. Also, the report will provide the management with a further opportunity to provide additional comments which will be considered during preparation of the draft audit report. All follow-up on the FAA will be addressed in the in-depth draft and final audit reports.
- c. The Flash Audit Alert will be processed expeditiously and in a final report format (see 2-4. d). Quality Assurance will review the FAA and supporting audit documentation to ensure adherence to GAS and the policies and procedures prescribed by the OIG. The AIGA will review the alert prior to issuance.

- d. The FAA reports will contain:
 - 1. a Transmittal Letter and/or Memorandum, as applicable, identifying the report as a "Flash Audit Alert" and providing the flash number and issue date; indicating the report recipients, purpose of the report, general observations concerning the problem area, and AIGA or Group Chief as the contact person (with applicable telephone numbers); and
 - 2. an explanation of the problem and the reason for the urgency; identification of possible benefits from taking immediate corrective action; background information; explanation of the audit results, including recommendations; and requests for management comments.
- e. When the draft and/or final audit reports are issued, the background section will indicate that the OIG has previously issued a FAA on the audit subject. Because the FAA is, in effect, an interim report, the FAA issue(s), any management response to the FAA finding(s) or recommendation(s), and an OIG analysis of the management response will be consolidated into the findings section of the draft and/or final report.

2-4. SUPPLEMENTAL AUDIT REPORT. Supplemental audit reports are required when events occur subsequent to the issuance of either a draft or a final report which affect the integrity and/or conclusions in one or more of the findings in the report. Note that where the integrity of substantially all of the report is affected, a revised report should be issued.

Supplemental audit reports may be used in both the draft and final audit report stages. The supplemental report must comply with the same basic audit report preparation, standards, and processing as detailed in Chapters 2400 and 2410 of the OPM OIG Audit Manual.

- a. One rationale for using a supplemental audit report is that it allows for the timely resolution of issues which have not changed from the original report. The final audit report can be issued regarding the unchanged findings while at the same time a supplemental report can be issued on any new or changed findings. The use of the supplemental audit report allows time for the audited entity to respond to new or changed issues without holding up the final report.
- b. Situations which would require the use of a supplemental audit report include, but are not limited to, the following:
 - 1. After issuance of a draft audit report, an additional finding is disclosed. In this case, a supplemental draft report will be issued addressing the additional finding

and allowing the audited entity time to respond to the heretofore undisclosed issue. If possible, the final report should incorporate the findings and responses of the original and supplemental draft reports. However, if time constraints prevent this, a comment should be made within the original final report that a supplemental final report will be issued addressing the issues covered in the supplemental draft report.

2. On occasion, a finding in the draft report is so significantly revised that the finding no longer resembles the original finding and the audited entity initial response is no longer relevant. In this case, we will follow the same procedures as detailed in b.1. above. This is necessary in order to allow the audited entity time to provide comments on the revised findings.
 3. If, during any phase of the reporting process, the auditor becomes aware of information which, had it been known at the time the audit report was issued, would have affected the report conclusions then a supplemental report is required. This could occur at either the draft or final report stage.
- c. If the purpose of the supplemental report differs from the purpose of the original report, then a new report, rather than a supplement, should be issued.
 - d. A supplemental report need not supersede the original audit report in its entirety. It should be limited to the affected item(s) of the prior report and should not generally restate previous information or recommendations. In the first two cases detailed in b. above, the supplemental report would generally not supersede any part of the original audit report, but rather would provide additional information and recommendations.
 - e. The supplemental report's narrative, including the purpose, scope, background, summary, etc. is to be limited to the reasons for the supplemental report and the new summary and/or recommendations resulting from the supplemental information.
 - f. Make the task of supplementing as easy as possible for the report recipient. If there are numerous pen and ink or TeamMate changes and page substitutions, it is often easier to replace a complete exhibit or schedule in the original report with a revised exhibit or schedule.
1. Precise instructions must be provided to enable the report recipients to incorporate any new pages, exhibits, etc. If the original audit report is to be replaced entirely, the following statement should be made:

"This supplemental report replaces our original report in its entirety."

2. If the original report is not being entirely superseded, instruct the recipient to make pen and ink or TeamMate changes or page substitutions. For example:

"Remove pages 2, 4, and 6 from our original report and replace with the attached revised pages ..."

In this case, add the following additional comment:

"Except as noted above, all other comments contained in the original report remain unchanged."

- g. The supplemental audit report number should contain the original audit report number, except for the last 3 digits which is a unique number assigned by ARRTS (i.e., 1A-10-13-04-XXX).
- h. The supplemental audit report cover sheet, title, and subject must clearly identify the report as a supplement.

2-5. INTERIM REPORT. Interim reports are issued when audits continue over extended periods of time. The Group Chief or designee will determine when periodic reporting is required. The OIG Office of Audits will issue interim reports in a draft report format and the results of the interim reports will be incorporated at the end of the audit into the final audit report. Interim audit reports will follow OIG reporting policies and procedures for draft reports contained in Chapter 2400 (Audit Report Preparation and Standards) and Chapter 2410 (Report Organization and Processing).

2-6. RATE RECONCILIATION AUDIT REPORT. The rate reconciliation audit (RRA) concept, implemented in 1996, is designed to be quick and responsive in order to assist OPM contracting officials in negotiating the final rates that community-rated health maintenance organizations (HMO) charge for providing health benefits to federal employees, annuitants and their dependents. The audits provide the officials with current, complete and accurate information on the appropriateness of the rates before the rates are finalized. This RRA approach supplements, but does not replace, the standard community-rated audits. RRA reports do not contain all of the wording found in the standard community-rated audits, but meet generally accepted government auditing standards.

Rate reconciliation is an annual process that allows HMO carriers to adjust the rates that they "propose" and actually go in effect on January 1 of each contract year. Since

HMO's are required to submit their community rates seven months in advance of the January 1 effective date of the new contract year, some of the data used to develop the rates is based on estimated or preliminary information. The rate reconciliation process gives the carriers the opportunity to adjust the rates based on more accurate and up-to-date information. The goal of the RRA process is to start and complete the audit, including the issuance of a final report to OPM contracting officials, in approximately a three-week period.

RRAs are limited to only the current year's rate reconciliation (one year). The audits of rate reconciliations start in May and are finished before the rate reconciliation process is completed in early August. This time frame coincides with the period that OPM's Office of Actuaries (OA) actually receives the rate reconciliation information from the carriers and finalizes the rates actually charged.

In contrast, our standard community-rated audits are usually conducted a number of years after the completion of the contract year and finalization of the rates through the reconciliation process. RRAs differ in that they are performed prior to the final rate settlement, thereby providing OPM program officials with a detailed analysis of the data supplied by the carriers in support of any adjustments to their "proposed" rates.

Due to the nature and purpose of RRAs, the content and reporting format differs from our standard audit reports. Rate reconciliation audit reports are in the form of a memorandum (See Chapter 2410, Report Organization and Processing), containing limited background information, including exhibits, and focus on providing the information OA needs to finalize the rates. No draft report is provided to the carrier for comment; doing so would take too much time and negate the purpose of performing the audits. However, the results are discussed with the carriers at an exit conference. Carriers have the opportunity to agree or disagree with the information we report when negotiating the final rates with OA. Report recommendations are tracked in the ARRTS system. Questioned costs are set up in ARRTS as a receivable. OPM's Healthcare and Insurance Office (HIO) receives confirmation that the rate reconciliation questioned costs have been resolved. The dollar amounts are posted by HIO in ARRTS as allowed, disallowed, or recovered.

Using 2013 contract rates as an example, if OPM determines that the contract rate charges to subscribers were too high, it can lower the 2014 rates to compensate for the 2013 overcharge or have the particular plan repay the amount of the overcharge directly to the FEHBP or reduce the plan's contingency reserve payment. If the reconciliation shows that the rates were too low, OPM is obligated to compensate that plan from the FEHBP funds maintained in the contingency reserve fund.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2505

Sampling Techniques

CHAPTER 2505 - SAMPLING TECHNIQUESCONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Background.....	1
SECTION 2. DETERMINING THE SAMPLING APPROACH	
2-1. Determining a Sampling Approach.....	2
2-2. Sampling Method and Design.....	2
2-3. Preparing a Sampling Plan.....	2
2-4. Identifying the Audit Objectives.....	3
2-5. Audit Universe/Population.....	3
2-6. Sample Size.....	3
2-7. Sample Selection.....	3
2-8. Analyzing and Using Sample Results.....	4
2-9. Documentation Requirements.....	4
EXHIBITS	
A. Glossary of Statistical Sampling Terms.....	5
B. Publications on Applications of Statistical Sampling Techniques.....	7
C. Examples Describing the Sampling Method Used in the Audit Report & WorkPapers..	8

CHAPTER 2505 - SAMPLING TECHNIQUESSECTION 1. GENERAL

- 1-1. PURPOSE This chapter presents the essential principles and methods of statistical sampling (sampling) applicable to an auditing environment. Sampling is a procedure by which the selection and analysis of a small number of a population's individual elements or members are used to accurately describe characteristics of the entire population.

This chapter provides general guidance in the selection and use of appropriate sampling methods for achieving the audit objectives. The guidance applies to both estimation and acceptance sampling.

- 1-2. BACKGROUND Sampling is a tool which may be used when the size of a population is too large to audit every item or the cost of the audit of each item is prohibitive. Sampling will provide accurate information about an entire population, while data extracts only allow conclusions to be drawn about the actual extracted records.

For reliable results, each item in the sample must have had a determinable probability of being selected from the universe. This result is achieved through a random selection of the items to be tested. The tested population need not include all universe elements, only all those elements that have the general characteristic the auditors wish to investigate.

Population stratification is the partitioning of the population into exclusive and exhaustive subsets that have an identifiable characteristic. This creates a "sub-universe" or strata. Stratification is only necessary if the auditor has a hypothesis that the characteristic to be tested differs significantly between the strata. For example, the auditor will often separate inpatient claims from outpatient claims because they are very different classes of claims. From the total population of all claims, the auditor may choose to review a subset, for example, drug claims, if audit objectives do not dictate the review of such subset.

SECTION 2. DETERMINING THE SAMPLING APPROACH

- 2-1. DETERMINING A SAMPLING APPROACH The specific audit objective, availability of data from which a sample is to be selected, and intended use of the sampling results will help the auditor to determine the most advantageous sampling approach.
- 2-2. SAMPLING METHOD AND DESIGN In general, there are no rigid rules as to the sampling approach that should be used on a particular audit. Rather, in developing a sampling approach that minimizes the amount of audit work, but that still gives useful results, the auditor needs to consider such factors as follows:
- a. Why is sampling necessary and how will it contribute to the overall audit objective? An important consideration to remember is that a sample is intended to be representative of a larger population. If auditors can efficiently review an entire population rather than a sample, they should normally do so. For example, an audit objective to determine if contract expenditures are allowable might be accomplished by 100 percent review if the contract data is available in electronic format. On the other hand, a judgmental sample of the largest contract transactions might equally satisfy the audit objectives.
 - b. How long will it take to evaluate each sampling unit? If two to three days are needed to review each sample item, a large sample size may not be feasible.
 - c. What is the expected error rate or variance in the population and how does the expected error rate compare with a tolerable rate? If the auditor expects a 50 percent error rate, but has criteria to show that the rate should not exceed 1 percent, a large sample will not be needed to show that there is a problem. On the other hand, an expected two percent error rate and a tolerable one percent error rate will require a much larger sample.
 - d. How precise does the auditor need to be in determining individual amounts, and how confident does the auditor need to be in the final results taken as a whole? Greater precision and confidence will normally be needed to support a recommendation to recover \$1 million than to support a recommendation that internal controls need to be improved.
- 2-3. PREPARING A SAMPLING PLAN In terms of planning and managing audits that involve statistical sampling, auditors should specifically address the characteristics listed below. This can be done by documentation in the audit work papers.

- 2-4. IDENTIFYING THE AUDIT OBJECTIVES Auditors need to be able to explain why sampling is necessary and how it contributes to the overall audit objective.
- 2-5. AUDIT UNIVERSE/POPULATION Auditors need to carefully identify the population from which a sample will be selected since sampling results will be affected by the reliability of the data from which the sample is drawn and how sampling items are defined.
- 2-6. SAMPLE SIZE In determining the size of sample needed, auditors first have to determine the levels of precision and confidence needed. These answers, in turn, are dependent on the size of the universe, the types of analysis planned, and the type of sampling used. However, the process of determining sample size is not solely mechanical in nature; it also requires auditors to make tradeoffs between the desire for greater precision versus the time, effort, and costs associated with assessing a large sample. Some general rules that may help auditors in determining sample size are as follows:
- a. In sampling for attributes, the auditor will normally have to select at least 30 items. Also, the definition of what constitutes an error and tolerable deviation rates should be determined before a sample is selected. For example, in a control review, the auditor should determine what constitutes a significant or material error, and how many deviations can occur before controls are deemed to be ineffective.
 - b. In sampling for variables, the auditor should normally select a sample that will generate at least 15 to 20 error values. Thus, with an expected 5 percent error rate, a sample size of 300 to 400 items would be needed to generate the 15 to 20 error values necessary to accurately project dollar impact. On the other hand, a sample of 50 items would normally generate a reasonable projection if a 40 to 50 percent error rate were encountered.
 - c. In selecting a stratified sample, at least 20 items should be selected in each stratum. If the number of items in a particular stratum is less than 20, all of the items should be reviewed. In order to project variables, the auditor should ensure that the sample size in each stratum is large enough to generate 8 to 10 errors. The total sample, i.e., all strata, should generate 15 to 20 errors in order for the auditor to ensure useable results.
- 2-7. SAMPLE SELECTION In order for a statistical sample to be used to make inferences about the universe, it must be based on the laws of probability. In most cases, random number sampling using computer-generated random numbers is a preferred method of selecting a sample since every sampling unit has the same probability of being selected.

Other methods of selecting sample items, such as systematic sampling, may result in a biased sample if the population is not arranged randomly. Random number sampling will also provide the auditor the most flexibility in adjusting to unexpected error rates and expanding or decreasing the sample size, particularly if sample items are reviewed in the same order that the random numbers were generated. Random based methods such as sequential or haphazard are permissible. The work papers should also include a discussion of how the sample results will be used.

- 2-8. ANALYZING AND USING SAMPLE RESULTS Auditors must use care in analyzing and presenting sample data. For example, if auditors selected samples consisting of 100 contract files at each of three audit sites, they might desire to present the combined results of their work. This could lead to inaccurate conclusions if the universe at each of the sites differs, such as 1,000 at one site, 5,000 at another, and 10,000 at the third. Combined results would be correct only if the sample results were weighted to reflect the differing number of contract files at each site. The audit report needs to state if the sample results are projected or not projected to the population.
- 2-9. DOCUMENTATION REQUIREMENTS The audit documentation must fully support and explain the sampling procedures followed during the audit. The auditors must ensure that the work papers include the following sections, as appropriate.
- (1) Sampling Method/Design (2-2) – Includes statistical or judgmental sampling strategy; i.e., How did you judgmentally select the sample? Was every n^{th} item selected? Were the sampled items stratified? By item? By dollar amount? Was SAS used for the sampling method? Did SAS generate the number of items to review? Were the sample items stratified? By item? By dollar amount?
 - (2) Objective (2-4);
 - (3) Audit Universe/Population (2-5), i.e., What was the total universe of items? What was the number of items out of how many items?;
 - (4) Sample Size (2-6) – Includes attributes of the sample (error rates, sample interval, confidence levels, etc.) and stratification methodologies;
 - (5) Basis for sample selection (2-7);
 - (6) Detailed results of the sample (2-8);
 - (7) Basis for projecting or not projecting the sample results (2-8), i.e., Can the sample be projected? Why or why not?

If the auditor cannot complete the process or decides not to project results, an explanation should be included in the audit documents.

Document the use of SAS software, as appropriate, in designing and conducting your sampling approach.

GLOSSARY OF STATISTICAL SAMPLING TERMS

Attribute Sampling. The sampling process used to estimate the number of times a characteristic or situation occurs in a population.

Cluster Sampling. Sampling from groups of items that may be conveniently broken down into subgroups or "clusters"; for example, trays of file cards. Each cluster is evaluated as if it were a single observation.

Confidence Level. Indicates the risk the auditors are willing to take in the sample selection. For example, in choosing a 95 percent confidence level, the auditors have used a method of estimation that is successful about 95 percent of the time.

Confidence Interval. Confidence interval refers to the magnitude or distance between the upper and lower limits of the true population value to the point estimate. When an auditor desires that the confidence interval be of a specified size (i.e., +/- 5 percent), the confidence interval is replaced by a precision factor statement.

Discovery Sampling. This type of sampling is sometimes referred to as detection or exploratory sampling. The audit objective is usually to locate at least one instance of some type of critical event where it occurs, rather than the frequency of occurrence as with estimating sampling of attributes.

Systematic Sampling. The process of selecting a random sample of items from a population (universe) on a fixed interval basis; for example, every 10th item. The method is useful when the population items are not numbered and to number them solely for the purpose of sampling would be costly.

Parameters. The mathematical quantities which describe a population. Sampling is used to estimate those quantities.

Population. The universe or group of items. It represents the total number of elements available to be sampled.

Probability Sample. Same as a random sample. A sample selected in a manner that assures that each remaining element in the strata or population has an equal chance of being selected.

Projection. The expansion of sample results to estimate a population value.

Sampling Precision. Precision is the selected range within which the estimate of the population characteristics will fall and is usually expressed in terms of a plus or minus value, such as $\pm 3\%$.

Simple Random Sample. A sample selected so that each element has an equal chance of being selected.

Standard Deviation. The term used to describe the degree of dispersion or variability in a set of individual item values about the population mean.

Stratified Random Sampling. A method of reducing sample variability for the purpose of improving the sample reliability. Stratified sampling consists of dividing the population into exclusive subgroups and sampling within the individual groups.

Universe. Same as population. The total group of items possessing a certain characteristic(s).

Variables Sampling. The sampling process used to measure characteristics in a population in terms of their individual magnitudes or values. More commonly called point estimation.

Exhibit B

PUBLICATIONS ON APPLICATION
OF STATISTICAL SAMPLING TECHNIQUES

1. Applications of Statistical Sampling to Auditing, Alvin A. Arens and James K. Loebbecke, Prentice-Hall, 1981.
2. Handbook of Sampling for Auditing and Accounting, Third Edition, Herbert Arkin, McGraw-Hill, 1984.
3. Practical Statistical Sampling for Auditors, Arthur J. Wilburn, Marcel Decker Inc., 1984.
4. Sample Design in Business Research, W.E. Deming, Wiley, 1960.
5. Sampling for Modern Auditors: A Personal Study Course, Institute of Internal Auditors, Inc., 1977.
6. Sampling Techniques, Third Edition, William G. Cochran, Wiley, 1977.
7. Statistical Methods, Eighth Edition, G.W. Snedecor and W.G. Cochran, Iowa State University Press, 1989.
8. Statistics for Business and Economics, Third Edition, H. Kohler, Harpercollins College Division, 1994.
9. Statistics for Business and Economics, Revised, 12th Edition, D.R. Anderson, D.J. Sweeney, T.A. Williams, J.D. Camm, and J.J. Cochran, South-Western College Publishing Company, 2014.
10. Statistics for Management, Third Edition, B.J. Mandel, Dangary Publishing Company, 1984.
11. Using Statistical Sampling, U.S. General Accounting Office, Revised May 1992.

EXAMPLES DESCRIBING THE SAMPLING METHOD USED IN THE AUDIT REPORT
AND WORK PAPERS

The following examples may help the auditors in describing how the sampling method should be shown in the audit report and work papers:

- To test the administrative and management activities at the (*audit entity*), we used a judgmental sampling method to select 100 fiscal year 2009 invoices from OPM's database files generated from GFIS. Our sample was selected by stratifying the population of 1,000 transactions by vendor and dollar amount and interest amount. The number of items selected was judgmentally determined based on the total stratum number of vendors and the total stratum dollar and interest amounts. Invoices were randomly selected in each stratum. For the 100 invoices reviewed, we discovered that 85 invoices (or 85 percent) in our sample were in error. Based on this result, when we project the 85 percent error rate to the population of 1,000 transactions, we estimate that a total of 850 invoices were in error.
- To determine if the 2009 Combined Federal Campaign's (CFC) receipts and disbursements were monitored in accordance with CFC regulations, we selected a systematic random sample of 25 out of the population of 8,000 pledge cards (by choosing every 550th pledge card) and compared them to the Pledge Card Report and actual pledge cards from the PCFO. We selected 10 pledge cards where the individual amounts pledged did not reconcile to the total amount pledged to the CFC. In addition, we selected 15 pledge cards that raised questions to the auditor. For the 25 pledge cards reviewed, we found that 20 pledge cards (or 80 percent) in our sample were in error. Based on this result, when we project the 80 percent error rate to the population of 8,000 pledge cards, we estimate that a total of 6,400 pledge cards were in error.
- To determine if OPM has effective controls in place to safeguard and ensure accountability of sensitive property, we judgmentally selected six out of eight program divisions to perform our detailed audit procedures. We used Interactive Data Extraction Analysis software to select random samples of sensitive property for testing. Samples were selected to verify physical existence as follows:

Exhibit C
Page 2 of 2

<u>Divisions</u>	<u>Laptops</u>	<u>Smart phones</u>	<u>GPS Units</u>
FISD	15 sampled 444 universe	9 sampled 54 universe	150 sampled 1572 universe
OIG:	10 sampled 167 universe	11 sampled 44 universe	
HRPS:	18 sampled 221 universe	43 sampled 168 universe	
HCLMSA:	4 sampled 56 universe	2 sampled 16 universe	
OCFO:	5 sampled 48 universe	4 sampled 29 universe	
SHRP:	13 sampled 42 universe	13 sampled 38 universe	
<hr/>			
Total:	65 sampled 978 universe	82 sampled 348 universe	150 sampled 1572 universe

Our review found the following three sensitive properties in total missing from the six divisions:

60 out of 65 laptops (92 percent error rate);
80 out of 82 smart phones (98 percent error rate); and,
140 out of 142 GPS units (99 percent error rate).

Based on these results, when we project the error rates to the universes of these three sensitive properties, we estimate the following items in total were missing from the six divisions:

900 laptops (92 percent error rate x 978 universe);
341 smart phones (98 percent error rate x 348 universe); and,
1556 GPS units (99 percent error rate x 1572 universe).

- To test the Plan's compliance with the FEHBP health benefit provisions, we selected and reviewed a judgmental sample of claims (referred to as our system review) that were paid during the period January 1, 2009 through December 31, 2009. For this period, the auditors identified 2,622,517 claim lines, totaling \$388,210,529 in payments, using a standard criteria based on our experience. From this universe, the auditors selected and reviewed a judgmental sample of 100 claims, (representing 1,308 claim lines) totaling \$9,185,382 in payments. We selected our sample from an OIG-generated "Place of Service Report" (a SAS application) that stratified the claims by place of service (POS), such as provider's office, and payment category, such as \$50 to \$99.99. We judgmentally determined the number of sample items to select from each POS stratum based on the stratum's total claim dollars paid. The results from the samples were not projected to the population because the sample tested was selected judgmentally.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2905

Release of Official Information

CHAPTER 2905 - RELEASE OF OFFICIAL INFORMATION

CONTENTS

	<u>Page</u>
 SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
 SECTION 2. RELEASE OF OFFICIAL INFORMATION	
2-1. General.....	2
2-2. Authority to Release Official Information.....	2
2-3. Reports Required to Be Posted by the IG Act.....	3
2-4. Releasing Official Information.....	3
2-5. General Policy and Procedures.....	3
2-6. Special Considerations.....	6
2-7. Documenting Records/Actions.....	8
 EXHIBITS	
A. The Freedom of Information Act	
B. The Privacy Act of 1974	
C. Confidential Commercial Information	
D. Office of Inspector General Policy Memorandums, Release of Official Information, dated May 12 and August 25, 1993	

CHAPTER 2905 - RELEASE OF OFFICIAL INFORMATIONSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter establishes the policies and procedures related to the release of information from official files in response to requests from the media, governmental entities, and the general public. It also applies to offering information from official files when there has been no specific request.
- 1-2. POLICY. **The only documents produced by the OIG that are public records are the Semiannual Reports and final audit reports as posted on the Office of the Inspector General (OIG) website.** The Office of Audits will release all other official information in accordance with the statutes and regulations that address freedom of information, privacy, and related topics and with OIG policy (Refer to Exhibit A for the Freedom of Information Act; Exhibit B for the Privacy Act; Exhibit C for regulations on Confidential Commercial Information; and Exhibit D for OIG policy).

SECTION 2. RELEASE OF OFFICIAL INFORMATION

- 2-1. GENERAL. Any individual, group, corporation, organization, government body, or any "person", may make a request for official information or express an interest in the activities or products of the Office of the Inspector General (OIG).

Front line staff members, (receptionists and administrative staff) who frequently come into contact with the general public, will typically be the recipients of verbal requests for official information. Written inquiries will often arrive addressed directly to the Inspector General (IG) or Assistant Inspector General for Audits (AIGA). However, an opportunity to receive a verbal request or written request for information exists for all Office of Audits (OA) personnel.

Generally speaking, OA staff members do not have the authority to respond directly to requests for the release of any official information and should, under no circumstances, offer to provide such information.

- 2-2. AUTHORITY TO RELEASE OFFICIAL INFORMATION.

- a. Final OIG Authority. The final authority to approve the release of official information on behalf of the OIG rests with the IG and the Deputy Inspector General (DIG).
- b. Delegations of Authority to the Office of Audits.
 - (1) Delegation to the AIGA and the Deputy Assistant Inspectors General for Audits. The IG has delegated authority to the AIGA and the Deputy Assistant Inspectors General for Audits (DAIGA) to release official information related to the operation of the OA **except** when the information is subject to the restrictions and processes of the Freedom of Information Act (FOIA), the Privacy Act, or is solicited by, or is to be provided to, the media. Sections 2-5. and 2-6. contain the guidelines that apply in those situations.
 - (2) Redelegation to Group Chiefs. Authority to respond to written and oral requests for official information from, or otherwise release official information to, inter- and intra-governmental entities has been redelegated to OA group chiefs **except** when the information requested is subject to the restrictions and processes of FOIA, the Privacy Act, is solicited by, or is to be provided to, the media, or involves Confidential Commercial

Information. Sections 2-5. and 2-6. contain the guidelines that apply in those situations.

In general, Group Chiefs should discuss all requests for official information with their DAIGA and/or the AIGA prior to its release.

- 2-3. REPORTS REQUIRED TO BE POSTED BY THE IG ACT. The IG Act requires the posting of copies of reports on the IG website. The OIG Reports Posting Procedures (located on (b) (7)(E) [REDACTED]) require that the AIGA provide a copy of the final audit report to the Office of Legal Affairs for redaction prior to the posting on the IG website.
- 2-4. RELEASING OFFICIAL INFORMATION. What official information can be released and by whom it can be released depends on the identity of the requester, or potential recipient, and the nature of the information requested, or to be released. The requesters, or potential recipients, listed in Section 2-1. fall into three broad categories: members of the media, governmental staff, and the general public. Section 2-5. describes how inquiries from, or releases of information to, each of these categories must be handled. Where special rules apply, such as with requests for, or release of, information subject to FOIA and the Privacy Act or requests, or releases, that involve Commercial Confidential Information, you will be referred to Section 2-6 for additional information.
- 2-5. GENERAL POLICY AND PROCEDURES.
- a. Media Inquiries. Disclosure of information at the request (or because of the expression of an interest in OA activities or products) of correspondents, publishers, television reporters, radio announcers, researchers, or other media journalists, requires the specific consent of the IG or DIG **prior** to release. Media inquiries are subject to the provisions of FOIA and the Privacy Act and to restrictions on the release of confidential commercial information (See Section 2-5. b.).

All members of the OA staff must refer any media contact involving OIG activities and work products to the Assistant Inspector General for Legal Affairs (AIGLA), immediately, on (202) 606-1200. The referral should provide the Office of Legal Affairs (OLA) with pertinent information, including such items as:

- (1) The type of information sought; such as applicable dates, report numbers, requests for the names of OA employees involved, title or name of the audited entities, and

- (2) the requester's name, title, organization, address, and telephone number.

If necessary, OLA will contact the media representative to further define the nature of the request and will advise the media representative that OPM's Office of Communications and Public Liaison has the responsibility to handle media relations for the OIG and to anticipate a forthcoming response from a representative from the Office of Communications and Public Liaison.

OLA will contact, without delay, the AIGA or DAIGA, describe the nature of the inquiry, present FOIA and/or Privacy Act implications; provide a forecast of the extent of media attention in response to the proposed reply by the OIG; or recommend referral of the inquiry to a more appropriate AIG, if applicable.

If appropriate, the AIGA or the DAIGA, in coordination with other knowledgeable OA staff members, will draft and recommend an official response to the media request. Note that, normally, we will not disclose any information of a substantive nature regarding audits in progress. Acknowledgement of the fact that a particular audit is underway may be made only if the question is first raised by the media; disclosure does not compromise OIG's ability to complete the audit effectively; and release of this information is determined to be consistent with OIG's overall programmatic interests.

The AIGA or the DAIGA will obtain the required specific approval of the IG or DIG prior to releasing official information. When substantial media attention is likely to result from the subsequent public announcement, the AIGA or DAIGA will also be responsible for recommending that the IG apprise the Director of the Office of Personnel Management (OPM) of his response.

Once the IG has approved the proposed response, OLA will then coordinate disclosure of the information with an Office of Communications and Public Liaison public information specialist.

OA staff members will only deal directly with the media when so instructed by the AIGA or DAIGA.

- b. Inter- and Intra-governmental Inquiries or Other Contacts. Verbal and written inquiries from staff at OPM or other governmental organizations requesting official information, or expressing an interest in OA activities or products, may be received by any OA staff member. When the release of official information is

involved, these should be referred to an appropriate group chief for response. However, Group Chiefs should discuss all requests for official information with their DAIGA and/or the AIGA prior to its release.

FOIA does not pertain to requests from governmental entities. The Privacy Act does apply to governmental requests except that the release of information from Privacy Act records to other governmental entities in connection with implementation of regulations or civil or criminal laws is authorized as a "routine" use; i.e., information regularly permitted to be used in an official manner by government agencies (Refer to Section 2-6. for additional information on the Privacy Act). Before release, the request must be discussed with AIGLA.

Confidential Commercial Information may be provided in response to inquiries from other governmental entities in accordance with the foregoing policies and procedures and without prior notice to, or approval of, the subject of the information, since its release in those circumstances is authorized by law. Examples of such lawful releases include providing information pursuant to another agency's audit or investigation; to an agency conducting a peer review of OIG or to the U.S. Government Accountability Office in connection with its audits; to Congress, including congressional committees and subcommittees; and to other OPM organizations in connection with their official responsibilities. The Trade Secrets Act's prohibition on release of Confidential Commercial Information without prior notice to the subject applies only if such release is not authorized by another law. Before release, the request must be discussed with AIGLA.

When Confidential Commercial Information is released, the document should contain the following warning: **This document may contain information protected by federal law (18 U.S.C. 1905); therefore, while this document is available under the Freedom of Information Act, caution needs to be exercised before releasing it to the general public.**

Responses to inquiries related to specific audits are subject to the following restrictions:

- (1) Ongoing Audits. Official information concerning ongoing audits is not releasable if such disclosure would impair the OIG's ability to complete the audit. **The group chief should ensure that all responses concerning the status of ongoing audits are accompanied by a cautionary warning that states that the information being provided does not reflect the final audit position of the OIG.**

- (2) Audit Documentation, Draft Reports, and Final Reports. Our general policy is not to release audit documentation, audit documentation products, or draft reports to government agencies. Portions of final reports which have been redacted prior to posting on the OIG website must be treated as FOIA material.
- c. Miscellaneous Public Inquiries or Other Contacts. Verbal and written requests for official information, or expressions of interest in OA activities or products, from the general public received by staff members should be referred to OLA for response.

The only documents produced by the OIG that are public records are the Semiannual Reports and final audit reports as posted on the Office of the Inspector General (OIG) website. When a request is made for a document which is not a public record, then the request must be processed under FOIA or Privacy Act standards (Refer to Section 2-5. for additional information).

2-6. SPECIAL CONSIDERATIONS.

- a. Privacy Act Inquiries. Examples of Privacy Act requests include such items as inquiries concerning: an individual's arrest records, discipline records, political affiliation records, physical measurements, visa numbers, social security numbers; and an employee's home addresses and/or telephone numbers, job performance records, employment applications, judicial misconduct reports, customer complaints to federal agencies, union membership card information, information on accident involvement, and/or other personal information. A copy of the Privacy Act of 1974 can be found in Exhibit B of this attachment.
<http://www.justice.gov/opcl/privstat.htm>

The Privacy Act applies to governmental requests **except** that the release of information from Privacy Act records to other governmental entities in connection with implementation of regulations or civil or criminal laws is authorized as a "routine" use; i.e., information regularly permitted to be used in an official manner by government agencies.

All Privacy Act information requests must be written and include a description of the information requested. While it is helpful if the requester cites the Privacy Act, it is not required. The request should be mailed, faxed, or e-mailed to the following:

U.S. Office of Personnel Management
Office of the Inspector General
Freedom of Information/Privacy Act Officer
1900 E Street NW.
Room 6400
Washington, D.C. 20415

FAX: (202) 606-2153

E-mail: OPMOIGFOIA@opm.gov

Verbal requests for Privacy Act information should be referred to the Assistant Inspector General for Legal Affairs at (202) 606-1200.

All requests for the release of Privacy Act information require immediate response and accountability. A project control sheet will announce a Privacy Act request and require submission of input from involved OA officials within two working days. Negative replies are also required.

- b. Requests for Freedom of Information Act Information. FOIA inquiries concern such items as: information concerning the OIG's organization chart and employee locations; the methods by which the public may obtain information, make submittals or requests, or obtain OA information concerning OIG decisions and recommendations; statements concerning the OIG's general objectives and methods by which its functions are channeled and determined, including the nature and requirement of all formal and informal OA procedures available; rules of procedure, descriptions of local forms available or the places at which local forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations; final audit reports; and or administrative staff manuals and instructions to staff that affect the public. OIG does not consider audit documentation or draft audit reports to be subject to release under the terms of FOIA.

The only documents produced by the OIG that are public records are the Semiannual Reports and final audit reports as posted on the Office of the Inspector General (OIG) website.

All FOIA requests must be written and include a description of the information requested. While it is helpful if the requester cites FOIA, it is not required. The request should be mailed, faxed, or e-mailed to the following:

U.S. Office of Personnel Management
Office of the Inspector General
Freedom of Information/Privacy Act Officer
1900 E Street NW.
Room 6400
Washington, D.C. 20415

FAX: (202) 606-2153

E-mail: OPMOIGFOIA@opm.gov

All requests for release of FOIA information require immediate response and accountability. A project control sheet will announce a FOIA request and require input from involved OA officials within two working days. Negative responses are also required.

Requests for copies of final audit reports under FOIA will be referred to the AIGLA at (202) 606-1200.

A copy of the Freedom of Information Act is located in Exhibit A of these guidelines. http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm Specific requests for FOIA information should be directed to the Assistant Inspector General for Legal Affairs at (202) 606-1200.

- c. Confidential Commercial Information. All requests for Confidential Commercial Information, except those received from other governmental entities and authorized by law, must be coordinated with the AIGLA at (202) 606-1200. Release of Confidential Commercial Information must be performed in accordance with the procedures established by 5 CFR 294.112. A copy of these procedures is provided as Exhibit C to assist you in performing this type of information release.
- 2-7. DOCUMENTING RECORDS/ACTIONS. Whenever official information is released, the responding OA official is responsible for documenting the appropriate files. A verbal response must be documented by a brief written summary of the official information released. This summary must include information concerning the name and affiliation of the requester, the requester's address and telephone number, and a synopsis of the request and response (indicating applicable dates).

THE FREEDOM OF INFORMATION ACT**5 U.S.C. § 552**

As Amended in 2002

§ 552. Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public--

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying--

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

Exhibit A
(Page 2 of 12)

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;

(C) administrative staff manuals and instructions to staff that affect a member of the public;

(D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and

(E) a general index of the records referred to under subparagraph (D);

unless the materials are promptly published and copies offered for sale. For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction, or copies of records referred to in subparagraph (D). However, in each case the justification for the deletion shall be explained fully in writing, and the extent of such deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of an index on request at a cost not to exceed the direct cost of duplication. Each agency shall make the index referred to in subparagraph (E) available by computer telecommunications by December 31, 1999. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if--

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

Exhibit A
(Page 3 of 12)

(3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a (4))) shall not make any record available under this paragraph to--

(i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or

(ii) a representative of a government entity described in clause (i).

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that--

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

**Exhibit A
(Page 4 of 12)**

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section--

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed \$250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo, provided that the court's review of the matter shall be limited to the record before the agency.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records

Exhibit A
(Page 5 of 12)

and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause is shown.

(D) Repealed by Pub. L. 98-620, Title IV, 402(2), Nov. 8, 1984, 98 Stat. 3335, 3357.

(E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

Exhibit A
(Page 6 of 12)

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--

(i) determine within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

(B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days, except as provided in clause (ii) of this subparagraph.

(ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C).

(iii) As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular requests--

(I) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

Exhibit A
(Page 7 of 12)

(III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.

(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(C)(i) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(ii) For purposes of this subparagraph, the term "exceptional circumstances" does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.

(iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing the request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.

(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.

Exhibit A
(Page 8 of 12)

(iii) This subparagraph shall not be considered to affect the requirement under subparagraph (C) to exercise due diligence.

(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records--

(I) in cases in which the person requesting the records demonstrates a compelling need; and

(II) in other cases determined by the agency.

(ii) Notwithstanding clause (i), regulations under this subparagraph must ensure--

(I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and

(II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.

(iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

(iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.

(v) For purposes of this subparagraph, the term "compelling need" means--

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

**Exhibit A
(Page 9 of 12)**

(vi) A demonstration of a compelling need by a person making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person's knowledge and belief.

(F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.

(b) This section does not apply to matters that are--

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by

Exhibit A
(Page 10 of 12)

an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and--

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

**Exhibit A
(Page 11 of 12)**

(d) This section does not authorize the withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States a report which shall cover the preceding fiscal year and which shall include--

(A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(B)(i) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and

(ii) a complete list of all statutes that the agency relies upon to authorize the agency to withhold information under subsection (b)(3), a description of whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;

(C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median number of days that such requests had been pending before the agency as of that date;

(D) the number of requests for records received by the agency and the number of requests which the agency processed;

(E) the median number of days taken by the agency to process different types of requests;

(F) the total amount of fees collected by the agency for processing requests; and

(G) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests.

(2) Each agency shall make each such report available to the public including by computer telecommunications, or if computer telecommunications means have not been established by the agency, by other electronic means.

(3) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Government Reform and Oversight of the House of Representatives and the Chairman and ranking minority member of the Committees on Governmental Affairs and the Judiciary of the

**Exhibit A
(Page 12 of 12)**

Senate, no later than April 1 of the year in which each such report is issued, that such reports are available by electronic means.

(4) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.

(5) The Attorney General of the United States shall submit an annual report on or before April 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

(f) For purposes of this section, the term--

(1) "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(2) "record" and any other term used in this section in reference to information includes any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.

(g) The head of each agency shall prepare and make publicly available upon request, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including--

(1) an index of all major information systems of the agency;

(2) a description of major information and record locator systems maintained by the agency; and

(3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

Go to: [DOJ FOIA Page](#) // [Justice Department Home Page](#)

Last Updated December 23, 2002

THE PRIVACY ACT OF 1974**5 U.S.C. § 552a**

As Amended

§ 552a. Records maintained on individuals

(a) Definitions

For purposes of this section--

- (1) the term "agency" means agency as defined in section 552(f) of this title;
- (2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) the term "maintain" includes maintain, collect, use or disseminate;
- (4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;
- (5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;
- (6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13;
- (7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

Exhibit B
(Page 2 of 25)

(8) the term "matching program"--

(A) means any computerized comparison of--

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of--

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(B) but does not include--

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

(iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social

Exhibit B
(Page 3 of 25)

Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches--

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1));

(9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term "non-Federal agency" means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or

Exhibit B
(Page 4 of 25)

any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) Conditions of disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the

Exhibit B
(Page 5 of 25)

United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.

(c) Accounting of Certain Disclosures

Each agency, with respect to each system of records under its control, shall--

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

Exhibit B
(Page 6 of 25)

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) Access to records

Each agency that maintains a system of records shall--

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and--

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either--

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from

Exhibit B
(Page 7 of 25)

the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) Agency requirements

Each agency that maintains a system of records shall--

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--

(A) the authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information

Exhibit B
(Page 8 of 25)

and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include--

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

Exhibit B
(Page 9 of 25)

- (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;
- (6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;
- (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;
- (8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;
- (9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;
- (10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;
- (11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an

Exhibit B
(Page 10 of 25)

opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) Agency rules

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall--

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)(1) Civil remedies

Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

Exhibit B
(Page 12 of 25)

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) Rights of legal guardians

For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)(1) Criminal penalties

Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this

Exhibit B
(Page 13 of 25)

section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

(j) General exemptions

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is--

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) Specific exemptions

Exhibit B
(Page 14 of 25)

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is--

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

Exhibit B
(Page 15 of 25)

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(1) Archival records

(1) Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of Title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the

Exhibit B
(Page 16 of 25)

requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m) Government contractors

(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of Title 31 shall not be considered a contractor for the purposes of this section.

(n) Mailing lists

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) Matching agreements -- (1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying--

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to--

Exhibit B
(Page 17 of 25)

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

(ii) applicants for and holders of positions as Federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

(E) procedures for verifying information produced in such matching program as required by subsection (p);

(F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;

(G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

(H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;

(I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

(J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and

(K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

(2)(A) A copy of each agreement entered into pursuant to paragraph (1) shall--

Exhibit B
(Page 18 of 25)

(i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and

(ii) be available upon request to the public.

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if--

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) Verification and Opportunity to Contest Findings

(1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until--

- (A)(i) the agency has independently verified the information; or
(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that--
(l) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

Exhibit B
(Page 19 of 25)

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of--

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) Sanctions

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless--

Exhibit B
(Page 20 of 25)

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) Report on new systems and matching programs

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) [Biennial report] Repealed by the Federal Reports Elimination and Sunset Act of 1995, Pub. L. No. 104-66, § 3003, 109 Stat. 707, 734-36 (1995), amended by Pub. L. No. 106-113, § 236, 113 Stat. 1501, 1501A-302 (1999) (changing effective date to May 15, 2000).

(t) Effect of other laws

(1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.

(2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

(u) Data Integrity Boards

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board--

Exhibit B
(Page 21 of 25)

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including--

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

Exhibit B
(Page 22 of 25)

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5)(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

Exhibit B
(Page 23 of 25)

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that--

(i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;

(ii) there is adequate evidence that the matching agreement will be cost- effective; and

(iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3)(D). Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and submission of a cost-benefit analysis and the reasons for granting the waiver.

(7) In the reports required by paragraphs (3)(D) and (6), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) Office of Management and Budget Responsibilities

The Director of the Office of Management and Budget shall--

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

Exhibit B
(Page 24 of 25)

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

The following section originally was part of the Privacy Act but was not codified; it may be found at § 552a (note).

Sec. 7(a) (1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to--

(A) any disclosure which is required by Federal statute, or

(B) any disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

The following sections originally were part of P.L. 100-503, the Computer Matching and Privacy Protection Act of 1988; they may be found at § 552a (note).

Sec. 6 Functions of the Director of the Office of Management and Budget.

(b) Implementation Guidance for Amendments -- The Director shall, pursuant to section 552a(v) of Title 5, United States Code, develop guidelines and regulations for the use of agencies in implementing the amendments made by this Act not later than 8 months after the date of enactment of this Act.

Sec. 9 Rules of Construction.

Nothing in the amendments made by this Act shall be construed to authorize--

Exhibit B
(Page 25 of 25)

(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;

(2) the direct linking of computerized systems of records maintained by Federal agencies;

(3) the computer matching of records not otherwise authorized by law; or

(4) the disclosure of records for computer matching except to a Federal, State, or local agency.

Sec. 10 Effective Dates.

(a) In General -- Except as provided in subsection (b), the amendments made by this Act shall take effect 9 months after the date of enactment of this Act.

(b) Exceptions -- The amendment made by sections 3(b) [Notice of Matching Programs -- Report to Congress and the Office of Management and Budget], 6 [Functions of the Director of the Office of Management and Budget], 7 [Compilation of Rules and Notices], and 8 [Annual Report] of this Act shall take effect upon enactment.

Go to: [DOJ FOIA Page](#) // [Justice Department Home Page](#)

Updated page September 26, 2003

**Exhibit C
(Page 1 of 3)****Confidential Commercial Information**

[Code of Federal Regulations]

[Title 5, Volume 1]

[Revised as of January 1, 2002]

From the U.S. Government Printing Office via GPO Access

[CITE: 5CFR294.112]

[Page 106-107]

CONFIDENTIAL COMMERCIAL INFORMATION FED REG V 57 140 07/21/92

Document Number: 5 CFR 294.112

Date: 21 Jul 92

Subject: Freedom of Information Act

Commercial Information - Disclosure

Information Disclosure - Exemptions

Information Disclosure - Availability of Information

Office of Personnel Management - Duties and Responsibilities

TITLE 5--ADMINISTRATIVE PERSONNEL

CHAPTER I--OFFICE OF PERSONNEL MANAGEMENT

PART 294--AVAILABILITY OF OFFICIAL INFORMATION--Table of Contents

Subpart A--Procedures for Disclosure of Records Under the Freedom of
Information Act

Sec. 294.112 Confidential commercial information.

(a) In general, OPM will not disclose confidential commercial information in response to a Freedom of Information Act request except in accordance with this section.

(b) The following definitions from Executive Order 12600, apply to this section:

(1) Confidential commercial information means records provided to the Government by a submitter that arguably contain material exempt from release under Exemption 4 of the Freedom of Information Act, 5 U.S.C. 552(b)(4), because disclosure could reasonably be expected to cause substantial competitive harm.

(2) Submitter means any person or entity who provides confidential commercial information, directly or indirectly, to OPM. The term includes, but is not limited to, corporations, state governments, and foreign governments.

(c) Submitters of information shall designate by appropriate markings, either at the time of submission or at a reasonable time thereafter, any portions of their submissions that they consider to be confidential commercial information. Such designations shall expire 10 years after the date of submission unless the submitter requests, and provides reasonable justification for, a designation period of greater duration.

Exhibit C
(Page 2 of 3)

(d) OPM shall, to the extent permitted by law, provide prompt written notice to an information submitter of Freedom of Information requests or administrative appeals if:

- (1) The submitter has made a good faith designation that the requested material is confidential commercial information, or
- (2) OPM has reason to believe that the requested material may be confidential commercial information.

(e) The written notice required in paragraph (d) of this section shall either describe the confidential commercial material requested or include as an attachment, copies or pertinent portions of the records.

(f) Whenever OPM provides the notification and opportunity to object required by paragraphs (d) and (h) of this section, it will advise the requester that notice and an opportunity to object are being provided to the submitter.

(g) The notice requirements of paragraph (d) of this section shall not apply if:

- (1) OPM determines that the information should not be disclosed;
- (2) The information has been lawfully published or officially made available to the public;
- (3) Disclosure of the information is required by law (other than 5 U.S.C. 552);

(4) The information was submitted on or after August 20, 1992, and has not been designated by the submitter as exempt from disclosure in accordance with paragraph (c) of this section, unless OPM has substantial reason to believe that disclosure of the information would result in competitive harm; or

(5) The designation made by the submitter in accordance with paragraph (c) of this section appears obviously frivolous; except that, in such a case, OPM shall, within a reasonable number of days prior to a specified disclosure date, notify the submitter in writing of any final administrative decision to disclose the information.

(h) The notice described in paragraph (d) of this section shall give a submitter a reasonable period from the date of the notice to provide OPM with a detailed written statement of any objection to disclosure. The statement shall specify all grounds for withholding any of the material under any exemption of the Freedom of Information Act. When Exemption 4 of the FOIA is cited as the grounds for withholding, the specification shall demonstrate the basis for any contention that the material is a trade secret or commercial or financial information that is privileged or confidential. It must also include a specification of any claim of competitive harm, including the degree of such harm, that would result from disclosure. Information provided in response to this paragraph may itself be subject to disclosure under the FOIA. Information provided in response to this paragraph shall also be subject to the designation requirements of paragraph (c) of this section. Failure to object in a timely manner shall be considered a statement of no objection by OPM, unless OPM extends the time for objection upon timely request from the submitter and for good cause shown. The provisions of this paragraph concerning opportunity to object shall not apply to notices of

**Exhibit C
(Page 3 of 3)**

administrative appeals, when the submitter has been previously provided an opportunity to object at the time the request was initially considered.

(i) OPM shall consider carefully a submitter's objections and specific grounds for nondisclosure, when received within the period of time described in paragraph (h) of this section, prior to determining whether to disclose the information. Whenever OPM decides to disclose the information over the objection of a submitter, OPM shall forward to the submitter a written notice, which shall include:

(1) A statement of the reasons why the submitter's disclosure objections were not sustained;

(2) A description of the information to be disclosed; and

(3) A specified disclosure date.

(j) OPM will notify both the submitter and the requester of its intent to disclose material a reasonable number of days prior to the specified disclosure date.

(k) Whenever a requester brings suit seeking to compel disclosure of confidential commercial information, OPM shall promptly notify the submitter.

[57 FR 32150, July 21, 1992]



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, D.C. 20415-0001

Exhibit D
(Page 1 of 13)

May 12, 1993

MEMORANDUM FOR ALL OIG EMPLOYEES

FROM: PATRICK E. MCFARLAND
INSPECTOR GENERAL *Patrick E. McFarland*

SUBJECT: Office of the Inspector General Policy on Release
of Official Information

This memorandum establishes OIG policy regarding the release of information from official files in response to requests from the media, governmental entities, and the general public.

1. POLICY

a. SCOPE

Unless specifically stated otherwise, these guidelines apply to release of information in both written or spoken form. They are not intended to impede the normal exchange of information necessary to conduct the ongoing business of OIG.

b. AUTHORITY TO RELEASE INFORMATION

The Inspector General (IG) and Deputy Inspector General (DIG) hold the final authority to determine the release of official information in OIG's possession. Except as otherwise noted, however, this authority is delegated to each Assistant Inspector General (AIG) and the Special Counsel for information within their respective program areas.

c. SUPPLEMENTARY INSTRUCTIONS

AIG's and the Special Counsel may issue supplementary instructions to their staffs, to the extent that they do not conflict with the policies stated in this memorandum.

d. APPLICABILITY OF STATUTES AND REGULATIONS

This policy does not supersede any statutes or regulations which address freedom of information, privacy, or related topics.

ALL OIG EMPLOYEES

2. MEDIA INQUIRIES

a. COVERAGE

The media are defined as newspapers, magazines, newsletters, television and radio. Any individual who is a reporter, columnist, researcher, or contributing party is included in this definition.

b. AUTHORITY TO RELEASE INFORMATION TO THE MEDIA

Release of any information to the media requires the prior specific approval of the IG or DIG.

c. POLICY

It is OIG's policy to respond fully and promptly to media requests for information regarding OIG activities, within the guidelines established by this document. Absent circumstances which may warrant the direct involvement of OIG staff (see paragraph d.3, below), all responses to non-FOIA inquiries from the media should be handled through OPM's Office of Communications.

d. PROCEDURES

1. Any media contact related to the activities and work products of the OIG will be referred immediately to the AIG whose program area is principally affected by the inquiry. If the query does not involve the Freedom of Information Act, the AIG should indicate that OPM's Office of Communications handles media relations for the OIG, and that a response to them will be forthcoming through that organization.

2. The cognizant AIG will formulate a recommended approach to the media request and, after approval by the IG or DIG, will coordinate with a public information specialist designated by the Office of Communications to assure that an appropriate response is made to the media inquiry.

3. Direct contact on substantive matters between OIG employees and members of the media will be considered only in the following circumstances: (1) the subject-matter to be dealt with is so technically complex that a public information specialist could not reasonably be expected to master it sufficiently; (2) direct involvement by an OIG employee is deemed necessary as a means of providing additional emphasis, credibility, or authoritativeness to the information; or (3) the Office of Communications recommends that OIG become directly involved.

ALL OIG EMPLOYEES

4. Due consideration must be given to the need to respond to expressions of interest from the media in a timely manner.

5. Where a probability exists of substantial media attention being generated in response to a proposed release of information by OIG, the IG may inform the Director of his plans in advance, as necessary to assure appropriate coordination of OPM's overall public information posture.

6. When a decision has been made regarding the manner in which a media inquiry will be handled, the cognizant AIG should assure its appropriate dissemination within OIG in order that other media representatives seeking the same information will be treated in an equivalent manner.

e. FOIA/PRIVACY ACT STATUS OF REQUESTS

Any media inquiries which are specifically submitted as FOIA requests, or which seek the release of specific documents, must be processed under FOIA procedures. All restrictions concerning disclosure of information maintained in Privacy Act systems of records apply fully to media requests.

f. AUDITS

1. Audits in progress. Normally, OIG will not disclose any information of a substantive nature regarding ongoing audit work. Acknowledgement of the fact that a particular audit is underway may be made only if: (1) the question is first raised by the media; (2) disclosure does not compromise OIG's ability to complete the audit effectively; and (3) release of this information is determined to be consistent with OIG's overall programmatic interests.

2. Completed audits. Final reports of completed audits may be released in response to media inquiries under FOIA, subject to redaction of any confidential commercial information which they contain, and other deletions of material as permitted by FOIA.

g. INVESTIGATIONS

1. Open investigations. No information will be released to the media pertaining to open investigations, nor will any acknowledgement be made as to the identity of persons or entities who are or may be the subjects of open investigations.

2. Closed investigations. Final investigative reports may be considered for release under FOIA. All appropriate redactions of material will be made to protect the integrity of OIG's investigative processes. Information regarding closed

ALL OIG EMPLOYEES

cases provided to the media in spoken form will not go beyond that which would be releasable through strict application of FOIA principles.

h. PROHIBITION ON RELEASE OF INFORMATION CONCERNING INFORMANTS, WHISTLEBLOWERS AND OTHER PROTECTED INDIVIDUALS

The names and personal identifying information of whistleblowers protected under the provisions of Public Law 101-12 or others to whom confidentiality has been granted by OIG will not be released without a waiver from the affected individual.

i. CONFIDENTIAL COMMERCIAL INFORMATION

Audit or investigative records which are deemed to contain confidential commercial information will be considered for release only under the procedures outlined in 5 CFR 294.112. "Confidential commercial information" is defined by that regulation to include records provided by any person or entity which may arguably contain material which is exempt from release under exemption 4 of the FOIA, on the basis that disclosure could cause substantial competitive harm.

j. CASES PENDING LEGAL ACTION

Information pertaining to cases pending legal action before federal, state, or local judicial systems may be released in response to media inquiries only upon approval of the government attorney handling the case. Such responses, when authorized, should be accompanied by a cautionary statement explaining the status of the case and the sensitivity of the information.

3. OFFICIAL GOVERNMENTAL INQUIRIES

a. COVERAGE

Inquiries are considered to be "governmental" if they: (1) originate from federal departments, agencies, entities, and corporations; the governments of states and U.S. possessions; or local governmental entities such as cities, counties, and townships; and (2) the requested information is to be used in connection with an official function of the governmental entity.

b. POLICY

All governmental requests will be considered on a case-by-case basis. It is the policy of OIG to foster a high degree of cooperation with audit and investigative units in other

ALL OIG EMPLOYEES

federal, state, and local government entities. Therefore, requests from such sources should be afforded the fullest possible responses, consistent with statutory and regulatory restrictions.

c. PROCEDURES

Requests received in writing will be assigned for action to the pertinent AIG or the Special Counsel for processing and response. Oral requests for information can be responded to as directed by the controlling AIG or the Special Counsel, in accordance with the policies outlined in this document. In order to assure accountability, a brief written summary of the transaction, including the name and governmental affiliation of the requester and a synopsis of the information requested and provided, should be placed with the record copy of the documents from which information was released.

d. FOIA/PRIVACY ACT STATUS OF REQUESTS

The FOIA does not pertain to requests from governmental entities; however, FOIA principles will be applied to the release of confidential commercial information (see section f, below). The Privacy Act does apply, but release of information from Privacy Act records systems to other governmental entities in connection with implementation of regulations or civil or criminal laws is authorized as a "routine" (i.e., regularly permitted) use. Any question regarding the Privacy Act implications of a proposed release of information should be directed to the OIG freedom of information/privacy act officer.

e. ONGOING AUDITS AND INVESTIGATIONS

Requests for information regarding audit or investigative work in progress should be granted wherever they do not compromise OIG's ability to complete the project in question. All such releases must be accompanied by a cautionary warning to the effect that the information may not reflect the final position of OIG on the matters at issue.

f. PROHIBITION ON RELEASE OF INFORMATION CONCERNING INFORMANTS, WHISTLEBLOWERS AND OTHER PROTECTED INDIVIDUALS

The names or other identifying information of whistleblowers protected under the provisions of Public Law 101-12, or others to whom confidentiality has been granted by OIG will not be released without a waiver from such persons.

ALL OIG EMPLOYEES

g. CONFIDENTIAL COMMERCIAL INFORMATION

Confidential commercial information may be released only in accordance with the procedures established in 5 CFR 294.112. Any request which involves such information must be coordinated with OIG's Freedom of Information/Privacy Act officer.

h. CASES PENDING LEGAL ACTION

Information pertaining to cases pending legal action before federal, state, or local judicial systems may be released in response to inquiries from other governmental entities only upon approval of the government attorney handling the case. Such responses, when authorized, should contain a cautionary statement explaining the status of the case and the sensitivity of the information.

4. INTRA-OPM INQUIRIES

Requests from other OPM offices for release of information held by OIG will be considered on the same basis as other governmental inquiries, except that material relating to an ongoing audits or investigations will not be released if disclosure would impair OIG's ability to successfully complete the work in question.

5. PUBLIC INQUIRIES

Any request for information not covered in the above sections will be considered as a public inquiry. When the requester seeks release of a document which is not a public record, the request must be handled under FOIA or Privacy Act standards. Generally, the only documents produced by OIG which are in the public domain are the semiannual reports.

6. ADMINISTRATION OF THE FOIA AND PRIVACY ACT IN OIG

a. RECEIPT OF REQUESTS

Administration of OIG's FOIA and Privacy Act responsibilities is centralized with the Freedom of Information/Privacy Act officer in the Office of Policy, Resources Management, and Oversight. Requesters to whom the FOIA or Privacy Act applies must place their inquiries in a written form which cites the Act under which the request is being made and describes the material being sought. The correspondence should be mailed or faxed to the following address:

ALL OIG EMPLOYEES

U.S. Office of Personnel Management
Office of the Inspector General
Freedom of Information/Privacy Act Officer
Room 6400
1900 E Street NW.
Washington, D.C. 20415
FAX: (202) 606-2153

b. IDENTIFICATION OF MATERIAL SUBJECT TO REQUESTS

All FOIA/Privacy Act requests will be tracked through the OIG project control system. The original request will be forwarded to the FOI/Privacy Act officer, and copies will be provided to the IG, DIG, the Executive Assistant, AIG's, and the Special Counsel. The project control sheets will contain the following statement:

FREEDOM OF INFORMATION REQUEST--PLEASE NOTIFY THE AIG/PRMO WITHIN 2 WORKING DAYS WHETHER YOUR OFFICE HOLDS DOCUMENTS WHICH MAY BE COVERED BY THE ATTACHED CORRESPONDENCE. NEGATIVE REPLIES ARE ALSO REQUIRED.

c. PREPARATION AND CLEARANCE OF RESPONSES

The FOI/Privacy officer will review all documents identified as being potentially covered by each request against the requirements of the applicable statute and will formulate a response for signature by the AIG/PRMO. Prior to signature, the response will be routed to each office which held documents covered by the request for review and clearance. Responses will not be cleared or reviewed by any official outside OIG prior to signature and issuance by OIG.

d. COPIES OF RESPONSES

A copy of each response will be provided to the OIG office(s) whose documents were covered by the request.

e. LEGAL ADVISORIES

The Special Counsel to the Inspector General will be available to provide informal advice on FOIA and Privacy Act issues to the FOIA/Privacy Act officer and AIG's. However, in order to maintain the counsel's independent standing to adjudicate FOIA/Privacy Act appeals, he/she will not be in the clearance chain for any initial release of information.

f. APPEALS

The Special Counsel will receive and adjudicate appeals from denials of OIG records issued by the AIG/PRMO. In accordance

ALL OIG EMPLOYEES

with the provisions of 5 CFR 294.110 (e), this appeal constitutes the final level of administrative review which is available with respect to OIG documents.

May 1993



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT

WASHINGTON, D.C. 20415-0001

Exhibit D
(Page 9 of 13)

August 25, 1993

MEMORANDUM FOR ALL OIG EMPLOYEES

FROM: PATRICK E. MCFARLAND
INSPECTOR GENERAL

SUBJECT: Revision to OIG Policy on Release of Official
Information

On August 5, 1993, the Special Counsel to the Inspector General issued a legal opinion regarding the releasability of confidential commercial information to other governmental entities. In brief, the opinion indicated that such material could be released without providing prior notice to and obtaining the approval of the subject of the information if the disclosure is "authorized by law," as that term is used by the Trade Secrets Act. Among the forms of legally authorized disclosure are releases to Congress, GAO, peer review organizations, OPM offices with program responsibility in the subject-matter area of the information, and other agencies conducting audits and investigations to which the information is relevant.

We have modified the OIG policy on release of official information to reflect the impact of the Special Counsel's opinion, and have attached revised pages 5 through 8 to the policy statement which was issued on May 12, 1993. You should substitute these pages for the ones appearing in the earlier document. Please also bear in mind that OIG policy regarding disclosures of confidential commercial information to the media or the general public under the Freedom of Information Act has not changed.

If you have any questions regarding the impact of the Trade Secrets Act, contact (b) (6)

Attachment

ALL OIG EMPLOYEES

of cooperation with audit and investigative units in other federal, state, and local government entities. Therefore, requests from such sources should be afforded the fullest possible responses, consistent with statutory and regulatory restrictions.

c. PROCEDURES

Requests received in writing will be assigned for action to the pertinent AIG or the Special Counsel for processing and response. Oral requests for information can be responded to as directed by the controlling AIG or the Special Counsel, in accordance with the policies outlined in this document. In order to assure accountability, a brief written summary of the transaction, including the name and governmental affiliation of the requester and a synopsis of the information requested and provided, should be placed with the record copy of the documents from which information was released.

d. FOIA/PRIVACY ACT STATUS OF REQUESTS

The FOIA does not pertain to requests from governmental entities. The Privacy Act does apply, but release of information from Privacy Act records systems to other governmental entities in connection with implementation of regulations or civil or criminal laws is authorized as a "routine" (i.e., regularly permitted) use. Any question regarding the Privacy Act implications of a proposed release of information should be directed to the OIG freedom of information/privacy act officer.

e. ONGOING AUDITS AND INVESTIGATIONS

Requests for information regarding audit or investigative work in progress should be granted wherever they do not compromise OIG's ability to complete the project in question. All such releases must be accompanied by a cautionary warning to the effect that the information may not reflect the final position of OIG on the matters at issue.

f. PROHIBITION ON RELEASE OF INFORMATION CONCERNING INFORMANTS, WHISTLEBLOWERS AND OTHER PROTECTED INDIVIDUALS

The names or other identifying information of whistleblowers protected under the provisions of Public Law 101-12, or others to whom confidentiality has been granted by OIG will not be released without a waiver from such persons.

g. CONFIDENTIAL COMMERCIAL INFORMATION

Confidential commercial information may be provided in

ALL OIG EMPLOYEES

response to inquiries from other governmental entities in accordance with the foregoing policies and procedures and without prior notice to or approval of the subject of the information, since its release in those circumstances is authorized by law. Examples of such lawful releases include providing information (1) pursuant to another agency's audit or investigation; (2) to an agency conducting a peer review of OIG or to GAO in connection with its audits; (3) to Congress, including congressional committees and subcommittees; and (4) to other OPM organizations in connection with their official responsibilities. The Trade Secrets Act's prohibition on release of confidential commercial information without prior notice to the subject applies only if such release is not authorized by another law.

h. CASES PENDING LEGAL ACTION

Information pertaining to cases pending legal action before federal, state, or local judicial systems may be released in response to inquiries from other governmental entities only upon approval of the government attorney handling the case. Such responses, when authorized, should contain a cautionary statement explaining the status of the case and the sensitivity of the information.

4. INTRA-OPM INQUIRIES

Requests from other OPM offices for release of information held by OIG will be considered on the same basis as other governmental inquiries, except that material relating to an ongoing audits or investigations will not be released if disclosure would impair OIG's ability to successfully complete the work in question.

5. PUBLIC INQUIRIES

Any request for information not covered in the above sections will be considered as a public inquiry. When the requester seeks release of a document which is not a public record, the request must be handled under FOIA or Privacy Act standards. Generally, the only documents produced by OIG which are in the public domain are the semiannual reports.

6. ADMINISTRATION OF THE FOIA AND PRIVACY ACT IN OIG

a. RECEIPT OF REQUESTS

Administration of OIG's FOIA and Privacy Act responsibilities is centralized with the Freedom of Information/Privacy Act officer in the Office of Policy, Resources Management, and

ALL OIG EMPLOYEES

Oversight. Requesters to whom the FOIA or Privacy Act applies must place their inquiries in a written form which cites the Act under which the request is being made and describes the material being sought. The correspondence should be mailed or faxed to the following address:

U.S. Office of Personnel Management
Office of the Inspector General
Freedom of Information/Privacy Act Officer
Room 6400
1900 E Street NW.
Washington, D.C. 20415
FAX: (202) 606-2153

b. IDENTIFICATION OF MATERIAL SUBJECT TO REQUESTS

All FOIA/Privacy Act requests will be tracked through the OIG project control system. The original request will be forwarded to the FOI/Privacy Act officer, and copies will be provided to the IG, DIG, the Executive Assistant, AIG's, and the Special Counsel. The project control sheets will contain the following statement:

FREEDOM OF INFORMATION REQUEST--PLEASE NOTIFY THE AIG/PRMO WITHIN 2 WORKING DAYS WHETHER YOUR OFFICE HOLDS DOCUMENTS WHICH MAY BE COVERED BY THE ATTACHED CORRESPONDENCE. NEGATIVE REPLIES ARE ALSO REQUIRED.

c. PREPARATION AND CLEARANCE OF RESPONSES

The FOI/Privacy officer will review all documents identified as being potentially covered by each request against the requirements of the applicable statute and will formulate a response for signature by the AIG/PRMO. Prior to signature, the response will be routed to each office which held documents covered by the request for review and clearance. Responses will not be cleared or reviewed by any official outside OIG prior to signature and issuance by OIG.

d. COPIES OF RESPONSES

A copy of each response will be provided to the OIG office(s) whose documents were covered by the request.

e. LEGAL ADVISORIES

The Special Counsel to the Inspector General will be available to provide informal advice on FOIA and Privacy Act issues to the FOIA/Privacy Act officer and AIG's. However, in order to maintain the counsel's independent standing to

ALL OIG EMPLOYEES

adjudicate FOIA/Privacy Act appeals, he/she will not be in the clearance chain for any initial release of information.

f. APPEALS

The Special Counsel will receive and adjudicate appeals from denials of OIG records issued by the AIG/PRMO. In accordance with the provisions of 5 CFR 294.110 (e), this appeal constitutes the final level of administrative review which is available with respect to OIG documents.

August 1993

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2910

Office of Audits Subpoena Issuances

CHAPTER 2910 - OFFICE OF AUDITS SUBPOENA ISSUANCES

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. CONDITIONS LEADING TO SUBPOENA ISSUANCES	
2-1. General.....	2
2-2. Categories of Records.....	2
SECTION 3. DENIAL OF ACCESS TO RECORDS	
3-1. Initial Request.....	3
3-2. Categories of Records.....	3
SECTION 4. ISSUING A SUBPOENA FOR DENIED RECORDS	
4-1. Coordination with the Counsel to the Inspector General.....	5
4-2. Coordination with Contracting Officer.....	5
4-3. Coordination with OIG Investigations.....	5
SECTION 5. PREPARING THE SUBPOENA	
5-1. Inspector General Subpoena Authority.....	7
5-2. Issuing Subpoenas.....	7
5-3. Method of Delivery of Subpoena.....	9
SECTION 6. FAILURE TO COMPLY	
6-1. Failure to Comply.....	12
EXHIBITS	
A. Memorandum to Request Issuance of a Subpoena.....	13

CHAPTER 2910 - OFFICE OF AUDITS SUBPOENA ISSUANCESSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides guidance to be followed by auditors within the Office of Audits (OA) when seeking subpoena issuance on behalf of the Inspector General to an audited entity that is denying official representatives from the Office of the Inspector General (OIG) access to their records. Where fraud or illegal acts are suspected, the policy and procedures in Chapter 2325 (Fraud, Illegal Acts, and Abuse) apply.
- 1-2. POLICY. OA Staff will apply for subpoena issuance to obtain access to necessary records when the audited entity has denied all reasonable requests to provide the necessary records and the records are deemed necessary to conduct the audit. All subpoena issuances must be coordinated with the Counsel to the Inspector General (CIG).

SECTION 2. CONDITIONS LEADING TO SUBPOENA ISSUANCES

- 2-1. GENERAL. These procedures are applicable only after OIG auditors have exhausted all other means at their disposal to obtain records necessary to successfully complete audits initiated under the jurisdiction of the OIG. Subpoenas may be issued by the Inspector General only for records related to OPM programs.
- a. With respect to its mandated responsibilities, the OIG has a right of access to all records necessary to perform audits under its jurisdiction.
 - b. There are four basic categories of records subject to subpoena procedures (see 2-2. below). In addition, OA staff can obtain information in connection with audit functions from federal, state, and local governmental agencies and from contractors or subcontractors.
- 2-2. CATEGORIES OF RECORDS. Generally, the OIG subpoena power applies to the following basic categories of records:
- a. Business records: The Inspector General Act enables the OIG to require production of any business record, even those that are not normally made available under the audit clause of a contract. Furthermore, records may be obtained from a business, subcontractor, or others who may not be subject to the audit clause of a particular contract.
 - b. Personal records: An individual can be required to produce records in his or her personal possession, including tax returns, bank statements, and employment records. For example, personal records of a corporate officer can be obtained, in addition to business records of the corporation.
 - c. Financial Institution records: Banks, saving institutions, credit unions, loan companies, and credit card companies can be required to produce their records and those of their customers. In many situations, however, the Right to Financial Privacy Act of 1978, which requires customer notice, is applicable.
 - d. Government records: A state, municipal, or quasi-governmental body or agency can be required to produce relevant documents. The OIG subpoena power **is not** available to obtain records and information from other federal agencies.

SECTION 3. DENIAL OF ACCESS TO RECORDS

- 3-1. INITIAL REQUEST. An initial request for records may be either verbal or written. Requests should be documented in the audit documentation in accordance with procedures for documenting evidence contained in Chapter 2220, Audit Documentation and Files. If the first request is denied, the audit documentation should be documented to reflect the denial. Appropriate action after a denial of access depends on whether the records are subject to subpoena and/or should be available under the audit clause of a contract.
- 3-2. CATEGORIES OF RECORDS. The following procedures apply to requests for records:
- a. Records not subject to subpoena. Records of federal agencies cannot be subpoenaed by the OA.
 - (1) After an initial denial of access to a federal agency's records, the OA will prepare an administrative request for the records.
 - (2) The request should originate from the Inspector General and should be addressed to the head of the federal agency. A properly executed request should describe the specific information sought, the results of the initial request, and provide justification for the request. It must be cleared by the CIG. Unreasonable denials are reported to Congress.
 - b. Records subject to subpoena. OIG subpoenas, enforceable by order of a U.S. District Court, may be issued for non-federal government, business, personal, and financial institution records. The subpoena can require the production of all information, records, documents, reports, answers, papers, and other data necessary in the performance of functions assigned by the Inspector General Act. A subpoena is used only after all other available means of obtaining the information have been exhausted.
 - (1) Where an audited entity denies the OIG access to records subject to subpoena procedures, the OA should send a written request to the audited entity citing the audit clause, explaining that the clause gives the OIG authority to examine and audit the records requested.

- (2) Although it is not mandatory to send the request via registered or certified mail, it is desirable to do so since it provides proof of receipt by the audited entity and is helpful in the event that we need to bring a subpoena enforcement action.
- (3) The request should impose a reasonable deadline for the audited entity response.
 - (i) Reasonableness depends on the circumstances of each case. The auditor should evaluate such factors as the volume of documents requested and consider the estimated time needed for the audited entity to retrieve the records.
 - (ii) Any deadline imposed should be reviewed by the CIG for reasonableness.
 - (iii) Any deadline given is not legally binding and is, therefore, negotiable by the audited entity.
 - (iv) If we determine that a deadline imposed is reasonable and the audited entity thereafter objects, we should subpoena the documents.
- (4) It is discretionary as to whether we advise the audited entity that non-compliance with the written request for access to records will result in issuance of a subpoena. If an audited entity appears to be taking a strong position against granting OIG access to records and needs to be advised of the full range of OIG authority, informing the audited entity of our subpoena power may make the request more forceful.
- (5) A log should be kept showing the date the written request was sent, the deadline for response, and any other correspondence or discussions that take place between the audited entity and the OA concerning access to records. Copies of letters sent or received, registered or certified mail receipts and memoranda of conversations should also be retained.

SECTION 4. ISSUING A SUBPOENA FOR DENIED RECORDS.

- 4-1. Coordination with the Counsel to the Inspector General. Any proposed issuance of an OIG subpoena must be coordinated with the CIG.
- a. Coordination with the CIG should be requested in writing. Memorandums should be addressed to the CIG and prepared for the signature of the Deputy Assistant Inspector General for Audits (DAIGA). They must be submitted through normal clearance channels.
- (1) Requests should provide background information on the situation giving rise to the need to issue a subpoena and, as appropriate, identify the audited entity involved, the nature of the records being denied, and the section(s) of law or regulation in question. The memorandum should summarize differing positions on the issue and should provide copies of relevant documents.
 - (2) Requests should indicate the date by which a response is needed, if appropriate.
 - (3) Requests should include a point of contact (and telephone number) in the event the CIG needs additional information in order to respond.
- 4-2. Coordination with Contracting Officer. If an audited entity refuses to provide records, the OA should inform the contracting officer of this refusal. If the contracting officer fails to gain access to the records, a subpoena should be issued under the audit clause of the OPM contract.

The OA need not involve the contracting officer in attempts to gain access to audit records unless it is determined that intervention by the contracting officer would be useful.

- 4-3. Coordination with OIG Investigations. The OA should coordinate with the OIG Office of Investigations (OI) in all cases where the withholding of records gives the appearance that criminal or civil fraud may be the motivating factor for withholding the requested information.

In any event, contact with OI should only be initiated by an OA management official, a Group Chief, or their designee. Individual auditors are not authorized to request OI assistance on subpoena issuances. Where OI assistance or advice is considered to be

necessary, the auditor will discuss such OI involvement with his/her supervisor and the supervisor will initiate coordination as necessary.

SECTION 5. PREPARING THE SUBPOENA

- 5-1. INSPECTOR GENERAL SUBPOENA AUTHORITY. The Inspector General Act authorizes the OIG to obtain by subpoena all information, documents, reports, records, accounts, papers, and other data and documentary evidence necessary to perform functions assigned to the OIG by the Inspector General Act.
- a. When a document or record is available under the audit clause of a contract, attempts to obtain the documents by reference to that authority should be made.
 - b. The clause contained in the Federal Acquisition Regulations (FAR), 48 CFR, paragraph 52.215-2, which is included in Federal Employee Health Benefits Program (FEHBP) contracts, should be cited as giving the OA authority to examine FEHBP carrier's records.
- 5-2. ISSUING SUBPOENAS. A subpoena should be used only after other available means of obtaining the information have been exhausted. However, the auditor may use a subpoena to obtain information that will augment, clarify, or amplify documents already obtained through subpoena power. Auditors seeking to issue a subpoena for an audited entity's personal records must obtain the approval of the DAIGA.
- a. In situations where a subpoena must be used to obtain documents that should have been provided under the contract, the AIGA and the CIG should consider referral to the contracting officer for appropriate contract action.
 - b. In issuing subpoenas, the auditor needs to specifically define the documents needed and show that a right to access is required. If the subpoenaed party files a motion to quash the subpoena, the OIG must be able to demonstrate that the information cannot be obtained through normal procedures. However, a number of circumstances could justify the issuance of a subpoena on a more immediate basis. These circumstances include the immediate need to obtain documents to prevent their loss, alteration, or destruction. In complex audits, it may be necessary to issue numerous subpoenas at various stages of the audit in order to fully develop the audit issue.
 - c. Auditors should consult with the AIGA and the CIG as early as possible when considering use of a subpoena. Early discussions with the AIGA and CIG can help significantly in determining the appropriateness of a subpoena, considering alternative means of acquiring needed materials, and in framing and processing the subpoena request as well as the subpoena itself. The CIG and the Auditor-In-Charge

or Team Leader will determine whether the subpoena should be served personally by the auditor or sent by registered or certified mail. In either case, the subpoena is served with an Appendix which outlines the items the auditor is seeking (see Attachment A).

- d. When it has been determined that the OA will issue a subpoena for records, the AIGA serves as the focal point for all matters relating to the use and issuance of OIG subpoenas. All requests for subpoenas must be processed in accordance with procedures set forth below and must be reviewed and approved by the CIG prior to being forwarded to the Inspector General. The Group Chief or designee is responsible for ensuring preparation of all necessary subpoena documentation, attachments, and appendices describing the documents sought and a memorandum to the Inspector General requesting approval of the subpoena (see Exhibit A for a sample subpoena request).
- (1) Requests for subpoenas should contain the information listed below. A sample memorandum is provided as a format in Exhibit A.

- Background of Subject Matter Under Audit

This section sets forth a concise history of the audit to date. It includes the authority for the audit, an identification of the contracts or records and individuals involved, the ultimate goal of the audit, and identification of all known agencies that may be conducting a similar or joint audit or investigation.

- Description of Items

This section describes as precisely as possible those items that are to be obtained by the subpoena. While individual documents need not be identified, documents should be divided into certain categories, e.g., payroll records, payment invoices, bank statements, or income tax returns, and identified as completely as possible by date and party. In some cases, certain individual documents should be identified.

In consultation with the CIG, consideration should be given to use of the phrase "including but not limited to ..." to assure that both specifically known documents and other relevant materials that may not be individually known or identifiable are obtained. If appropriate, the document categories should be cross-referenced to a particular contract or

record. The auditor should remember that a subpoena request need not be all inclusive. If subsequent audit work shows that other documents are needed or that other parties are involved, additional subpoenas may be issued.

- Justification for Subpoena Request

This section explains why the documents cannot be obtained by other means. Any lack of cooperation by the party under audit or the holder of the records should be discussed. The request should specify the particular audit goals that will be furthered by the subpoena. In requiring the production of documents and information by subpoena, the OIG is not required to determine that there is probable cause to believe that a violation of criminal or civil statute or administrative regulations has been committed, and that the materials sought constitute evidence of such violation. The OIG only needs to determine that the items sought are reasonably necessary to further proper OIG audit activities.

- Time and Place for Return of Service

The requestor should establish a date, time, method of delivery, and a location for the delivery of the subpoenaed documents. Where delivery to OPM is impractical, arrangements may be made to allow return at another appropriate federal facility.

5-3. METHOD OF DELIVERY OF SUBPOENA. In serving subpoenas the CIG, in conjunction with the requesting Auditor-In-Charge or Team Leader, selects a due date for compliance with the subpoena. In most cases, the date should be at least 10 calendar days after the date of service. The CIG and the Auditor-In-Charge or Team Leader determine whether the subpoena should be served personally at the corporate location or sent by registered or certified mail.

- a. If service is executed by mail, the subpoena is mailed with Attachment A to the parties concerned. If personal service is chosen, the subpoena is given to the requesting Auditor-In-Charge or Team Leader to serve. The auditor then delivers the subpoena to the addressee as expeditiously as possible.
- b. Personal service upon a corporation is made during business hours and to the addressee. The auditor should obtain the addressee's signature to verify delivery. If the addressee is unavailable, a corporate officer or the corporate registered agent for

service of process will suffice. If an individual other than the addressee receives the subpoena, the auditor should obtain the recipient's signature, and then execute the remaining portions of the Certificate of Return of Service, and place it in the audit documentation.

- c. Cases in which the subpoenaed party seeks modifications to the subpoena, or in which the subpoenaed party is represented by counsel, are referred through the CIG. In all cases involving a subpoena, close coordination and consultation between the auditor and CIG are maintained.
 - (1) Modifications in the scope and location of return of documents subpoenaed may be accomplished by mutual agreement between the recipient and the OIG. Prior to the date of return, the auditor may be asked to examine the documents on the premises of the recipient to verify the existence and volume of the documents sought.
 - (2) The recipient of a subpoena is required to provide the requested documents on the date and time specified. The requesting auditor should be prepared to receive the documents on the specified date and time, and have adequate personnel resources available to begin complete examination. While no precise time limits can be set for the completion of the examination of the records, the requesting auditor will examine and analyze all records as expeditiously as possible.
 - (a) Original documents are normally obtained unless the respondent can effectively demonstrate that the absence of the original documents will act as a major impediment to the operation of his or her business. In such cases, the auditor may accept certified copies in lieu of originals. However, the original records must be made available for verification if required by the auditor. Any questions should be referred to the CIG.
 - (b) At the outset of any examination of the documents, it may be difficult to determine which, if any, of the documents will be used as evidence in a resulting civil, criminal, or administrative proceeding. Therefore, the auditor must be aware of the need to maintain a chain of custody.
 - (c) Upon receipt, subpoenaed documents should be marked individually or by category and assigned an exhibit number. The auditor will examine each record and determine which records are to be retained for later use, and which records may be returned to the respondent.

- (d) Any record that may serve as evidence in a resulting civil, criminal, or administrative proceeding is retained until all proceedings have been exhausted. Records not needed for potential use in such proceedings will be returned to the respondent. A receipt will be obtained for all documents returned to the respondent.

SECTION 6. FAILURE TO COMPLY

- 6-1. FAILURE TO COMPLY. When a subpoenaed party refuses to provide documents as required by a subpoena, the auditor will inform the AIGA and CIG immediately. CIG is responsible for resolving such cases and for initiating subpoena enforcement actions where necessary.

EXHIBIT A

Memorandum to Request Issuance of a Subpoena

MEMORANDUM FOR [NAME OF INCUMBENT]
Inspector General

THRU: [NAME OF INCUMBENT]
Assistant Inspector General
for Audits

FROM: [AUDITOR]

SUBJECT: Request for Issuance of a Subpoena

I request that you issue a subpoena in the matter described below:

1. Authority: IG Act of 1978, 5 U.S.C. App. I, et seq.
2. OIG audit number: **(Use ARTS audit report number)**
3. Nature of the inquiry: Audit
(Check one) Joint audit/investigation
 Other
4. OPM office and/or program:
5. Subject(s) of inquiry :**(Name and title of person or organization)**
6. Name of person **(and title, if person is to be subpoenaed in representative capacity or entity to be subpoenaed):**
7. Address :**(Name, organization, complete address, and zip code)**

08/15

(NAME OF INCUMBENT)

2

8. Relationship of person/entity to be subpoenaed to subject of inquiry: **(Complete if applicable)**

9. Background of entity/program involved. **(Attach brief narrative)**

10. Purpose(s) of subpoena: **(To obtain records, etc.)**

11. Description of records sought. **(Attachment A)**

12. Are records available under statute, regulation, or audit access clause of a contract or other agreement?

Yes No **(Check one)**

If "yes" - Identify authority for access to records.

13. Have efforts been made to obtain records by means other than subpoena?

Yes No **(Check one)**

If so, how and with what results?

If not, why not?

14. Is the person/entity to be subpoenaed the subject of any non-OIG investigation or any civil, criminal, or administrative proceedings?

Yes Do Not Know **(Check one)**

If yes, describe:

15. Has the subject of this inquiry been discussed with the FBI, a United States Attorney's Office, or the Department of Justice in Washington, D.C.?

08/15

(NAME OF INCUMBENT)

3

Yes No (Check one)

If "yes" - Explain time and nature of discussions.

16. OIG employee to receive the records: (Name of auditor)

17. Location for in-person production of records: (If applicable)

18. Will production of records be permitted by mail?

Yes No (Check one)

If yes, explain:

19. Date and time for production: (Discuss with Special Counsel)

[SECTIONS 20, 21, AND 22 MUST BE COMPLETED]

FOR FRONT OFFICE USE (Group Chief or designee should initial and date here)

20. Approved by AIGA: Yes No
Initials and date:
Comments, if any:

21. Cleared by Special Counsel: Yes No
Initials and date:
Comments, if any:

22. Approved by IG or Deputy IG: Yes No
Initials and date:
Comments, if any:

ATTACHMENT A

In this section, outline the specific items subpoenaed. This may include any additional records or documents related to the request.

Include the names and addresses of individuals or companies you are seeking information about. It could include specialized data like certain time frames, item numbers, or other identifying information.

The attachment must be clear and concise to enable the reader to clearly understand exactly what the subpoena is asking for.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2915

**Requesting Legal Opinions and
Interpretations**

CHAPTER 2915 - REQUESTING LEGAL OPINIONS AND INTERPRETATIONS

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. LEGAL OPINIONS AND INTERPRETATIONS	
2-1. General.....	2
2-2. Making the Request.....	2
2-3. Responses.....	3
2-4. Emerging Issues.....	3

CHAPTER 2915 - REQUESTING LEGAL OPINIONS AND INTERPRETATIONSSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter provides guidance to be followed when legal opinions or interpretations are needed by the OIG Office of Audits (OA).
- 1-2. POLICY. All requests for legal opinions and interpretations should be directed to the Office of Legal Affairs (OLA). The OLA protects the independence of this office. OPM's Office of General Council (OGC) will not be consulted except with express permission of OLA.

SECTION 2. LEGAL OPINIONS AND INTERPRETATIONS

- 2-1. GENERAL. Auditors may find it necessary to rely on the work of the OLA to (1) determine those laws and regulations that are significant to the audit objectives, (2) design tests of compliance with laws and regulations, or (3) evaluate the results of those tests. Auditors also may find it necessary to rely on the work of the OLA when audit objectives require testing compliance with provisions of contracts or grant agreements. Therefore, procedures are necessary to ensure that legal opinions and interpretations from the OLA are properly documented in related audit documentation and other OA files. Use of these procedures also will ensure that opinions and interpretations that may impact more than one audit group are disseminated appropriately. These procedures do not apply to routine requests for legal citations or for Lexis searches, which can be handled through informal contacts with the OLA, or for other routine matters which OLA advises that the provisions of Section 2-2 below need not be used.
- 2-2. MAKING THE REQUEST. The following procedures apply to requests for legal opinions and interpretations from OLA.
- a. Requests must be submitted in writing.
 - b. Memorandums requesting legal opinions and interpretations should be addressed to the Assistant Inspector General for Legal Affairs and prepared for the signature of the Deputy Assistant Inspector General for Audits (DAIGA). They must be submitted through normal clearance channels.
 - c. Requests should provide background information on the situation giving rise to the request and, as appropriate, identify the section(s) of law or regulation in question; summarize differing positions on the issue; and provide copies of relevant documents.
 - d. Requests should indicate the date by which a response is needed, if appropriate.
 - e. Requests should include a point of contact (and telephone number) in the event the OLA needs additional information in order to respond.
 - f. When the OLA determines that an official agency interpretation of a statute or regulation is needed, the OLA will prepare a memorandum from the Inspector General to the OGC.

2-3. RESPONSES.

- a. The OLA will address responses to the DAIGA. The DAIGA will determine the appropriate distribution for the responses.
- b. A copy of the response will be filed in the related audit documentation or subject file.

2-4. EMERGING ISSUES. In order to ensure that the OLA keeps abreast of emerging issues, OA staff members should inform the OLA of all contacts with OGC. For example, if an auditor attends a meeting with OPM and OGC staff to discuss issues identified during an audit, the auditor will prepare a brief summary of the meeting and submit it to the OLA through the DAIGA. In addition, OLA should be informed if it is anticipated that an OGC attorney or outside counsel will attend a meeting with an auditor. If an OLA representative attends the meeting, a meeting summary for OLA does not need to be prepared unless one is requested.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2920

Career Enhancement

CHAPTER 2920 - CAREER ENHANCEMENT

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. ESTABLISHING THE CAREER ENHANCEMENT PLAN	
2-1. Background.....	2
2-2. Initiating the Enhancement Plan.....	2
2-3. The First Enhancement Plan Appointment.....	2
2-4. Plan Implementation.....	3
EXHIBITS	
A. OPM-OIG Office of Audits Guidelines for Developing a Career Development Plan	
B. OPM-OIG Office of Audits Career Development Action Plan	

CHAPTER 2920 - CAREER ENHANCEMENTSECTION 1. GENERAL1-1. PURPOSE.

Office of Inspector General (OIG), Office of Audits (OA) management and staff desire a formalized program to assist all staff members in identifying and pursuing individual career goals. To enhance their professional skills and careers, each staff member is encouraged to develop an individualized training program consisting of formal training courses, on-the-job assignments, and cross training within the office, consistent with achieving one year and five year goals established by each individual. The program should encompass the training opportunities as outlined in Chapter 2205 (Quality Control and Quality Assurance), as well as the GAS continuing education requirements.

1-2. POLICY.

OIG OA managers and supervisors will be available to assist individual OA staff members in identifying and pursuing a career enhancement program to attain one year and five year goals established by each individual. After establishment of a career enhancement plan, the OA will, as resources and workloads permit, accommodate each enhancement plan through formal training, on-the-job assignments, and cross training within the office.

SECTION 2. ESTABLISHING THE CAREER ENHANCEMENT PLAN2-1. BACKGROUND.

Highly motivated and qualified staff are critical to the on-going and future success of the audit office. In order to meet the needs of the OA and to promote team work and employee morale within the office, the OA has determined that it is desirable to offer each OA staff person an opportunity to establish career enhancement goals and for OA management to participate in the development and execution of the enhancement plan. To ensure that the office and individual staff members meet their collective and individual objectives, the OA will assist, to the extent resources and work load demands permit, in successful implementation of staff career enhancement goals. Responsibility for initiating a career enhancement plan will be with the staff person; responsibility for implementing an established plan will be the joint responsibility of OA management and individual employees.

2-2. INITIATING THE ENHANCEMENT PLAN.

Participating in the career enhancement policy will be on a voluntary basis and should be initiated by the employee. Career enhancement plans are fluid and should be amended as necessary to meet the needs and goals of the staff member. Each employee interested in developing an enhancement program may initiate the process at any time by making an appointment with his/her supervisor. Supervisors will meet with the staff member as soon as possible, but, in no event, more than two weeks from the date of the request.

2-3. THE FIRST ENHANCEMENT PLAN APPOINTMENT.

- a. The employee is expected to be prepared to initiate a career enhancement plan when attending the first appointment with his/her supervisor. The employee should be prepared to identify his/her one year and five year goals and have a general plan to achieve the goals in mind. The employee, on a preliminary basis, should identify and verify the offering of formal training courses consistent with achieving both short and long term goals. The employee should further be prepared to discuss the types of on-the-job training assignments that would be necessary to help meet the employee's goals. In addition, the employee should be able to identify desirable cross-training involving work in organizations outside the employee's immediate organization.
- b. The employee's supervisor should be prepared to discuss the employee's goals with a realistic view as to whether or not the goals are achievable considering the OA resources and needs. Short and long term goals may be modified as appropriate to help insure implementation of the intermediary steps necessary to meet the established

goals. The supervisor should also be prepared to help the employee develop detailed plans for career enhancement, encouraging the employee in assuming leadership responsibilities and innovative methods.

- c. The career enhancement plan may be developed using Exhibit A, Guideline for Developing a Career Development Plan. The attached form, Career Development Action Plan outlined in Exhibit B (or a similar form) may be used to document the Career Development Plan and will be kept on file by all concerned parties. The employee should document their one year and five year goals (in a narrative format in the employee's own words) and will detail implementation steps considered necessary in leading to achievement of identified goals and update quarterly. To this end, the employee should detail the formal training considered necessary in achieving both the short term and long term goals. Formal training needs identified should show the source, available dates, and cost of the training. Formal training should be prioritized to show the order that courses should be taken. On-the-job training opportunities should be identified by the supervisor, giving consideration to upcoming scheduled assignments and opportunities to afford the employee work experience at higher levels or in different areas of the OA. Each employee, however, must recognize that circumstances may not permit on-the-job training possibilities. OA management assures that all on-the-job training opportunities will be distributed among interested employees in an equitable manner.

2-4. PLAN IMPLEMENTATION.

A review of the progress of the career enhancement plan should be made when the Group Chief presents the interim and final performance evaluations. Such reviews will help to assure that implementation is progressing satisfactorily.

**OPM-OIG
OFFICE OF AUDITS
GUIDELINES FOR USE IN DEVELOPING A CAREER DEVELOPMENT PLAN**

This document is intended as a guideline for discussions between OIG employees and their managers on the subject of the employee's career goals. This process is intended to document the steps that the employee and the manager agree can be taken in order to achieve the employees goals. This process is completely voluntary on the part of the employee and it is the employee's responsibility to initiate the process with their manager. The following questions are meant to be a discussion guide only. Please feel free to develop your own questions using whatever format is most useful to you.

I. EMPLOYEE CAREER GOALS

A. WHAT ARE YOUR CAREER GOALS? (Think about your long-term goals and what intermediate objectives you will need to achieve in order to reach your long-term goals.)

B. PROBLEMS

What barriers, resistance, interruptions, obstacles, etc. (anticipated and unforeseen) might you encounter as you implement your Career Plan?

C. SOLUTIONS

How do you plan to avoid or deal with the problems that you've just listed? Respond to each problem separately.

II. SHORT-TERM ACTION PLAN (ONE YEAR)

A. In order to reach your career goals, what are your current short-term objectives (Examples: within the audit process, within the OIG, beyond the OIG, etc.)?

B. How do you plan to reach your short-term objectives? (What action plan in the short-term will help you get started towards your career goals?)

1) What types of on-the-job training might help you reach your goals?

2) What type of classroom training might help you reach your goals?

3) Would cross-training in other OIG units be useful?

4) What independent pursuits might help you reach your goals (e.g. joining professional organizations, studying for CPA, CIA, etc.)?

C. PROBLEMS

What barriers, resistance, interruptions, obstacles, etc. (anticipated and unforeseen) might you encounter as you implement your Short-term Action Plan?

D. SOLUTIONS

How do you plan to avoid or deal with the problems that you've just listed? Respond to each problem separately.

III. LONG TERM ACTION PLAN (ONE TO FIVE YEARS)

A. What other intermediate objectives will you need in order to achieve your career goals?

B. How do you plan to meet these other intermediate objectives?

1) What types of on-the-job training might help you reach your goals?

2) What type of classroom training might help you reach your goals?

3) Would cross-training in other OIG units be useful?

4) What independent pursuits might help you reach your goals (e.g. joining professional organizations, studying for CPA, CIA, etc.)?

C. PROBLEMS

What barriers, resistance, interruptions, obstacles, etc. (anticipated and unforeseen) might you encounter as you implement your Long-Term Action Plan?

D. SOLUTIONS

How do you plan to avoid or deal with the problems that you've just listed? Respond to each problem separately.

EXHIBIT B

**OPM-OIG
OFFICE OF AUDITS
CAREER DEVELOPMENT ACTION PLAN**

	Target Date	Date Achieved
--	-------------	---------------

A. Final Goal(s)

B. Intermediate Objectives

	Date Action Taken	Date Action Completed
--	-------------------	-----------------------

III. Long-term Action Plan (One to Five Years)	Date Action Taken	Date Action Completed
--	-------------------	-----------------------

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2925

Travel Policies and Procedures

CHAPTER 2925 - TRAVEL POLICIES AND PROCEDURES

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy.....	1
SECTION 2. TRAVEL TIME	
2-1. Authorized Returns to the Official Duty Station during Extended Assignments.....	2
2-2. Revised OIG Travel Policy.....	2
SECTION 3. TELEPHONE POLICY	
3-1. Revised OIG Telephone Policy.....	10

CHAPTER 2925 - TRAVEL POLICIES AND PROCEDURESSECTION 1. GENERAL

- 1-1. PURPOSE. This chapter prescribes the policies and procedures for OIG personnel traveling on temporary or official business. These policies and procedures are not intended to duplicate detailed instructions contained in General Services Administration's Federal Travel Regulations or to cover all situations encountered by a traveler.
- 1-2. POLICY. Each OIG official who directs, performs, reviews, or approves travel is responsible for exercising good judgment and following proper practices in travel matters. All travelers are responsible for keeping abreast of pertinent travel regulations and utilizing the most cost-effective means to carry out the OIG mission.

SECTION 2. TRAVEL TIME

- 2-1. AUTHORIZED RETURNS TO THE OFFICIAL DUTY STATION DURING EXTENDED ASSIGNMENTS - The OIG travel policy allows an authorized return trip on the second weekend of a temporary assignment of more than three weeks, and every second weekend thereafter.

The following restrictions are included in this travel policy:

- a. In no case will an audit be extended because members of the audit team returned to their official duty station every two weeks instead of every three.
 - b. Travelers should work at least one half day on the day they are returning to their official duty station and must work one half day on the day they return to their temporary duty station. In planning return flights, we expect the staff to schedule flights in the afternoon to maximize their hours at the audit site, yet arrive at their official duty station at a reasonable time in the evening (i.e., between 6:00 PM and 8:00 PM). Also, we expect the staff to return to their temporary duty station on the first available flight (i.e. between 7:00 AM and 9:00 AM). Deviations from this general schedule must be approved by the appropriate supervisor.
 - c. Travelers will be permitted to work the “5-4/9 Work Schedule” (eight 9 hours days, one 8 hour day and one day off each pay period), in accordance with CAD’s current AWS travel policy. However, travelers will not be permitted to work the “4/10 Work Schedule” (four 10 hour days and one day off each week) and be authorized to return to their official duty station every two weeks.
- 2-2. REVISED OIG TRAVEL POLICY – The following pages contain the revised OIG travel policy which was updated October 11, 2005 by the OIG’s Policy, Resources Management, and Oversight. The OIG policy supplements the GSA travel regulations. The policy is to be used as a guide for official OIG travel.



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

MEMORANDUM FOR ALL OIG STAFF

FROM: DANIEL K. MARELLA *Daniel K. Marella 10/11/05*
ASSISTANT INSPECTOR GENERAL FOR
POLICY, RESOURCES MANAGEMENT, AND OVERSIGHT

SUBJECT: OIG Travel Policy

Attached is a new OIG travel policy that supplements the GSA travel regulations. The policy provides guidance on OPM and OIG aspects of travel as well as examples on the more complex elements of travel, such as constructing costs. In addition, OPM recently issued regulations on earning compensatory time while in a travel status. This policy also offers explanatory examples pertaining to the compensatory time regulation.

This guidance is not intended to override any GSA Federal Travel Regulation. Periodic updates may be made to the OIG policy as necessary. This policy and all updates will be posted on the OIG O:\Policy drive. If you have travel questions that are not addressed in the GSA regulations or in this policy, check with your supervisor or contact Dan Marella or Terri Fazio.

OIG-01
May 1999

October 2005

OIG TRAVEL POLICY

This OIG travel policy establishes supplemental guidance regarding official travel for OIG employees. The prevailing GSA Federal Travel Regulations are the authoritative guidance on travel issues and this OIG policy provides examples and information to clarify how to apply the rules to our circumstances. Below are terms, definitions, and examples related to official travel that may assist when preparing a travel authorization, travel voucher, or planning a trip for official business. The information below also includes information to assist with the interpretation of recent OPM regulations regarding earning compensatory time (comp time) while in a travel status.

Airline Agent Fees

Fees charged by travel agents for the booking of airplane reservations are reimbursable. Employees shall itemize the agent fee along with the transportation expense, as a line item, categorized as "Ticketing Fee/Lodging Tax", in the normal travel voucher process.

Annual Leave While on Official Travel

If an employee takes greater than 4 hours of annual leave or comp time in a single day while on official travel, the employee is not eligible for per diem that day.

Cash Advances

The employee must estimate the amount of cash needed for travel related expenses not covered by the Government travel card and cash advances must not exceed the amount necessary. Please note that there may be daily limits imposed by banks on cash advances.

Compensatory Time While in a Travel Status

In general, travel should take place during normal work hours to avoid the necessity for earning compensatory time. In circumstances where it is necessary to travel on a weekend or during hours outside the normal work day, comp time may be earned while in a travel status (See Definition). Supervisors or managers will make the determination whether it is necessary to travel outside normal duty hours.

Some examples of when travel during non-duty hours may be necessary include:

- (1) For audits that are two weeks in duration or less, it may be desirable to begin the audit on Monday morning in order to get the audit completed in the allowed time period.
- (2) When out-of-town training or conferences begin on Monday morning, travel on Sunday may be necessary to ensure your attendance on Monday morning.

October 2005

- (3) When circumstances surrounding travel do not allow advance planning and there is an urgent need to get to a destination quickly without having to wait to the next duty day to do the travel.

For purposes of calculating compensatory time while in a travel status, the following examples show time that may **not** be included in your comp time total:

- (1) Time spent for meals;
- (2) Time spent resting or shopping;
- (3) Delays greater than 2 hours;
- (4) Layovers or transportation connections greater than 2 hours;
- (5) Time spent getting to/from a transportation center, where the time generally equates to a normal commute; and
- (6) Additional time incurred when a traveler decides to drive to a destination rather than using a commercial carrier, such as an airplane. An employee must take leave for the official duty hours needed in excess of the normal travel time. If the employee was authorized by their supervisor or manager to travel on non-duty time, the employee is able to earn comp time for the travel up to the amount expected to be earned if traveling by commercial carrier.

In general, a 2 hour rule applies to transportation delays, early arrivals (limited to actual amount of early arrival or 2 hours, whichever is less), and layovers. Any time over 2 hours spent awaiting transportation or connections, is not compensable. For example, if you encounter a delay greater than 2 hours at an airport while waiting for a flight, your compensable time is limited to those 2 hours while waiting for your flight. The accumulation of compensable time resumes when you board the plane en route to your destination.

If you are authorized to travel during non-duty hours, any time spent traveling to or from a transportation terminal is considered normal commuting time and should not be counted in your compensable time total. For example, if you leave home on a Sunday at 8:00 a.m. and taxi to the airport, arriving at 8:45 a.m., the 45 minutes you spent traveling to the airport is considered normal commuting time and is not compensable.

All comp time earned while in a travel status must be used within 26 pay periods or it will be forfeited.

Comp Time vs. Law Enforcement Availability Pay (LEAP)

Under availability pay provisions, all unscheduled duty hours are considered compensable hours, since availability pay represents full compensation for all

October 2005

unscheduled duty hours. Therefore, compensatory time rules do not generally apply for anyone on LEAP.

Constructed Costs

Any travel related cost incurred for transportation or per diem that is outside of the normal method of incurring these costs. For instance, if a traveler decides to drive rather than travel by commercial carrier to or from a site; or if a traveler decides to travel outside the authorized travel location over a weekend while on official travel. The traveler may use constructed costs to claim the lesser of amounts for actual expenses or the normal method of incurring costs. Also, if the employee returns home on a constructed cost weekend, the employee will not be entitled to an allowance for meals and incidental expenses (M&IE).

A traveler may decide to drive to an official duty station rather than using a commercial carrier, such as travel by airplane. In doing so, the traveler may use constructed costs to file for reimbursement on their travel voucher. A traveler may be reimbursed actual costs not to exceed the constructed cost of transportation by commercial carrier.

If official travel requires an employee to stay over a weekend and into the next week, the employee may construct costs during the weekend. For example, if lodging per diem is \$200 per day, the employee may decide to check out of the hotel on Friday and not check back in until Monday. The employee can construct costs up to the amount that would have kept you in the hotel for the 3 nights which would be \$600 in this example. The employee may travel out of the area and claim reimbursement for actual expenses up to the \$600.

Another example is that an employee stays in a hotel at \$150 per day where the lodging per diem is \$200 per day. The employee decides to construct costs and check out of the hotel for 3 nights over the weekend. The employee can construct costs for actual expenses up to \$450, which is the actual amount to keep you there. However, since the employee's lodging rate is \$50 below per diem, they can use the \$50 savings for gainsharing.

For example submissions, see Attachment 1

Dry Cleaning and Laundry

Professional dry cleaning shall be reimbursed at the rate of the actual dry cleaning expenses incurred not to exceed an average of \$3 per day. To be reimbursed, travel must involve a minimum of four consecutive overnight stays.

Laundry shall be reimbursed at the rate of the actual laundry expenses incurred not to exceed an average of \$1.50 per day. An employee on travel status has the option of doing his or her laundry or having it done professionally, such as by a dry cleaning establishment. To be reimbursed, travel must involve a minimum of four consecutive overnight stays.

October 2005**Gainsharing**

See official OIG policy entitled "OIG Gainsharing Travel Savings Award Program", a copy of which is located on our server at O:\POLICY\Gainsharing.doc.

Government Travel Cards

Employees are required to use their government travel card for all official expenditures while in a travel status. Wherever possible, the travel card shall be used to pay for such expenses as hotel bills, meals, taxi fees, transportation (including airfares), etc. Procedures for payment of official expenditures in the event of a suspended/revoked card will be handled under separate policy.

Meals and Incidental Expenses (M&IE)

M&IE rates are set by the Government-wide Per Diem Advisory Board, established by GSA. For current per diem rates by city and state, please go to the GSA web site at www.gsa.gov. The web site will even provide a meal and incidental expense breakdown. From the amount provided for M&IE, \$3 per day is for incidental expenses. Incidental expenses include fees and tips given to porters, baggage carriers, bellhops, hotel maids, etc. It can also cover transportation between places of lodging or business and places where meals are taken.

Receipts

When filing a travel voucher for reimbursement of expenses, receipts must be provided for any expense over \$75. Receipts for \$75 or less must be retained by the traveler and may be requested during a quality assurance review.

Reimbursable Hotel Taxes

When making hotel reservations, make sure to inquire whether a hotel accepts tax-exempt forms. It is the traveler's responsibility to obtain these tax-exempt forms prior to departure on travel status. Lodging taxes are reimbursable as miscellaneous travel expenses if the hotel does not accept the tax-exempt forms. Lodging taxes are reimbursable only at the actual cost up to the tax rate on the maximum per diem lodging rate.

Rental Cars

The following rules generally apply to the size and number of rental cars, when a rental car is authorized:

Mid-size for 1-3 people
Full-size for 4 people
2nd or additional car for 5 or more people

Telephone Use

Cell phones provided to an employee for use while in a travel status may be used for up to 20 minutes per day for personal calls. International calls are not permitted. Employees with government cell phones may not file for reimbursement for phone calls.

October 2005

In situations where a cell phone is not provided, the situation will be handled on a case by case basis between the employee and their supervisor.

Travel Status

An employee is considered to be in a travel status from the moment of departure from his or her residence until returning there again based on the travel orders. Periods during a trip, where there is a break in official travel at either the beginning or end of a trip for personal travel, is not included in calculating periods on travel status.

Turn Around Trips

If you are in a travel status for an extended period of time, you are authorized a turn around trip at government expense. If you are on official travel for 4 weeks or more, you are authorized 1 turn around trip; for 6 weeks on official travel, you are authorized 2 turn around trips; and for 8 weeks on official travel, you are authorized 3 turn around trips, etc.

Accumulation of comp time is not authorized during turn around trips. Supervisors or managers may authorize official duty time or early departure from a duty station for turn around travel.

Vouchers

When filing a travel voucher against an existing travel authorization, the voucher may be a partial or a final voucher. A partial voucher includes a request for reimbursement for only part of the expenses you incurred while on official travel. While on longer trips, several vouchers may be filed during the trip requesting partial repayment of expenses incurred. For some shorter trips, you may choose to only file one final voucher at the conclusion of the trip. In either case, when the final voucher is filed, you must make sure the "FINAL" indicator is checked in the FEDDESK Travel System when entering data into the travel voucher system. The indicator is found on the first screen when entering the voucher online.

If you have any questions or comments regarding this policy, please contact Dan Marella, Assistant Inspector General for Policy, Resources Management, and Oversight on 202-606-2638 or Terri Fazio, Deputy Assistant Inspector General for Policy, Resources Management, and Oversight on 202-606-0846.

CONSTRUCTED COSTS: Example 1

CONSTRUCTED TRANSPORTATION:

(For the purpose of determining most advantageous transportation cost)

REASON: Traveler drove P.O.V. for personal reasons.

SUNDAY, DECEMBER 2, 2001:

Taxi from Residence to Washington National Airport
 Depart airport via US AIRWAYS Flight #1275/2235
 Arrive Louisville, Kentucky Airport
 Arrive hotel

Taxi - \$40.00
 AIRFARE \$659.50

THURSDAY, DECEMBER 13, 2001:

Depart TDY site for Louisville Airport.
 Depart airport via US AIRWAYS Flight #828/988
 Arrive Washington National Airport
 Arrive residence via taxi.

Taxi -- \$40.00
TOTAL - \$739.50

ACTUAL TRANSPORTATION COST:

DECEMBER 1, 2001-DEPART RESIDENCE VIA P.O.V. FOR OHIO
 STAY WITH RELATIVES THAT NIGHT.
 DECEMBER 2, 2001-DEPART OHIO FOR LOUISVILLE, KENTUCKY
COSTS: MILEAGE: 602 MILES X \$0.485 per MILE = \$291.97
TOLL - PA. TURNPIKE = \$3.60

RETURN:

DECEMBER 13, 2001-DEPART TDY SITE VIA P.O.V. FOR ZANESVILLE, OHIO
 DECEMBER 14, 2001-DEPART OHIO FOR RESIDENCE (Falls Church, Va.)

COSTS: MILEAGE: 615 MILES X \$0.485 per MILE = \$298.28
TOLL-PA. TURNPIKE = \$3.60

MOTEL: ONE NIGHT (12/13/01) - \$61.24 RECEIPT ATTACHED

TOTAL -- \$658.69

CLAIMING ACTUAL TRANSPORTATION COST BECAUSE OF LESS EXPENSE TO THE GOVERNMENT.

SECTION 3. TELEPHONE POLICY

- 3-1. REVISED OIG TELEPHONE POLICY – The following page contains the revised OIG telephone policy which was updated October 2, 2007.



Office of the
Inspector General

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

October 2, 2007

MEMORANDUM FOR ALL OIG STAFF

FROM:

NORBERT E. VINT

Deputy Inspector General

A handwritten signature in black ink that reads "Norbert E. Vint".

SUBJECT:

OIG Policy for Reimbursement of Personal Telephone Calls While In a Travel Status

Effective October 1, 2007, personal telephone calls while in travel status shall be reimbursed for the cost of the calls not to exceed an average of \$1 per day, accumulated weekly. Since this is a nominal amount and many travelers use personal cell phones or calling cards that do not facilitate maintaining records, detailed documentation will not be required. However, if you do not incur personal telephone call expenses, you are not entitled to claim reimbursement on your travel voucher.

This policy replaces any previous policy regarding the issue of reimbursement for personal telephone calls while in a travel status. This policy does not apply to employees who have been issued a cell phone for official use. Employees who are issued a cell phone may not file for reimbursement for phone calls as described above, however, they may use their OIG-issued cell phone for up to 20 minutes per day for personal calls while in a travel status.

**Office of Personnel Management
Office of the Inspector General
Office of Audits**

Chapter 2930

**The Audit Report and Receivable Tracking
System (ARRTS)**

CHAPTER 2930 - THE AUDIT REPORT AND RECEIVABLE TRACKING SYSTEM

CONTENTS

	<u>Page</u>
SECTION 1. GENERAL	
1-1. Purpose.....	1
1-2. Policy	1
SECTION 2. ARRTS OPERATIONS	
2-1. Roles and Responsibilities	2
2-2. The Flow	2
2-3. The ARRTS Process	3
2-4. Primary Modules.....	4
2-5. System Security and Database Access.....	5
2-6. The ARRTS Application.....	5

CHAPTER 2930 - THE AUDIT REPORT AND RECEIVABLE TRACKING SYSTEM
(ARRTS)

SECTION 1. GENERAL

1-1. PURPOSE. This chapter provides the policies and procedures that the Office of the Inspector General (OIG) and the Office of Personnel Management (OPM) will follow regarding the Audit Report and Receivable Tracking System (ARRTS). Also see Chapter 2410, Report Organization and Processing for additional guidance.

1-2. POLICY.

The OIG and OPM will conduct the audit follow-up process in accordance with:

- a. Office of Management and Budget Circular A-50, Audit Follow-up;
- b. Generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States; and
- c. The Audit Report and Receivable Tracking System.

SECTION 2. ARRTS OPERATIONS

- 2-1. ROLES AND RESPONSIBILITIES - The Office of the Inspector General (OIG) is the audit authority and is responsible for performing audits at the Office of Personnel Management (OPM). The OIG may decide to conduct an audit or respond to an OPM program office request to perform an audit. When audits are requested by organizations outside of the OIG, e.g., the Healthcare and Insurance Office (HIO), the requesting organization becomes the customer of the OIG and the OIG becomes the owner of the audit material. Audits may be conducted by OIG staff or provided by an outside contractor. The OIG conducts audits of health and life insurance carriers, the Combined Federal Campaign, and internal OPM practices and processes.

The OIG has the primary responsibility for the audit until the final audit report is issued. Once an audit is completed and the final report issued, the implementation and/or resolution and reconciliation of the audit findings and recommendations becomes the responsibility of Merit System Accountability and Compliance's Internal Oversight and Compliance or HIO's Federal Employee Insurance Operations (FEIO) Audit Resolution. Audit recommendations are categorized as monetary, non-monetary (procedural), and better dollar use. When monies are involved in the resolution of an audit finding, the HIO's Federal Employee Insurance Operations (FEIO) Audit Resolution, has the responsibility for monitoring the collection and/or payment. The Chief Financial Officer has the responsibility updating the appropriate Federal fund.

- 2-2. THE FLOW – The following description applies to the OIG's overall audit flow and HIO's responsibility for monitoring, as well as collecting any funds due from the audit recommendations.
- The OIG plans audits at the beginning of the fiscal year.
 - During the fiscal year, some audits are dropped and others are added.
 - The OIG audit team requests an audit report number using the Audit Record - ARRTS Input Worksheet (Exhibit H or available electronically).
 - The OIG audit team begins the audit.
 - The OIG audit team completes the field work.
 - The OIG audit team produces a draft audit report with recommendations and associated findings.
 - The auditee responds to the draft audit report.
 - The OIG issues a final audit report.
 - The OIG audit team completes the Final Audit Report - ARRTS Input Worksheet (Exhibit I or available electronically).
 - The OIG inputs the recommendations (monetary and procedural) into ARRTS.
 - The OIG releases the final audit report to HIO or other OPM organizations.
 - FEIO Audit Resolution makes determinations based on the recommendations.

- Accounts receivable are established for financial determinations when monies are owed to the Government.
- Accounts receivable are placed under FEIO Audit Resolution for collection.
- Auditees are notified of their financial obligations.
- The OIG is kept current by FEIO Audit Resolution through various correspondences such as quarterly reports and final decisions concerning outstanding audit findings and recommendations.
- An auditee may appeal.
- Interest and penalties are charged.
- Bills are sent to the auditee.
- Appeals are decided and principal and interest are adjusted.
- Recovery payments are received from the auditee.
- Accounts are closed as receivables are paid off.

2-3. THE ARRTS PROCESS - The ARRTS database and the software are designed to update and retrieve information as the audit progresses. The ARRTS database design and the internal table structure correspond to the operational division for performing the audits.

Within the ARRTS database, the audits and recommendations tables are tied to the planning and execution of the audits. Once the audit recommendations are set up for reconciliation with the auditee, the determinations, appeals, and decisions tables are built and updated. FEIO Audit Resolution is responsible for creating and maintaining the determinations, appeals, and decisions. For all final determinations, which result in monetary actions, i.e., dollars owed to the Government, the financial database tables are used to track results and generate the appropriate transaction for updating the appropriate Government fund. As the audit process progresses and the database is updated, the ADP system will apply strict validation rules to ensure audit information validity and consistency. Additionally, since audit information is often organizational-sensitive, access rules will determine levels of personnel access to the database.

- 2-4. PRIMARY MODULES – There are three primary modules that make up ARRTS: (1) the Audit Management Module (AMM), (2) the Financial Management Module (FMM), and (3) the System Administration Module (SAM).

The Audit Management Module (AMM) -

- Supports the adding, updating, deleting, and viewing of audit-related database tables (e.g., audits, recommendations, determinations, appeals, and decisions).
- Allows the selection of the ARRTS standard reports.
- Provides a spontaneous query capability against the audit tables.
- Allows the creation of accounts receivable and Sustained Appeal financial transactions.

(All ARRTS users have access to this application)

The Financial Management Module (FMM) -

- Supports the financial management of the accounts receivable database including the generation of financial transactions (e.g., payment recoveries).
- Generates billing to the auditees (i.e., the Plans).
- Produces the Financial Aging report.
- Produces transactions to the OPM general ledger system.

(Only appropriate FEIO users have access to this application)

The System Administration Module (SAM)

- Supports the management of ARRTS user information.
- Assigns access rights to users.
- Supports the management of the database Lookup tables (e.g., Plan codes)
- Supports the management of the History Record tables.

(Only the ARRTS System Administrator (ASA) and the appropriate OIG and HIO database managers have access to this application).

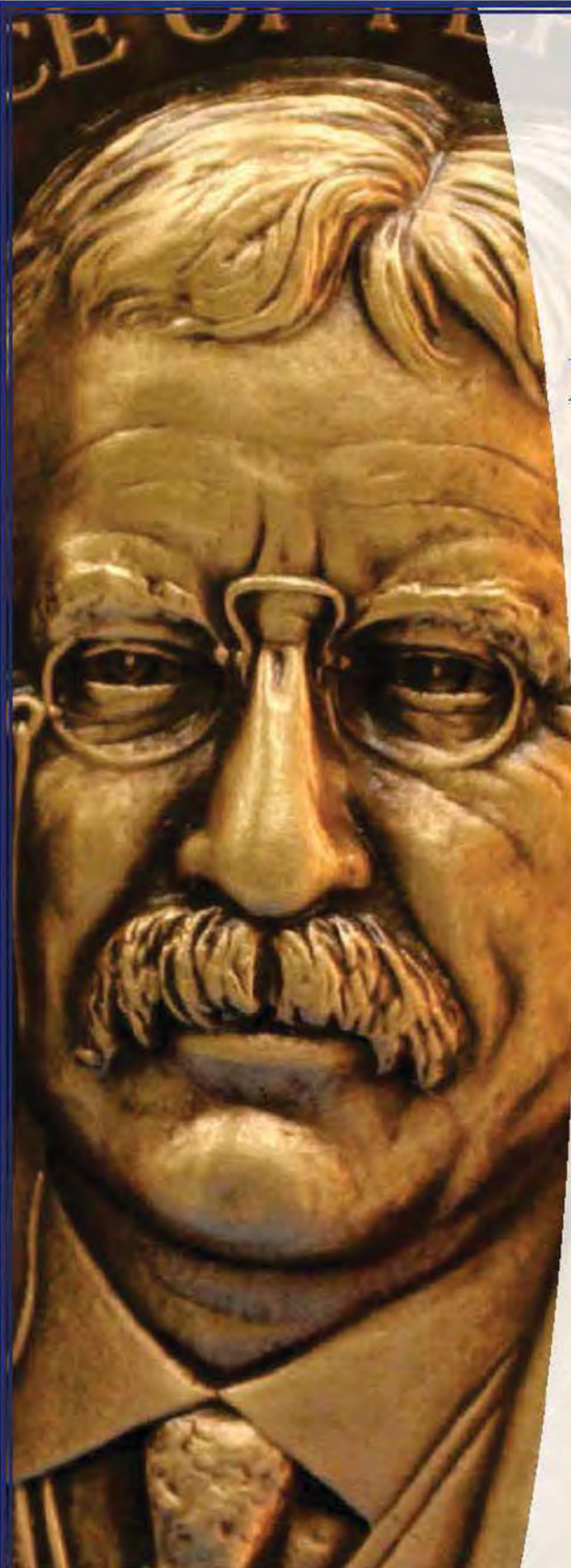
- 2-5. SYSTEM SECURITY AND DATABASE ACCESS - ARRTS uses a system administration module, internal parameters, and software logic to control access to the audit information database. This access capability is based on a set of rules and a database of user identification codes with access level authority. Access is defined as controlling who has the authority to create, update, delete, and view specific information in the database. The organization that is responsible for the data controls the data.
- 2-6. THE ARRTS APPLICATIONS – The following Exhibits display and describe the ARRTS screens and applications used to track the audit reports and the corresponding recommendations.

U.S. OFFICE OF
PERSONNEL MANAGEMENT



OFFICE OF THE INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS INVESTIGATIVE MANUAL



Theodore Roosevelt
U.S. Civil Service Commissioner

February 20, 2015



OFFICE OF INVESTIGATIONS

This manual is the property of the OIG Office of Investigations, U.S. Office of Personnel Management. It is to be used for official business only and is not to be reproduced without approval of the Assistant Inspector General for Investigations.

Table of Contents

Chapter 1 Guide to Investigative Manual

100.00	Introduction.....	1-1
100.10	Establishment of the OIG	1-1
100.20	Organization.....	1-2
100.30	Types of OIG Investigations.....	1-2
100.31	Definition of Investigation.....	1-3
110.00	Guide to Manual	1-3
110.10	Manual Effective Date and Distribution.....	1-3
	Figure 100-01 – OIG Organization Chart.....	1-4
	Figure 100-02 – Office of Investigations Organization Chart.....	1-5

Chapter 2 Authority and General Policy

200.00	Law Enforcement Authority	2-1
210.00	Quality Standards of Conduct.....	2-2
210.10	General Standards for Investigations.....	2-2
210.20	Qualitative Standards for Investigations.....	2-2
210.30	Additional OIG Standards for Investigations	2-2
211.00	Appearance and Behavior.....	2-3
211.10	Lautenberg Amendment	2-3
212.00	Use of Badge and Credentials.....	2-4
220.00	Training.....	2-4
220.10	Entry-Level Training	2-5
220.20	In-Service Training	2-5
230.00	OIG Relationship with Prosecutive Authorities and Other Law Enforcement.....	2-5
230.10	OIG Relationship with U.S. Attorneys	2-5

230.20	OIG Relationship with the Department of Justice	2-6
230.30	OIG Relationship with Other Law Enforcement Agencies	2-6
230.35	CIGIE Mutual Assistance Policy	2-7
230.40	Procedures for Referrals to Other Law Enforcement Agencies	2-8
230.50	Procedures for Referrals Involving Threats Against Government Officials	2-8
230.60	OIG Relationship with State and Local Prosecutors	2-9
230.70	OIG Relationship with Office of Special Counsel	2-9
240.00	Use of Government Vehicles	2-9
240.01	Penalties for Improper Use	2-10
240.10	Record Keeping/Log Sheet.....	2-10
240.20	Personal Responsibility.....	2-10
240.21	Safe Driving.....	2-10
240.22	Valid Driver’s License.....	2-10
240.23	Reasonable Protection from Theft or Damage	2-11
240.24	Obey Traffic Laws	2-11
240.25	Personal Liability for Fines.....	2-11
240.30	Prohibitions.....	2-11

(b) (7)(E)

240.40	Maintenance	2-12
240.45	Charge Cards.....	2-13
240.50	Damage/Accidents	2-13
240.60	Emergency Equipment.....	2-14
240.70	Home-To-Work Transportation (HTW)	2-14
240.80	Requesting Reimbursement for Tickets/Penalties Incurred as a Necessary Part of Performing Official Duties	2-14
240.90	Parking Permits for Federal Parking Facilities	2-15
250.00	Law Enforcement Availability Pay.....	2-16
250.10	General Rules.....	2-17
250.11	Voluntary Opt-Out.....	2-17
250.12	LEAP Reporting Requirements	2-18
250.13	Biweekly Activity Reports.....	2-18

Chapter 3 Complaint Control

300.00	Complaint Control - General	3-1
310.00	OIG Hotline, Reporting Fraud, Waste and Mismanagement.....	3-1
310.10	Complaint Processing	3-1
310.11	Advising Hotline Sources on Policies for Protecting Their Identities.....	3-2
311.00	Threats Against the President of the United States, Cabinet Members, and Members of Congress	3-3
320.00	Whistleblower Protection	3-3
320.10	Whistleblower Protection for Federal Employees, Former Employees, and Applicants for Employment	3-4
320.11	Procedures for Responding to Claims of Retaliation by Revocation of an OPM Employee's Security Clearance.....	3-5
320.20	Whistleblower Protection for Employees of Federal Contractors, Subcontractors, and Grantees.....	3-6

Chapter 4 Investigative Management

400.00	Investigative Management Procedures	4-1
400.10	Preliminary Investigative Activity.....	4-1
400.20	Proactive Investigative Activities	4-1
400.30	Investigative Sources and Informants.....	4-2
410.00	Initiation of Investigative Activity.....	4-2
410.10	Accepting a Case for Investigation.....	4-3
410.20	Referring a Case for Action by Agency Program Officials.....	4-3
410.30	Referral to OPM Organizations	4-3
410.40	Referral to Another Government Agency.....	4-4
410.50	Rejecting a Case Not Within the Scope of the OIG Jurisdiction or Investigations Policy.. ..	4-4
420.00	Administrative Case Control	4-4
420.10	Case Control Number	4-5
420.20	File Organization for Hotlines and Raw Data	4-5
420.21	File Organization for Complaints	4-5

420.30	File Organization for Investigations	4-6
420.40	File Organization for Proactive Projects.....	4-7
420.50	File Security, Shipment, and Storage	4-7
430.00	Caseload Management.....	4-9
430.10	Case Assignment.....	4-10
430.11	Transfer of Cases Between Geographic Areas of Responsibility.....	4-10
430.12	Lead Requests	4-10
430.13	Case Reporting Requirements	4-10
430.14	Documentation of Quality Standards Benchmarks.....	4-11
440.00	Case Planning	4-11
440.10	Case Review	4-12
440.11	Case Disposition	4-12
450.00	Reports to OPM Management and the Congress.....	4-12
450.10	Reports to OPM Management	4-12
450.20	Reports to Congress.....	4-13

Chapter 5

Investigative Policies and Procedures

500.00	Introduction.....	5-1
500.10	Media Contacts and Press Releases	5-1
501.00	Sources of Information-Documentary Evidence	5-2
501.10	OPM Sources of Documentary Information.....	5-2
502.00	Confidential Sources and Informants	5-3
502.11	Definitions	5-4
502.12	Policies.....	5-4
502.13	Developing Confidential Informants	5-5
502.14	Payment of Confidential Informants.....	5-6
502.15	Reporting Violations of Criminal Law by Confidential Informants.....	5-6
502.16	Protecting Identities of Confidential Informants	5-7
502.17	Confidential Informant Files.....	5-7
502.18	Referencing Confidential Informants in Reports.....	5-7
502.19	Protecting Confidential Informants' Identities in the Courts	5-7

503.00	Subpoenas	5-8
503.10	Responsibility in OIG for Processing Subpoenas.....	5-9
503.11	Policy on Use of Subpoenas	5-9
503.12	Procedures for Requesting Subpoenas.....	5-10
503.13	Approval and Processing of Subpoenas.....	5-11
503.14	Service of Subpoenas.....	5-11
503.15	Return Proceedings	5-12
503.16	Handling of Subpoenaed Documents	5-12
503.17	Failure to Comply.....	5-13
503.18	Subpoena to Financial Institutions.....	5-13
503.19	Reimbursement to Financial Institutions for Cost Incurred.....	5-14
504.00	Search Warrants.....	5-14
504.10	Safe Execution of Search Warrants	5-14
504.20	Handling of Seized Evidence.....	5-14
504.30	Seized Firearms.....	5-14
505.00	Warnings and Rights.....	5-15
505.10	Warnings and Rights during Custodial Criminal Investigation Interviews.....	5-16
505.11	Warnings and Assurances During Administrative Interviews.....	5-16
506.00	Affidavits and Statements.....	5-17
506.10	Guidelines for Preparing Affidavits.....	5-17
506.11	Authority to Administer Oath.....	5-18
507.00	Interviews.....	5-18
507.10	Memorandum of Interview	5-18
507.11	Preparation for Interview	5-18
507.12	Time and Place of Interview.....	5-19
507.13	Voluntary Response.....	5-19
507.14	Interview of Minors	5-20
507.15	Interview of Members of the Opposite Gender	5-20
507.16	Interview of Hostile Individuals	5-20
507.17	Union Representation During Interviews	5-20
507.18	Confidentiality During Investigative Interviews	5-22
508.00	Special Investigative Procedures	5-22
508.10	Polygraph Examinations.....	5-22

508.11	Requesting Polygraph Examinations	5-22
508.20	Surveillance	5-23
508.21	Electronic and Video Surveillance	5-23
508.22	Electronic Tracking Devices.....	5-24
508.23	Pen Registers and Trap and Trace Devices	5-24
508.24	Video-Only Surveillance	5-24
508.25	Stored Electronic Communications	5-25
508.30	Consensual Monitoring.....	5-25
508.31	Request for Approval of Consensual Monitoring.....	5-26
508.32	Execution of the Consensual Monitoring	5-26
508.33	Obtaining Monitoring Equipment.....	5-27
508.34	Safeguarding Materials	5-27
509.00	Undercover Techniques	5-27
509.01	Definitions of Undercover Terms	5-28
509.10	Authorization to use Undercover Techniques	5-28
509.11	Undercover Memoranda of Request, OPM/OIG Lead Agency.....	5-29
509.12	Undercover Memoranda of Request, Other Agency Lead	5-30
509.13	Task Force Assistance	5-30
509.14	Scope and Duration.....	5-31
509.20	Approval Authority for Undercover Techniques.....	5-31
509.30	FBI Notification.....	5-31
509.40	Coordination with Prosecutors.....	5-32
509.50	Conduct of Undercover Activities/Operations	5-32
509.60	Considerations in Health Care Fraud Undercover Operations	5-32

(b) (7)(E)

510.00	Investigative Equipment	5-35
511.00	Use of Email for Case Related Communication.....	5-35

Figure 500-01	– Subpoena Memorandum Request Form Format (Non-Financial)	5-37
Figure 500-02	– Subpoena Memorandum Request Form Format (Financial Institution)	5-43
Figure 500-03	– "Tracing of Firearms in Connection with Criminal Investigations"	5-51

Figure 500-04 – Miranda Warning	5-53
Figure 500-05 – Garrity Warning	5-55
Figure 500-06 – Kalkines Warning	5-56
Figure 500-07 – Sworn Statement	5-57

(b) (7)(E)

Chapter 6 Health Care Fraud Investigations

600.00	Introduction.....	6-1
600.10	Types of Health Care Fraud.....	6-1
601.0	Federal Statutes Used to Prosecute Health Care Fraud Matters.....	6-2
602.00	Jurisdiction/Venue	6-2
603.00	Investigative Techniques	6-3
604.00	Sharing of Information with Other Agencies	6-3
605.00	Prioritization	6-3
605.10	Evaluation of health care fraud allegations.....	6-4
606.00	Desk Review	6-4
607.00	Presenting the Case for Prosecution	6-5
608.00	Approval for Civil Settlements	6-5
609.00	Recoveries to the FEHB Trust Fund.....	6-5
610.00	Other OPM Administered health care programs	6-6
620.00	Multi-State Plan Program	6-6
Figure 600-01	– Health Care Fraud Restitution Memo (Criminal)	6-7
Figure 600-02	– Health Care Fraud Restitution Memo (Civil)	6-9

Chapter 7 Retirement Fraud Investigations

700.00	Introduction.....	7-1
700.10	OPM’s Two Federal Retirement Systems	7-1
700.20	Retirement Services (RS).....	7-7-1
701.00	Various Types of Retirement Fraud.....	7-2

702.00	Federal Statutes Used to Prosecute Retirement Fraud.....	7-2
703.00	Jurisdiction/Venue	7-3
704.00	Investigative Techniques	7-3
704.10	Steps Needed to Investigate an Annuity Overpayment.....	7-3
704.20	Check Copies	7-5
704.30	Subpoenas	7-5
705.00	Testifying and the Use of Expert Witnesses.....	7-6
706.00	Case Closing Procedures	7-6
707.00	Investigation/Complaint Case Close-Out	7-8

Chapter 8

Federal Investigative Services, Computer Forensics, and Combined Federal Campaign Investigations

800.00	Federal Investigative Services	8-1
801.10	Advisement of Rights and Administrative Warnings.....	8-1
801.20	Major FIS Contractors	8-2
801.30	FIS Investigations	8-2
802.00	Computer Crimes Investigations.....	8-2
802.20	Computer Forensics Training	8-3
802.30	Computer Forensic Examination Responsibilities.....	8-3
802.40	Computer Crime and Forensic Assistance Request Procedures	8-4
802.50	Request for Examinations on Previously Collected Evidence.....	8-5
802.60	Handling of Digital Evidence During Computer Forensics Examinations	8-5
802.70	Computer Forensic Examination Reporting Procedures	8-6
803.00	Combined Federal Campaign	8-7
803.10	Combined Federal Campaign Investigations.....	8-7
803.20	Criminal Statutes.....	8-7
803.30	Definitions	8-7
803.40	CFC Investigations	8-8
804.00	Bribery/Kickback Investigations	8-9
804.10	Authority.....	8-9
804.20	Definitions	8-11

804.30	Methods of Payment	8-11
804.40	Indicators of Bribery Payments	8-12
804.50	Bribery Investigations.....	8-13

Chapter 9

Arrest Procedures

900.00	Arrest Procedures.....	9-1
900.10	Statutory Provisions and References	9-1
900.11	Authority.....	9-1
900.12	Definitions.....	9-2
900.13	Training.....	9-2
900.14	Use of Force.....	9-2
900.15	Obtaining Arrest Warrants.....	9-3
900.16	Execution of Arrest Warrants	9-4
900.17	Search Incident to Arrest	9-5
900.18	Arrest and Search in/near a Vehicle	9-7
900.19	Inventory.....	9-8
900.20	Prisoner Processing.....	9-9
910.00	Juveniles.....	9-11
920.00	Foreign Nationals.....	9-16
930.00	Non-Federal Crimes.....	9-17

Chapter 10

Weapons, Protective Equipment, Security, and Critical Incident Response

1000.00	Background.....	10-1
1000.10	Violations.....	10-1
1000.11	Definitions	10-1
1000.12	Use of Force Policy	10-2
1000.13	Application of the Use of Force.....	10-3
1000.14	General Policies	10-4
1000.15	Firearms Training	10-5
1000.16	Weapons Issuance and Security.....	10-9

1000.17	Carrying and Concealing Weapons	10-10
1000.18	(b) (7)(E)	
(b) (7)(E)	
1000.20	Protective Equipment.....	10-13
1000.21	Non-Lethal Weapons	10-13
1000.22	Use of Force Resulting in Physical Injury.....	10-13
1000.23	Critical Incident Response Procedures	10-15
1000.24	Post-Incident Administrative Inquiry	10-19
1000.25	Employee Assistance Program (EAP).....	10-19

Chapter 11 Reports of Investigation

1100.00	Reports of Investigation - General.....	11-1
1110.0	Report Standards.....	11-1
1110.10	Planning and Care in Report Writing	11-2
1120.00	Report of Investigation Format.....	11-2
1130.00	Report of Investigation Content.....	11-3
1130.10	Introduction.....	11-4
1130.20	Program Overview	11-4
1130.30	Basis of Investigation	11-6
1130.40	Statutes Violated	11-7
1130.50	Case Summary	11-7
1130.60	Conclusion/Disposition.....	11-8
1130.80	Approvals.....	11-8
1130.90	Subjects of Investigation.....	11-8
1130.91	Attachments	11-8
1140.00	Investigative Activity Reports	11-9
1150.00	Transmittal Memorandum	11-9
1160.00	Management Advisory Report.....	11-9
1170.00	Memoranda of Interview - General	11-10
1170.10	Opening Statement.....	11-11
1170.20	Vital Information	11-11

1170.30	Factual Body.....	11-11
1180.00	Reports and Correspondence Retention.....	11-12
1190.00	Writing Style.....	11-13
1191.00	Sample Reports.....	11-15

Chapter 12

Administrative Sanctions

1200.00	Introduction.....	12-1
1201.00	FEHBP Administrative Sanctions	12-1
1201.10	Authority.....	12-1
1201.11	General.....	12-1
1201.12	Definitions	12-2
1201.13	Effect of Debarment.....	12-2
1201.14	Exceptions to the Effect of Debarments and Suspensions.....	12-3
1201.15	Types of Debarment.....	12-3
1201.16	Suspension	12-7
1201.17	Grounds for Suspension.....	12-7
1201.18	Policies and Procedures in an OI Matter to Determine if an Administrative Sanction Action is Warranted.....	12-8
1202.00	OPM Administrative Sanctions	12-10
1202.01	Authority.....	12-10
1202.02	General.....	12-10
1202.03	Policies and Procedures for OI Recommendations for OPM Administrative Sanctions...	12-11
1203.00	Program Civil Remedies (Reserved)	12-11

Chapter 13

Law and Evidence

1300.00	Law and Evidence - General.....	13-1
1300.10	Definitions of Law	13-1
1300.11	Common Law	13-1
1300.12	Statutory Law.....	13-1
1300.13	Definitions of Crimes.....	13-1
1300.14	Evidence.....	13-1
1300.15	The Law of Evidence.....	13-2
1300.16	Evidence in Administrative Actions.....	13-2
1300.17	Evidence in Civil Actions.....	13-3
1300.18	Evidence in MSPB Appeals.....	13-3
1300.19	Classification of Evidence	13-3
1300.20	Forms of Evidence	13-3
1300.21	Collection of Evidence.....	13-4
1300.22	Collection and Preservation of Evidence.....	13-4
1300.23	Marking and Initialing of Evidence.....	13-4
1300.24	Receiving, Identifying, and Tagging Physical Evidence.....	13-5
1300.25	Preserving Documentary and Physical Evidence	13-5
1300.26	Evidence Log Procedures	13-6
1300.27	Documenting the Chain of Custody.....	13-6
1300.28	Disposition of Evidence.....	13-7
1301.00	Protection of Grand Jury Material	13-7
1301.10	Safeguarding Grand Jury Material.....	13-10
	Figure 1300-01 – Evidence Tag.....	13-11
	Figure 1300-02 – Evidence / Chain-of-Custody Form	13-12

Chapter 14
Witness/Victim Assistance Program

1400.00	Introduction.....	14-1
1400.10	Statutory and Regulatory Provisions	14-1
1400.11	Background.....	14-1
1400.12	Definitions	14-2
1400.13	Policy	14-3
1400.14	Legal Status of Guidelines.....	14-3
1400.15	Procedures and Individual Responsibilities.....	14-3

Chapter 15
Medical and Physical Standards

1500.00	Background.....	15-1
1501.00	Definitions	15-1
1502.00	Medical Requirements	15-1
1503.00	Hiring Standards	15-2
1503.10	Minimum/Maximum Age Requirements.....	15-2
1503.20	Medical Examinations	15-2
1503.30	Application of Physical and Medical Standards.....	15-3
1503.40	Employability Determinations.....	15-3
1503.50	Waiver of Physical Requirements/Medical Standards.....	15-4
1504.00	Physical Fitness Program.....	15-4
1504.10	Administration of Physical Fitness Program	15-5
1504.20	Physical Fitness Training.....	15-5
1504.30	Physical Fitness Training and LEAP	15-5
1504.40	Physical Fitness Training and the Use of the Government Vehicle	15-6
1504.50	The Physical Efficiency Battery	15-6
Appendix Listing		A-1

Chapter 1

Guide to Investigative Manual

100.00 Introduction

The Investigative Manual (IM) was designed for the use of all investigative staff of the U. S. Office of Personnel Management (OPM), Office of the Inspector General (OIG), Office of Investigations (OI). It was drafted under the direction and approval of the Assistant Inspector General for Investigations (AIGI), along with guidance from the Assistant Inspector General for Legal Affairs. Material appearing in the IM has been issued under the authority of the Inspector General (IG) or his designee; or the AIGI.

The IM is a basic investigative guide. It is not intended to cover every situation that may arise. Its provisions do not substitute for good judgment or common sense. It is designed to allow flexibility. It provides basic guidelines in most areas, with fixed rules and regulations in others.

The IM is distributed to all investigative staff in the Office of Investigations.

100.10 Establishment of the OIG

In the late 1970's, there were reports of widespread fraud, waste, and corruption within the Government, which prompted Congress to formulate and enact the Inspector General Act of 1978 (IG Act) (**Appendix A**). The IG Act reorganized the Executive Branch by creating Offices of Inspector General (OIGs). These offices consolidated existing audit and investigative resources to more effectively combat waste, fraud, abuse, and mismanagement. The IG Act set forth the fundamental duties, responsibilities, authorities, and reporting requirements of the OIGs. Public Law 100-504, the Inspector General Act Amendments of 1988, required the Office of Personnel Management (OPM) to establish a statutory Office of the Inspector General. The Office of the Inspector General at OPM was established in conjunction with that law on April 17, 1989.

The Inspector General concept, as implemented in OPM, is the consolidation of audit and investigative capabilities under the direction of a single high-level official, the Inspector General, who reports directly to the head of the agency and to the Congress. This organization and structure provides two essential elements: (1) a single focal point to effectively deal with waste, fraud, and abuse; and (2) coordination of audit and investigative activities.

The IG Act establishes a mandate for two important features: independence and objectivity. The statutory IG is appointed by the President with the consent of the Senate. Although the IG is under the general supervision of the agency head, the agency head cannot prevent or prohibit the IG from initiating, performing, or completing any audit or investigation.

The IG Act gives the IG no conflicting policy responsibilities within the agency, thereby assuring objectivity. The IG's sole responsibility is to promote economy and efficiency and to detect and prevent fraud and abuse through a program of audits, investigations, and other activities.

100.20 Organization

The Inspector General Act and its amendments require the establishment of two OIG components, Audits and Investigations. Accordingly, the OPM Office of the Inspector General has an Office of Audits, headed by the Assistant Inspector General for Audits (AIGA), and an Office of Investigations, headed by an AIGI. In addition, the OIG has an Office of Management and an Office of Legal Affairs, both headed by an Assistant Inspector General. This basic organizational structure is designed to promote coordinated, balanced, and integrated accomplishment of the OIG mission, goals, and objectives (**Figure 100-01**).

The Office of Investigations includes a Headquarters component and geographic regions. Headquarters personnel include the Assistant Inspector General for Investigations, Deputy Assistant Inspector General for Investigations (DAIGI) - Operations, Deputy Assistant Inspector General Investigations – Special Investigations, an Investigations Support Group and headquarters Special Agents. Each geographic region is supervised by a Special Agent in Charge (SAC), with assistance from an Assistant Special Agent in Charge (ASAC). In the absence of a SAC or other supervisor, a group chief may be designated to provide oversight and guidance to a Headquarters division or geographic region (**Figure 100-02**).

100.30 Types of OIG Investigations

The OPM/OIG investigates allegations regarding the actions of Office of Personnel Management employees or contractors involved in possible waste, fraud, and abuse; and also investigates allegations of waste, fraud, or abuse perpetrated against OPM administered programs. Responsibilities include the investigation of suspected offenses against the criminal or civil laws of the United States or violations of OPM regulations.

Investigations generally fall into the following categories:

- Fraud, waste, abuse and mismanagement in OPM programs, activities, and functions.
- Fraud related to the Federal Employees Health Benefits Program (FEHBP)
- Fraud related to the retirement and insurance trust funds.
- Contract and procurement fraud and improprieties.

- OPM employee misconduct and improprieties.
- Conflict of interest and ethics violations

100.31 Definition of Investigation

An investigation is a planned, systematic search for relevant, objective, and sufficient facts and evidence derived through interviews, record examinations, and the application of other approved professional investigative techniques.

110.00 Guide to Manual

The numbering system for the IM is as follows:

- Chapter 000
- Section 000
- Subsection 000.
- Paragraph 000.0
- Subparagraph 000.00
- Item 000.00-A

Figures referred to in chapters appear at the end of those chapters. Appendices are external documents hyperlinked to the manual.

110.10 Manual Effective Date and Distribution

Updates to the IM will be made periodically when a chapter or section is revised. An email indicating the effective date and electronic location of the IM will be submitted to personnel assigned to the Office of Investigations whenever an updated IM is published. Each IM will have an effective date listed at the bottom of the IM's front cover. A read-only version of the IM will be made available to all personnel of the Office of Investigations on the shared or G: network drive. All users are instructed to be informed of its contents.

Figure 100-01 – OIG Organization Chart

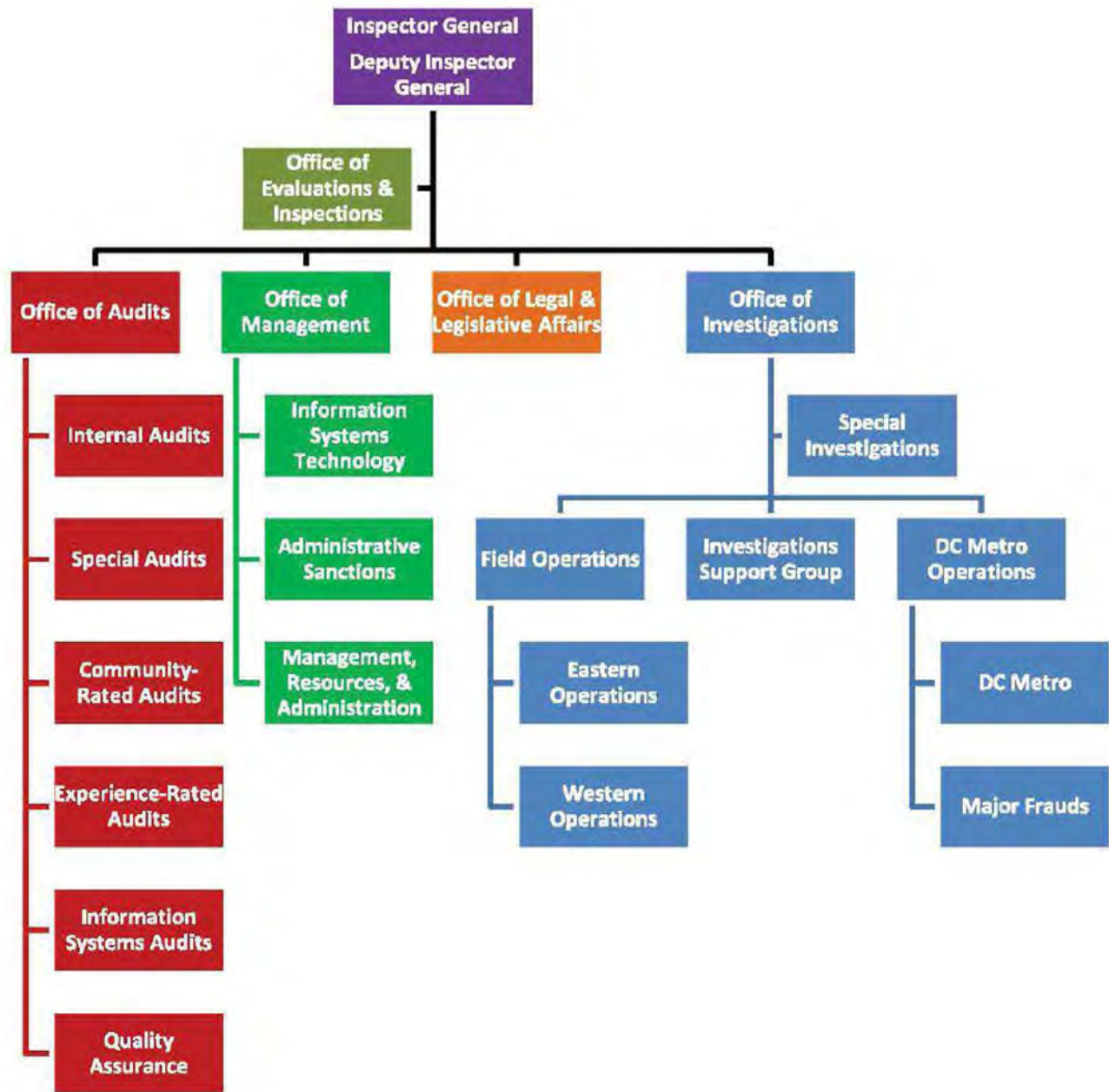
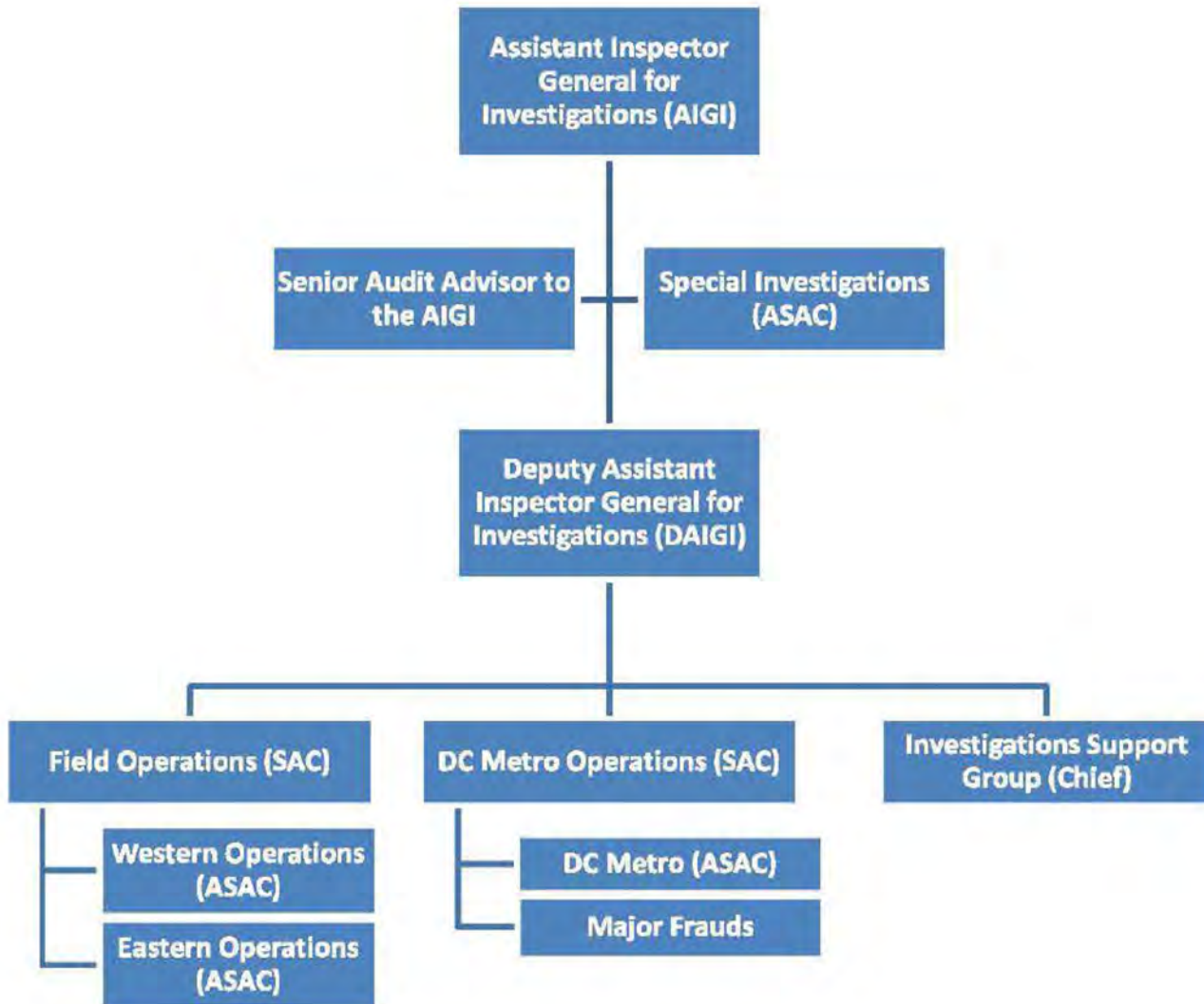


Figure 100-02 – Office of Investigations Organization Chart



Chapter 2

Authority and General Policy

200.00 Law Enforcement Authority

Special Agents of the OIG are empowered with law enforcement authorities pursuant to 5 U.S.C. app. 3, the Inspector General Act of 1978 as amended in section 812 of the Homeland Security Act of 2002 (P.L. 107.296), and the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority.

These authorities may be exercised when reasonably related to the performance of the duties, functions, and responsibilities assigned to the Inspector General. Agents are authorized, therefore, in order to prevent and detect fraud and abuse in the programs and operations of, and official misconduct within, OPM to:

- carry firearms;
- seek and execute arrest warrants;
- seek and execute search warrants;
- arrest without a warrant any person for any offense committed in their presence or for any felony offense if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony;
- serve subpoenas issued under authority of the Inspector General Act or issued by a federal grand jury or Federal court;
- serve legal writs, summons, and complaints; and,
- have access to records, reports, audits, reviews, documents, papers, recommendations, and other material which relate to the programs and operations of OPM; and,
- administer or take from any person an oath, affirmation, or affidavit.

210.00 Quality Standards of Conduct

OIG investigations are conducted in accordance with the *Quality Standards for Investigations adopted for Federal Offices of Inspectors General* by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) on November 15, 2011 (**Appendix B**).

Special agents and other investigative staff have a responsibility to maintain their objectivity so that judgments used in obtaining evidence, conducting interviews and making recommendations will be viewed as impartial by knowledgeable third parties.

210.10 General Standards for Investigations

Special agents and other investigative staff assigned to the OIG must possess professional proficiency and personal integrity in the conduct of OIG investigations.

In all matters relating to the investigative mission, the Office of Investigations must be free, both in fact and appearance, from impairments to independence. The office will maintain both an objective attitude and an organizational independence.

Due professional care must be used in conducting investigations and in preparing related reports..

210.20 Qualitative Standards for Investigations

Investigations should be conducted in a timely, efficient, thorough, and legal manner.

Investigative priorities should be established, and objectives should be developed to ensure that individual case tasks are performed in an efficient and effective manner.

Reports must thoroughly address all relevant aspects of the investigation. They must be accurate, objective, timely, understandable, and logically organized.

Results of investigations should be stored in a manner allowing effective security, retrieval, cross-referencing, and analysis.

210.30 Additional OIG Standards for Investigations

(b) (7)(E)

A large black rectangular redaction box covers the majority of the text in this section. The text "(b) (7)(E)" is visible in the top left corner of the redacted area.

(b) (7)(E)



211.00 Appearance and Behavior

The success of OIG investigations may depend upon voluntary cooperation of witnesses. The personal appearance and conduct of OIG special agents may influence this cooperation.

(b) (7)(E)



Special agents and investigative staff will carry out their responsibilities in a tactful, polite, considerate and highly professional manner. When dealing with an uncooperative or hostile witness, remain calm, confident and objective. Attitude and conduct should convey to the witness that all leads will be pursued and all pertinent information will be obtained in a professional manner.

211.10 Lautenberg Amendment

The Lautenberg Amendment, 18 U.S.C. Subsection 922(d)(9), amended the Gun Control Act of 1968 to make it a felony for those convicted of misdemeanor crimes of domestic violence to ship, transport, possess, or receive firearms or ammunition. This statute applies to federal law enforcement officers in the performance of their official duties. Therefore, government employees

who have been convicted of a disqualifying misdemeanor may not receive or possess firearms or ammunition to perform official duties.

Special Agents will immediately inform their supervisor and the AIGI if they are charged with any crime by law enforcement, including but not limited to domestic violence.

Beginning in fiscal year 2007, and each fiscal year thereafter, Special Agents will be required to submit an annual certification affirming their compliance with the Lautenberg Amendment. The annual certifications will be maintained in firearms files.

Special Agents are also advised that the OIG will conduct periodic National Crime Information Center (NCIC) queries of all employees subject to the provisions of the Lautenberg Amendment, to verify compliance with the Lautenberg Amendment.

212.00 Use of Badge and Credentials

OIG badges and credentials are to be used for official identification only and not for personal identification, advantage, or special favor. Any misuse of badges or credentials will result in disciplinary action.

Special agents should always present their credentials and badges and identify themselves as OIG special agents unless precluded by the nature of the specific assignment, such as undercover work. Other investigative staff should likewise present their credentials in the same manner.

Special agents must exercise every precaution necessary to prevent the loss or unauthorized use of credentials and badges. Special agents are not authorized to make photocopies of their badge or credentials or allow others to make photocopies. A special agent who loses his or her credentials or badge should immediately report the loss to his or her immediate supervisor and to the local law enforcement authorities. The agent will then submit a written statement detailing the circumstances of the loss to include steps taken to locate the credentials and badge. Depending on the circumstances of the loss of the credentials or badge, the special agent may be subject to disciplinary action.

220.00 Training

It is desirable that all newly appointed criminal investigators possess a degree from an accredited four-year college or equivalent work experience. It is OIG policy to provide entry-level special agents and other investigative staff with appropriate formal basic training to ensure development of skills in the following areas:

- Proficiency in obtaining information from people;

- the ability to analyze and evaluate facts, draw sound conclusions, and make constructive recommendations; and,
- the ability to deliver concise, factual summaries of the results of the investigation, both orally and in writing.

220.10 Entry-Level Training

Special agents are required to complete a program of instruction that fulfills all the basic criminal investigative training requirements for the professional Federal law enforcement officer. All entry-level special agents must successfully complete the basic criminal investigative training course at the Federal Law Enforcement Training Center at Glynco, Georgia or equivalent training. Entry-level special agents must also successfully complete the Inspector General Criminal Investigator Training Program at the Inspector General Criminal Investigator Academy (IG Academy). Experienced special agents hired from other Federal law enforcement agencies, but who are new to the OIG community, must successfully complete the IG Academy's Transitional Training Program.

Other investigative staff of OI will be provided entry-level training appropriate to their position description and tasks they are assigned. For example, analysts and forensic auditors must successfully complete the IG Academy's Basic Non-Criminal Investigators Training Program.

220.20 In-Service Training

All special agents and investigative staff, as appropriate, will receive periodic in-service training in the following areas: trial process; federal criminal and civil legal updates; interviewing techniques and policy; law of arrest, search and seizure; and physical conditioning/defensive tactics. OPM/OIG/OI requires special agents to complete FLETC's Continuing Legal Education Training Program (CLETP), the IG Academy's Periodic Refresher Training, or an equivalent refresher training course, every three years. In addition, all personnel will attend firearms, defensive tactics and program specific training as required to meet the mission of the OIG.

230.00 OIG Relationship with Prosecutive Authorities and Other Law Enforcement

230.10 OIG Relationship with U.S. Attorneys

All investigative staff in the OIG are expected to establish and maintain working relationships with U.S. Attorneys' Offices that permit both formal and informal discussion of OIG investigations.

Formal presentations of investigative cases to U.S. Attorneys' Offices normally occur after completion of all investigative steps. However, special agents are expected to consult with the U.S. Attorney's Office as soon as information is developed indicating an investigation may corroborate an allegation of a criminal violation. Early consultation will allow the OIG to focus investigative efforts on cases with prosecutive potential, and to ensure that investigations fully support prosecutive potential.

230.20 OIG Relationship with the Department of Justice

Upon determining that a complaint or allegation warrants investigation, the AIGI, DAIGI, SAC, or ASAC will decide whether referral to the FBI is appropriate. Once a complaint is converted to an investigation, the DAIGI, within 30 days, will notify FBI Headquarters, who in turn will notify the FBI district in which the investigation is being conducted.

In cases involving allegations against high level OPM officials, a determination will be made whether or not to contact the Department of Justice Public Integrity Section.

230.30 OIG Relationship with Other Law Enforcement Agencies

Upon receipt of an allegation, AIGI, DAIGI, SAC or ASAC will decide whether to initiate an OIG investigation, refer the complaint or allegation to another law enforcement agency, or conduct a joint investigation with another law enforcement agency.

A complaint or allegation may be referred to another law enforcement agency when one or more of the following conditions apply:

- The subject matter is by law investigated by another agency;
- the complaint or allegation does not involve OPM employees, contractors, programs, or property;
- the complaint or allegation indirectly involves OPM employees, programs, or property, but has a major impact on another agency; and,
- the complaint or allegation involves a threat to the safety of the President or any other high government official.
- the OIG lacks sufficient resources to address the allegation, and another agency shares jurisdiction.

230.35 CIGIE Mutual Assistance Policy

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) has instituted procedures to obtain assistance from another OIG in the execution of Search and Arrest warrants.

On June 28, 2010, the Attorney General issued Order No. 3168-2010, which authorized:

special agents of each Office of Inspector General ("OIG") otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act, (b) (7)(E)

The Order authorizes such assistance only for (b) (7)(E)

The Order also states that "assistance provided by one IG to another ... must comply with procedures to be established by the Council of Inspectors General on Integrity and Efficiency."

Procedures

Pursuant to the Attorney General's instruction in Order No. 3168-2010, CIGIE establishes the procedures contained herein. These procedures reflect the sole means by which an OIG may obtain from other OIGs the assistance authorized by the Attorney General's Order. These procedures are applicable only to assistance provided pursuant to this Attorney General's Order, and are not applicable to any other form of assistance provided by one OIG to another.

1. The Inspectors General, or their designees, must individually determine whether their OIGs will participate in the program of inter-OIG mutual assistance authorized by the Attorney General. The decision to participate in the program does not obligate an IG to commit personnel in response to any particular request, which is a decision that will be made on a case-by-case basis.
2. A participating OIG in need of additional manpower for the execution of a Federal search or arrest warrant (Requesting OIG) must submit a request in writing to the appropriate Inspector General, or his or her designee, of another participating OIG (Assisting OIG). The written request must contain, at minimum, the following:
 - a. case background sufficient to establish the Requesting OIG's jurisdiction;
 - b. the type of operation (search or arrest);

- c. the operational plan (including the number of personnel needed and the duration of the assistance to be provided and a discussion of foreseeable risks); and
 - d. a statement that the appropriate Federal prosecutor has been notified of the request.
3. The written request -- once approved and signed by the Inspectors General (or their designees) of both the Requesting and Assisting OIG -- will serve as the basis for an Inter-Agency Agreement governing the Requesting OIG's use of the Assisting OIG's personnel, but only for the purposes of the operation described therein.
4. Nothing in the Attorney General's Order or in these procedures obligates reciprocal assistance on the part of an OIG that has received assistance in the past. It remains within the discretion of an OIG to approve or to deny, in whole or in part, a request for assistance. Additionally, the Attorney General's Order and these procedures do not specifically prohibit other types of mutual assistance that is consistent with law and regulation.
5. Special agents designated to participate in response to a request may be provided to the requesting agency on a reimbursable basis, unless otherwise prohibited by law.

230.40 Procedures for Referrals to Other Law Enforcement Agencies

Referrals are made by the AIGI, DAIGI or SAC to the appropriate official of the other agency's office having jurisdiction over the allegation.

All referrals will be made via letter, except in urgent circumstances. In those instances, referrals will be made either telephonically or in person, but must be confirmed in writing as soon as possible.

Referral letters should contain a presentation of the complaint or allegation and any facts developed by the OIG, as well as a statement that the matter is being referred for informational purposes and any action judged appropriate. When appropriate, an offer of OIG assistance and support will be made..

230.50 Procedures for Referrals Involving Threats Against Government Officials

(b) (7)(E)



(b) (7)(E)

230.60 OIG Relationship with State and Local Prosecutors

When federal prosecutors decline OIG referrals or express no Federal interest during early consultation on an investigative case, special agents should be mindful for opportunities to seek prosecution by state or local authorities. Examples of violations experienced in OIG investigations that could be prosecuted in state or local courts are: theft of Government property from non-federal premises, fraud by health providers, and criminal trespass, etc.

When state or local prosecutors accept OIG cases, special agents will provide assistance and follow the same administrative and reporting procedures as in federal prosecutions.

230.70 OIG Relationship with Office of Special Counsel

The Office of Special Counsel is responsible for investigating allegations and other information regarding prohibited personnel practices, primarily reprisal against Whistleblowers, prohibited political activities by federal employees (Hatch Act), arbitrary or capricious withholding of information in violation of the Freedom of Information Act, and other activities prohibited by any civil service law, rule, or regulation (**Appendix C**). The Office of Special Counsel also initiates disciplinary and corrective actions before the Merit Systems Protection Board when warranted.

The Office of Special Counsel is also responsible for receiving and referring to the appropriate agency information that alleges: a violation of any law, rule, or regulation; mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.

All matters that are reported to the Office of Special Counsel on behalf of the OIG should be coordinated by the AIGI.

240.00 Use of Government Vehicles

Reference is made to Title 31 of the United States Code, Section 1344, and other statutes and regulations pertaining to the use of Official Government Vehicles (GOVs). An employee

operating a GOV is required to obey General Services Administration (GSA) regulations concerning vehicle usage. These are contained in the Federal Management Regulations, 41 CFR, Subchapter B, Part 102-34, Motor Vehicle Management.

The use of a GOV is a privilege that brings with it a great deal of personal responsibility, to include the potential for personal liability if relevant laws, regulations, and policies are not followed. Every person driving a GOV must ensure that it is used only for official business within the scope of the driver's employment, that the vehicle is maintained in good operating condition, and that it is driven in a safe and legal manner.

240.01 Penalties for Improper Use

Pursuant to 31 U.S.C. 1349(b), any employee who uses a GOV for other than official purposes, or authorizes another person to use a GOV for other than official purposes, shall be suspended without pay for thirty days. When circumstances warrant, an employee can be suspended longer, or summarily removed from Government service for abuse of a GOV.

240.10 Record Keeping/Log Sheet



240.20 Personal Responsibility

Your responsibilities while operating a GOV include:

240.21 Safe Driving

You are responsible for driving safely. This includes wearing your seat belt, using any other provided safety devices, and following motor vehicle manufacturer safety guidelines (Reference 41 CFR §102-34.250).

240.22 Valid Driver's License

You must have a valid driver's license in order to operate a GOV. If the state which issued your driver's license revokes, suspends, or restricts your driver's

license, you must report it immediately to the AIGI.

240.23 Reasonable Protection from Theft or Damage

You are responsible for parking the GOV in a manner that reasonably protects it from theft or damage. This includes locking an unattended car (Reference 41 CFR §102-34.230). (b) (7)(E)

(b) (7)(E)

240.24 Obey Traffic Laws

Per 41 CFR §102-34.235, “You must obey all motor vehicle traffic laws of the State and local jurisdictions, except when the duties of your position require otherwise. You are personally responsible if you violate State or local traffic laws. If you are fined or otherwise penalized for an offense you commit while performing your official duties, but which was not required as part of your official duties, payment is your personal responsibility.” If cited for a traffic violation while operating a GOV, you must attach a copy of the notice of infraction to your monthly mileage log.

240.25 Personal Liability for Fines

If you are fined for a parking violation while operating a GOV, you are personally responsible for paying the fine (Reference 41 CFR §102-34.245). If you receive a parking ticket, you must attach a copy of it to your monthly mileage log. You are responsible for filing any appeals of tickets, if applicable.

240.30 Prohibitions

Certain actions are prohibited while operating a GOV, such as:

240.31

(b) (7)(E)

(b) (7) (E)

240.32

240.33

240.40 Maintenance

All investigative staff with assigned GOVs are responsible for the cleanliness and safe operation of the GOV. Use regular, unleaded, self-service fuel, unless the assigned GOV specifically requires a different fuel for safe operation. Drivers must obtain in a timely manner any routine or general maintenance, necessary repairs, and required State inspections. Depending on the State, required inspections may include federally-mandated emissions inspections and/or motor vehicle safety inspections (Reference 41 CFR §102-34.275 - §102-34.280).

Oil changes and other general maintenance are not to be performed until notified by your local GSA Fleet Service Representative (FSR). Once notification is received, maintenance shall be performed promptly. You must use a GSA approved vendor. If maintenance or repairs need to be completed before notification by the FSR, the GSA Maintenance Control Center (MCC) will be contacted by using the telephone numbers on the back of the GSA charge card. When obtaining an estimate for repairs or maintenance from a vendor, the vendor will contact GSA directly.

The OIG vehicle manager is responsible for timeliness of GOV maintenance on vehicles not assigned to specific investigative staff members.

The OIG will coordinate with the General Services Administration (GSA) to ensure that the GOVs used by the OIG are the smallest, most fuel efficient, and least greenhouse gas emitting vehicles necessary to execute mission requirements.

240.45 Charge Cards

Each vehicle has a GSA charge card assigned to it. Gasoline is charged to this charge card, and the driver must ensure that the current mileage is entered into the pump mechanism along with the GSA assigned access code. Fill the gas tank at least once per month so that GSA has a record of the GOV's odometer reading.

The GSA charge card will be used for maintenance upon approval by GSA. All charge slips, maintenance receipts, and monthly mileage logs will be scanned into the ITS and the hard copy will be maintained by the SA.

The GSA charge card may also be used to procure "immediately consumable" items in accordance with GSA policy, provided the items are necessary for the safe operation of the GOV, such as car washes, motor oil, and windshield washer fluid. GSA charge cards are for the operation and maintenance of the affiliated GOV **only**. Do not use your GSA charge card for a different GOV, or for any other type of procurement. (For example, you would use your travel card, **not** your GSA charge card, to put gas in a short-term rental car that you leased while traveling.) Misuse or abuse of a GSA charge card is grounds for disciplinary action.

240.50 Damage/Accidents

If a driver is involved in an accident, the primary responsibility of the driver/passengers is to obtain aid for any injured party and to notify the appropriate local law enforcement agency. All accidents involving damage and/or personal injury will immediately be reported to the agent's supervisor and the AIGI. GOVs will be equipped with Standard Form (SF) 91, "Motor Vehicle Accident Report" and SF-94, "Statement of Witness." As soon as practicable after the accident, the driver is required to submit a memorandum to the AIGI explaining the circumstances of the accident, with completed forms SF-91 and SF-94 attached. At the scene of the accident, notify the GSA Accident Management Center by calling the toll free telephone number on the back of the GSA charge card.

If a driver notes damage to an assigned vehicle(eg. miscellaneous scratches/dents, vandalism, storm damage, damaged upholstery, chipped windshields, etc.), timely notification should be made to the driver's supervisor. A written report of the damage will be provided to the SAC with a copy to the OIG vehicle manager. The GSA MCC should be contacted by using the telephone number on the back of the GSA charge card. The MCC will provide instructions including providing GSA approved vendors for the repairs.

If a GOV is damaged due to misconduct of the driver, the driver shall be held financially responsible. Misconduct includes, but is not limited to, vehicle operation under the influence of alcohol or narcotics and the willful abuse or misuse of the vehicle.

240.60 Emergency Equipment

Emergency equipment present in or on GOVs, such as lights, sirens or other items are to be operated only when necessary for the successful accomplishment of law enforcement missions. Misuse of emergency equipment is grounds for disciplinary action. Operation of emergency equipment does not provide immunity from traffic rules. Drivers must obey all local traffic laws and regulations and are responsible for any violations that occur.

(b) (7)(E)



240.70 Home-To-Work Transportation (HTW)

(b) (7)(E)



- ▶ 
- ▶ 
- ▶ 

240.80 Requesting Reimbursement for Tickets/Penalties Incurred as a Necessary Part of Performing Official Duties

The OIG, as well as many local traffic and parking enforcement authorities, recognize that law enforcement officers may encounter exigent circumstances in which it may be in the public interest for the officer to violate traffic or parking rules. (Reference 41 CFR §102-34.235) If fined or

penalized for a violation necessitated by your official duties, it is appropriate to appeal to the appropriate state or local authorities, who typically weigh the violation against the official business being conducted when adjudicating the appeal. If you appeal such a ticket, the appeal is denied by the issuing authority, and you pay the ticket despite a personal conviction that the ticket was issued and/or adjudicated improperly, you may formally request approval to be reimbursed via miscellaneous voucher.

A request for reimbursement should take the form of a memorandum to the AIGI and provide a detailed explanation of the circumstances surrounding the incident. This explanation should include the nature of the official business in which you were engaged at the time of the violation, any applicable exigent circumstances, proof that an appeal was filed and adjudicated, and any other relevant facts to support your request that the OIG assume liability for the expense. The bottom of the request memorandum should include space in which the AIGI may mark whether your request is approved or denied, the date, and a signature line for the AIGI. Requests for reimbursement for fines/penalties will **not** be routinely approved; you must present a compelling argument sufficient to overcome both the presumption of personal liability and the presumption of proper adjudication by the state/local authority. Requests for reimbursement will only be approved if it can be demonstrated that the violation was necessary in order to perform your official duties and that it was in the interest of public safety.

240.90 Parking Permits for Federal Parking Facilities

(b) (7)(E)

. When space in Federal parking facilities is at a premium, GOVs are granted space on a priority basis. Agents issued parking permits must be cognizant of the fact that parking in a Federal facility is a privilege many OPM employees do not have and that it has significant financial value. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) |

An email exchange is sufficient. (b) (7)(E)

Supervisors and employees must keep in mind that abuses of permits for Federal parking facilities may result in revocation of the permit by the relevant parking authority. (b) (7)(E)

250.00 Law Enforcement Availability Pay

Law Enforcement Availability Pay (LEAP), as authorized by the Law Enforcement Availability Pay Act of 1994, codified at 5 U.S.C. §5545a, is the 25% premium paid to ensure the “availability” of criminal investigators for unscheduled duty in excess of their 40-hour basic workweek. LEAP is paid to law enforcement officers, as defined under 5 U.S. C. 5541(3), whose position is properly classified under the GS-1811 or GS-1812 series in the General Schedule Classification System. LEAP will be considered as part of basic pay for the computation of retirement benefits, lump sum annual leave, life insurance, advances in pay, severance pay, and workers compensation. Special Agents eligible to receive LEAP are exempt from the Fair Labor Standards Act of 1938.

Availability means that an agent shall be either performing official duties during unscheduled duty hours or considered generally and reasonably accessible to perform official duties during unscheduled duty hours based on the needs of the OIG. Unscheduled duty hours are those hours that are not a part of the 40 hours in the basic workweek and not regularly scheduled overtime payable under 5 U.S.C. 5542.

(b) (7)(E)

(b) (7)(E) The agent is generally responsible for recognizing, without supervision, circumstances that require the agent to work during unscheduled hours, or to be available for unscheduled duty. However, supervisors may place an agent in availability status by directing the agent to be available during designated periods to respond to specific OIG needs. LEAP will be recorded and certified in the ITS.

250.10 General Rules

SAs shall continue to be paid LEAP if their annual daily average of unscheduled hours is equal to or greater than two hours per qualifying work day. Exemptions to the qualifying work day, also known as excludable days, include any day on which an agent took four or more hours of leave, including time-off incentive awards; received four or more hours of training; traveled four or more hours while on official travel orders; was excused from work for relocation; and any legal public holiday designated by the federal government. An excludable day will also result if time spent on any combination of the above exempt activities totals four or more hours (eg. two hours spent training, plus two hours of official travel).

SAs will continue to receive LEAP in the event of agency sanctioned training; relocation; travel; and annual leave, sick leave, or any excused absence with pay.

Compensation, either by overtime pay or compensatory time off, for unscheduled duty hours worked in excess of the required annual average is not authorized for those receiving LEAP pay.

A SA who is directed by a supervisor to be available for duty during unscheduled duty hours is not necessarily required to remain in the office or at home, but may be reachable by telephone at the discretion of the supervisor.

Outside employment or other activities is generally not approved for agents receiving LEAP. The AIGI may, in rare instances, approve outside activities or employment under certain circumstances where the agent has no specific time commitment and availability for LEAP will not be impacted. Please see the OIG policy regarding "Employee Disclosure of Outside Activities" for further information.

An involuntary reduction in pay resulting from a denial of certification and removal from LEAP is considered an adverse personnel action. As such, all such actions must be coordinated through the AIGI and the OIG Administrative Officer. A supervisor may propose revoking an SAs LEAP certification at the end of the certification period based on a finding that the agent has failed to meet the required annual daily average of unscheduled hours (e.g. due to the avoidance of work or non-availability of the agent).

250.11 Voluntary Opt-Out

The Law Enforcement Availability Pay Act of 1994 contains a voluntary opt-out provision. SAs experiencing a personal or family hardship situation may submit a written request to be exempt from working unscheduled duty hours for a designated period of time, with the understanding that availability pay will not be payable during that time. The OIG will consider voluntary opt-out requests on a case by case basis.

250.12 LEAP Reporting Requirements

Before being placed on LEAP, and at the beginning of each fiscal year thereafter, each agent must certify in the ITS that they agree to be available for unscheduled duty based on the needs of the OIG.

By October 31st of each year, each Special Agent in Charge will certify that all agents under their supervision met the LEAP requirements in the previous fiscal year and are expected to meet the requirements in the upcoming fiscal year. The AIGI in turn certifies annually to the Inspector General that the agents (listed by individual names and titles) met the LEAP requirements for the preceding fiscal year and are expected to continue doing so. The Inspector General annually notifies the Director of OPM that the LEAP requirements have been met.

Agents will record their unscheduled duty hours for annual LEAP certification purposes by accurately completing the Investigative Tracking System Biweekly Activity Report. The agent's supervisor will review and approve these reports.

250.13 Biweekly Activity Reports

The Biweekly Activity Reports will correspond to official pay periods, which end on alternate Saturday nights at midnight. Agents will submit their Reports to their supervisor no later than Friday following the pay period ending date, or at the first opportunity if assigned duty prevents access to the Investigative Tracking System.

Time reported under the various categories will be rounded to the nearest quarter hour. Time spent traveling for official travel outside the regular workday or basic workweek may be claimed as unscheduled duty hours, and should be charged to the activity with which the travel was associated. Time spent on agency-permissible Physical Fitness Training will be charged as fitness training. On holidays, weekends, or when an agent takes a full day of leave, PT may NOT be counted as a LEAP activity.

Chapter 3 Complaint Control

300.00 Complaint Control - General

Information gathered from complaints received by the OIG is used to initiate investigations, audits and inspections and to alert the Inspector General, OIG components, as well as OPM management officials, of potentially serious problems in OPM programs and operations.

310.00 OIG Hotline, Reporting Fraud, Waste and Mismanagement

Anyone who has information regarding fraud, waste, mismanagement or whistleblower complaints in OPM programs and operations may send written complaints to:

**U.S. Office of Personnel Management
Office of the Inspector General
Fraud Hotline, Room 6400
1900 E Street, NW
Washington, D.C. 20415**

The OIG Fraud Hotline can be reached by calling 1-877-499-7295. Hotline complaints can also be submitted anonymously online at <http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse/>.

310.10 Complaint Processing

All allegations and/or complaints received by the Office of Investigations will be entered in the Office of Investigations, Investigative Tracking System (ITS). This includes complaints received on OIG hotlines, letters, and notifications or referrals received from all sources. All Hotline complaints, including correspondence, are initially screened by a member of the OI Investigations Support Group (ISG). Hotlines will be entered into the ITS by ISG in the Hotline section of the ITS. Hotlines refer only to information received by the OIG Hotline. Referrals from other sources, including the Department of Justice, other Federal and state investigative or prosecutorial agencies, OPM program offices, and OPM contractors, are evaluated by the DAIGI, SAC, or ASAC.

Allegations and/or complaints will be entered into ITS by the first and last name of the subject, without listing titles or educational degrees. However, in retirement cases where the subject is unknown, the case name will be the name of the deceased annuitant. The address of the subject, if known, will be included in the "Allegation" section of ITS.

Once a complaint has been entered in ITS, the SAC, or ASAC will approve the complaint.

ITS contains five numbering systems. Complaints are identified by a 'C'; Investigations are identified by a 'I'; Hotlines are identified by 'H'; Raw Data entries are identified by "R"; and, Proactive Projects are identified by 'P'. These initial letters are followed by the fiscal year received and successively numbered, i.e., C-12-00001 being the first complaint received in fiscal year 2012.

All allegations received by OI are initially numbered as a complaint, excluding hotlines, raw data and proactive projects, for preliminary inquiry by investigative staff. A hotline or raw data allegation that cannot be immediately assessed without preliminary inquiry shall be converted to a complaint. Likewise, when a proactive project identifies an allegation regarding a particular subject or target, a complaint number shall be generated.

If an assigned complaint is resolved or closed at the preliminary inquiry stage, without ever being converted to an investigation. When closing a complaint special agents should complete a short Investigative Activity Report that would include the following information: date received, referred from, allegation, findings, closing date and reason for closure (b) (7)(E)

- ▶ [REDACTED]
- ▶ [REDACTED]
- ▶ [REDACTED]

For purposes of this investigative manual, the term 'case or cases', will be used to describe complaints and investigations.

310.11 Advising Hotline Sources on Policies for Protecting Their Identities

The **Inspector General Act of 1978**, provides in part that the identity of employees who make complaints shall not be disclosed "...without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation." The **Civil Service Reform Act of 1978** contains similar requirements, as codified at 5 U.S.C. §12066(b)(1)(B).

All requests for confidentiality should be documented in the Investigative Tracking System (ITS). The person answering the Hotline call should be prepared to provide advice and information to Hotline complainants about protection of identities as follows:

1. When a Hotline complainant asks about confidentiality, the complainant should be advised that, consistent with the IG Act, the identity of an OPM employee complainant will be protected from disclosure, unless such disclosure is unavoidable during the course of the investigation. The identity of a complainant who is not an OPM employee will be provided the same degree of confidentiality as an OPM employee even though the IG Act addresses only complainants who are agency employees.
2. When a complainant specifically requests confidentiality, he or she should also be advised that confidentiality can never be fully guaranteed, since disclosure could be necessary in a case involving judicial action (See IM 502.16 – 502.19).
3. When a Hotline complainant states that he or she has no objection to being identified as the source of the complaint in any referral to government officials, the complainant should be advised in general terms of the course such a referral could take in order to minimize the possibility of a misunderstanding about identity disclosure.

311.00 Threats Against the President of the United States, Cabinet Members, and Members of Congress

(b) (7)(E)



320.00 Whistleblower Protection

Federal whistleblower protection laws prohibit employers from taking personnel actions in retaliation against individuals who disclose information they reasonably believe evidences fraud, waste, abuse, or mismanagement. The laws provide legal and administrative remedies for individuals who are subjected to whistleblower retaliation. These remedies offer the victims of reprisal the opportunity to be made whole, and also act as a deterrent to dissuade managers from engaging in retaliatory prohibited personnel practices.

When a person contacts the OIG, it is foreseeable they may also have questions about the possible consequences of their decision to speak up. Some individuals may seek reassurance from the OIG before they are willing to disclose the information that inspired them to reach out. Others may contact the OIG specifically because they feel they have been or might be subjected to retaliation

for a disclosure they previously made and want to know what to do. It is essential that investigative staff be familiar not only with the ways that the OIG can assist these individuals, but also with the limitations on what the OIG can do, and how to direct claimants to appropriate resources.

Different laws establish different procedures depending on whether the individual in question is a Federal employee (or former employee, or applicant for employment) or an employee of a Federal contractor (or subcontractor or grantee). Additionally, there is a separate process governing allegations by Federal employees that their access to classified information has been revoked in retaliation for making a protected disclosure. The requirements that must be met for an individual to be considered a “whistleblower” also differ in each situation. In each of these three situations, the OIG plays a different but important statutory role in the process. The procedures for responding to claims of whistleblower retaliation in each situation are described below.

Additional information regarding whistleblower rights and protections can be found on the websites of the Office of Special Counsel (www.osc.gov) and Merit Systems Protection Board (www.mspb.gov). The OIG also maintains a Whistleblower Protection Information page on its website (www.opm.gov/our-inspector-general/whistleblower-protection-information/) in fulfillment of the Whistleblower Protection Enhancement Act’s requirement that the OIG maintain a Whistleblower Protection Ombudsman program.

320.10 Whistleblower Protection for Federal Employees, Former Employees, and Applicants for Employment

The Whistleblower Protection Act of 1989, as amended, establishes the right of federal employees, former employees, and applicants for employment to appeal to the Office of the Special Counsel (OSC) or the Merit Systems Protection Board (MSPB) if they believe that they have been subjected to punitive personnel actions because of whistleblowing activities. Specifically, it is a prohibited personnel practice for an agency official to take or fail to take, or threaten to take or fail to take, a personnel action against an employee or applicant for employment because of that person’s disclosure of wrongdoing. “Personnel action” in this context means an appointment, promotion, disciplinary action, detail, transfer, reassignment, reinstatement, restoration, or reemployment; a decision concerning performance evaluations, pay, benefits, awards, education, training; or any other significant change in duties, responsibilities, or working conditions. In addition, the law prohibits retaliation for filing an appeal, complaint, or grievance; helping someone else file or testifying on their behalf; or cooperating with or disclosing information to the OIG.

To establish a case of whistleblower retaliation, a claimant must first show that he or she made a disclosure of information that an employee, former employee, or applicant for employment reasonably believes evidences—

- violation of any law, rule, or regulation;
- gross mismanagement;
- gross waste of funds;
- abuse of authority; or
- substantial and specific danger to public health or safety.

Once this threshold is established, the claimant must show that the agency official responsible for the alleged retaliatory personnel action knew of the disclosure, and that the disclosure was a contributing factor in the personnel action.

Federal employees who wish to pursue the remedies provided by whistleblower protection laws must file a claim with OSC. Although the OIG can receive, investigate, and issue reports of findings and recommendations regarding complaints of prohibited personnel practices within OPM programs, including whistleblower retaliation, the OIG is prohibited from intervening or advocating on behalf of an employee making such a claim. Unlike the OIG, the OSC has authority not only to investigate claims, but also to seek administrative and legal remedies on behalf of retaliation victims, including working with the agency and, when merited, seeking an order from MSPB.

320.11 Procedures for Responding to Claims of Retaliation by Revocation of an OPM Employee's Security Clearance

As defined under the WPA, "personnel action" does not include an action affecting an employee's access to classified information, so victims of retaliation in that form are not covered. However, effective July 8, 2013, Presidential Policy Directive 19 (PPD-19) extends whistleblower protection coverage to employees who experience this type of retaliation. The types of protected disclosures covered by PPD-19 are more limited than under the WPA: the protection only extends to employees whose disclosures were 1) to a supervisor in the employee's direct chain of command, including the Director of OPM, or 2) to the Inspector General, or 3) to an employee designated by either of the above officials for the purpose of receiving such disclosures. The protection also extends to employees who cooperate with or disclose information to the OIG in connection with an audit, inspection, or investigation.

Unlike the prohibited personnel practices established by the WPA, retaliation or threatened retaliation relating to an employee's security clearance is not within the jurisdiction of the Office of Special Counsel or the Merit Systems Protection Board. Instead, PPD-19 requires each agency to establish an internal review process to address whether the denial or revocation of an employee's clearance should be reconsidered because it was based on retaliation for the employee's protected whistleblower disclosures. A requirement of this process is that the OIG investigate the allegation and issue a report of findings to the Director of OPM that may recommend corrective or disciplinary action. Any OPM employee whose security clearance is denied or revoked should receive a notice from OPM

Facilities, Security and Contracting fully explaining the review and appeals process.

320.20 Whistleblower Protection for Employees of Federal Contractors, Subcontractors, and Grantees

The National Defense Authorization Act of 2013 (NDAA) established a pilot program extending protection to employees of contractors who disclose fraud, waste, and abuse. The elements of a whistleblower retaliation claim in this context are narrower than for Federal employees. Specifically, contractors, subcontractors, and grantees of Federal agencies may not discharge, demote, or otherwise discriminate against an employee as a reprisal for making a “protected disclosure” of information that the employee reasonably believes is evidence of:

- gross mismanagement of a Federal contract or grant;
- an abuse of authority relating to a Federal contract or grant;
- a substantial and specific danger to public health or safety; or
- a violation of law, rule, or regulation related to a Federal contract or grant.

“Protected disclosures” in this context include information shared with:

- members of Congress or representatives of congressional committees;
- an Office of Inspector General;
- the Government Accountability Office;
- a Federal employee responsible for contract or grant oversight or management;
- an authorized official of the Department of Justice or other law enforcement agency;
- a court or grand jury; or
- a manager or other employee of the contractor, subcontractor, or grantee who has responsibility for investigating, discovering, or addressing misconduct.

It is important to note that this protection extends only to contractors and subcontractors whose contracts became effective or were amended on or after July 1, 2013, or to whom new task orders have been issued since that date. Additionally, a complaint may not be brought more than three years after the date on which the alleged reprisal took place.

The OPM OIG is the only entity to which employees of OPM contractors may bring complaints of whistleblower retaliation. The NDAA requires that within 180 days following receipt of a complaint, or within any extended time period up to 180 days as agreed to with the complainant, the OIG will either:

- Investigate the complaint and submit a report of findings to the Director of OPM, the person who submitted the complaint, and the person’s employer; or

- Dismiss the complaint based on a determination that it is frivolous, fails to allege a violation of the whistleblower protection law, or has already been addressed in another judicial or administrative proceeding initiated by the complainant.

If the OIG proceeds with the investigation and issues a report, the Director will review the report and determine whether there is sufficient basis to conclude that the contractor or subcontractor has subjected the employee to a prohibited reprisal. The Director has 30 days following receipt of the report to issue an order either denying relief or granting one or more of the following corrective actions:

- Order the contractor or subcontractor to take affirmative action to abate the reprisal;
- Order the contractor or subcontractor to reinstate the complainant to the position held before the reprisal, together with compensatory damages (including back pay), employment benefits, and other terms and conditions of employment that would apply if the reprisal had not been taken;
- Order the contractor or subcontractor to pay the complainant an amount equal to the aggregate amount of all costs and expenses (including attorneys' fees and expert witnesses' fees) that were reasonably incurred by the complainant for, or in connection with, bringing the complaint, as determined by the Director.

If the Director denies relief or if no action has been taken within 210 days of receipt of the complaint (or 30 days following expiration of any extension agreed to between OPM OIG and the complainant), the complainant may bring an action in an appropriate United States district court against his or her employer as described under 41 U.S.C. § 4712.

If the Director orders a corrective action and the contractor or subcontractor fails to comply, the Director must file an action for enforcement in the appropriate United States district court. The complainant may also file or join such an action seeking enforcement of an order.

Chapter 4

Investigative Management

400.00 Investigative Management Procedures

The case management and control process enables management to monitor the assignments and responsibilities of the investigative staff. It also facilitates informed judgments about resource allocation, training needs, and investigative program development.

The AIGI, along with the DAIGI and SACs, approve the establishment of investigations, provide continuing guidance in conducting investigations, and approve dispositions of investigative cases.

These procedures are intended to ensure that all investigations are conducted:

- In a diligent and thorough manner, in accordance with all applicable laws, rules, and regulations.
- In a fair and impartial manner, with respect for the privacy and rights of those involved.
- With the persistence necessary to determine the facts.

Evidence will be gathered and reported in an unbiased and objective manner. Investigations will be conducted and reported in a timely manner.

400.10 Preliminary Investigative Activity

The investigative process begins upon the OIG's receipt of an allegation of fraud, waste, abuse, or mismanagement involving programs or activities within the jurisdiction of the agency.

The information may be general, citing a deficiency in a program's operation, or it may be specific, identifying individuals, contractors, or other entities engaged in illegal activities. The information may come from various sources, including agency employees or officers, other OIG components, other government or private sector agencies, private citizens not connected with OPM, the news media, confidential informants, or confidential sources.

400.20 Proactive Investigative Activities

Investigations also may be initiated as the result of information developed within the Office of Investigations rather than from expressed allegations of wrongdoing received by the OIG. Such proactive investigative activities are an important means of developing investigative cases.

The Office of Investigations may initiate investigations as a result of information developed through structured reviews of program areas with potential vulnerability to fraud, waste, or abuse. Additionally, investigative staff may, through independent leads and sources, develop information that warrants opening an investigation. Such information will be reviewed by the AIGI, DAIGI, or SAC to determine if an investigation is warranted.

400.30 Investigative Sources and Informants

Subject to appropriate laws, regulations and OIG policy, special agents are encouraged to develop sources and use confidential informants as discussed in **IM Para 502**.

A source is any person who furnishes information, whether or not the information has specific investigative value. Developing sources is a basic investigator skill requirement. Accepting information on a confidential basis and protecting identities of sources are important aspects of source development.

A confidential informant (CI) is an individual who expressly requests confidentiality; or a person a special agent recognizes as needing his or her identity protected. Confidential sources and informants are sources and informants of the OIG, and not of a specific special agent.

410.00 Initiation of Investigative Activity

(b) (7)(E) [Redacted]

[Redacted]

† [Redacted]

† [Redacted]

† [Redacted]

410.10 Accepting a Case for Investigation

(b) (7)(E)

410.20 Referring a Case for Action by Agency Program Officials

Many instances of waste, mismanagement, or minor misconduct can be addressed by responsible program officials in lieu of an OIG investigation. The OIG does not investigate minor disagreements and disputes between management and employees. Additionally, as a normal practice, the OIG does not investigate allegations regarding Equal Employment Opportunity (EEO). However, exceptions can be made when the allegations involve a senior manager and OPM may be held liable for his/her actions.

An allegation will be referred to an agency program official for action when:

1. Issues are clearly of a nature that would not logically lead to criminal prosecution or affirmative civil enforcement.
2. Issues are of the type that are traditionally resolved and corrected by program managers, supervisors, personnel officers, or employee relations officials.
3. Issues do not require complicated investigative techniques for resolution.

410.30 Referral to OPM Organizations

Cases referred to OPM organizations for action are assigned to an investigative staff member, who monitors activities and disposition of the case. This includes providing assistance to the official

involved by pointing out the specifics that need to be resolved and ensuring that 1) the results of the inquiries are responsive to the allegations, 2) the issues have been fully addressed, and 3) appropriate corrective action has been taken. OI assistance and monitoring efforts and results are placed in the case file.

410.40 Referral to Another Government Agency

An allegation will be referred to another agency when:

1. The allegation does not relate to OPM employees or programs but does pertain to employees or programs of another government agency.
2. The allegation pertains to an OPM employee, but the program responsibility lies within another agency. For example, an allegation that an OPM employee misused Veterans' benefits would be referred to the Department of Veterans' Affairs, with OIG follow-up and monitoring.
3. The allegation relates to an OPM employee, but another agency has enforcement or regulatory jurisdiction. For example, an allegation that an OPM employee forged a U.S. government check would be referred to the U.S. Secret Service, with OIG follow-up and monitoring.
4. The OIG and another agency share enforcement or regulatory jurisdiction over the alleged violation, and the OIG lacks sufficient resources to address it.

410.50 Rejecting a Case Not Within the Scope of the OIG Jurisdiction or Investigations Policy

A case will not be initiated if the matter does not pertain to OPM employees, funds, programs, or property; there are no allegations of specific acts or omissions; or the information relates to a matter which has already been investigated or acted upon.

420.00 Administrative Case Control

The investigative tracking system (ITS) permits the electronic storage and retrieval of case-related documents and files. All cases must be entered in the ITS, and related documents/files should be uploaded into the ITS case record. Electronic documents too large to upload into the ITS case record shall be saved in OI's electronic file cabinet (b) (7)(E) (b) (7)(E) The OI maintains records electronically to the maximum extent practical, in order to reduce the costs/risks associated

with shipping sensitive information and to conserve physical storage space. Staff may print working copies of electronically stored case records if needed, but such working copies should be destroyed when no longer needed.

Although the OI stores as much of the case record as possible in electronic form, since the OI handles materials of evidentiary value, certain types of documents must be retained in hard-copy, such as handwritten agent notes. Within any hardcopy case file, documents will be firmly fastened. The hardcopy case file will bear a typewritten label identifying the case control number.

420.10 Case Control Number

See IM 310.10.

420.20 File Organization for Hotlines and Raw Data

(b) (7)(E)



420.21 File Organization for Complaints

(b) (7)(E)



(b) (7)(E)



420.30 File Organization for Investigations

(b) (7)(E)



The following materials must be stored separately from the closed hard-copy case file:

(b) (7)(E)



[Back to Table of Contents](#)

(b) (7)(E)



420.40 File Organization for Proactive Projects

(b) (7)(E)



420.50 File Security, Shipment, and Storage

Each employee of the Office of Investigations (OI) is personally responsible for safeguarding investigative materials, law enforcement sensitive information, and personally identifiable

information (PII) from unauthorized access. (b) (7)(E)

Employees are responsible for the security of both hardcopy and electronic files in their possession and may be subject to disciplinary action if files are lost or mishandled. Employees should not leave investigative material unattended outside of authorized working areas. Investigative materials should be concealed from casual observation of visitors. (b) (7)(E)

. Closed hardcopy case files, along with all original documents, will be secured in (b) (7)(E) (b) (7)(E)

- █ [Redacted]
- █ [Redacted]
- █ [Redacted]
- █ [Redacted]

(b) (7)(E)

[Redacted]

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



Please see  for further information.

(b)
(7)(E)

430.00 Caseload Management

The Office of Investigations receives allegations of differing importance, complexity, and potential for return on the investment of resources applied. OI managers routinely monitor the workload of active cases to prioritize them and ensure that the personnel resources available to the OIG are assigned consistently with case priorities.

(b) (7)(E)



(b) (7)(E)

430.10 Case Assignment

When a case is established, the SAC, ASAC for supervisors in the Major Frauds and Investigations Support Groups assigns the case to a special agent or other investigative staff member, taking into account the priority of the case, the workload, geographic location, and any special skills that may be required. If a case requires a larger commitment of staff, more than one staff member may be assigned.

430.11 Transfer of Cases Between Geographic Areas of Responsibility

In some instances, it may become necessary to reassign a case from an Agent in one geographic area to another. When a case is transferred from one geographic area of responsibility to another, the transfer will be coordinated between the SACS or ASACs for the affected areas, or by the DAIGI.

430.12 Lead Requests

When an Agent requires investigative assistance from another geographic or operational area of responsibility, such as assistance conducting an interview, a search warrant, or an arrest, the SACs or ASACs will coordinate the lead request.

430.13 Case Reporting Requirements

Unless otherwise authorized by the AIGI or DAIGI, all active cases will be updated by the assigned staff member no less than every 90 days in the investigative tracking system. Memoranda of Interview, Memoranda for the Record, Reports of Surveillance and use of other investigative techniques will be documented in the investigative tracking system within five working days of their occurrence.

All criminal, civil and administrative actions will be documented as investigative statistics in the investigative tracking system within five working days of their occurrence.

When significant case events occur (i.e, arrests, indictments/informations, convictions, financial recoveries), assigned staff are required to submit a short Investigative Activity Report (IAR) through the investigative tracking system, within five days, describing the significant event. A similar IAR is required when closing a complaint.

Following the culmination of all criminal, civil and administrative action, Final Reports of Investigation will be completed within fifteen working days.

For the purposes of this section, a day is not considered a “working day” if it is a LEAP excludable day as defined in IM Section 250.10. At their discretion, the ASAC, SAC, DAIGI, or AIGI may also determine that certain days are not to be counted as “working days” for timely reporting purposes. Such determinations shall be documented in the investigative tracking system and must be justified by extraordinary circumstances or mission requirements, such as an employee’s lack of computer/internet access, temporary duty (TDY) assignments, or competing time-sensitive mission priorities (e.g., court appearance, search warrant execution, etc).

430.14 Documentation of Quality Standards Benchmarks

The Quality Standards for Investigations and the Attorney General Guidelines require that certain benchmarks be met and documented in the development of an Investigation. These include timely consultation with prosecutors, notification of the FBI within 30 days of the opening of a criminal investigation, and periodic supervisory review.

Each of the following items must be documented in the investigative tracking system:

INITIAL CONTACT WITH FEDERAL PROSECUTOR. (Include additional details as appropriate, such as name of AUSA, outcome of contact, etc.)

FBI NOTIFICATION. (This benchmark is entered by the Investigations Support Group, and documents formal written notification of FBI headquarters by the OIG. Informal communication between assigned OIG staff and local FBI representatives shall be documented as case activity type ‘law enforcement coordination’.)

SUPERVISORY REVIEW. (Include additional details as appropriate. Supervisory case review should be conducted and documented in the ITS at least once per quarter for all open cases, including active, unassigned, and pending cases.)

440.00 Case Planning

When an investigation is assigned, the assignee should study the documentation and decide on an investigative plan of action, including what questions and issues will be addressed, and an action

plan for addressing them. The plan should be discussed with the appropriate SAC or ASAC and documented in the ITS.

While planning is essential for effective case management, investigative plans are not intended to serve as rigid checklists. They are, rather, guides which should be followed with professional discretion. If significant deviation from a plan becomes necessary as facts are developed, the necessary changes should be coordinated with and approved by the SAC or ASAC as appropriate.

440.10 Case Review

SACs or ASACs will arrange periodic case reviews with each special agent or investigative staff member within their area of responsibility, to insure timeliness, thoroughness, and quality of the investigative effort. (See IM 430.14) Cases assigned to SACs will be reviewed by the DAIGI. Cases assigned to staff in the Investigations Support Group and the Major Frauds group will be reviewed by their respective supervisors.

All investigative staff should document case activities in the ITS, for each case assigned, to record a chronological summary of activities from the opening of the case until the case is closed.

440.11 Case Disposition

When an agent has completed the investigation and written the final report, the completed case file should be forwarded to the SAC or ASAC for review. The SAC or ASAC will refer to the File Inspection check list to ensure that the case file is complete and approved for closure. The SAC or ASAC will then forward the approved and closed case file to ISG for quality control review and filing. For specific instructions on disposal of case related materials please refer to IM 1180.00.

450.00 Reports to OPM Management and the Congress

The Inspector General furnishes a variety of reports to OPM management and provides Semi-annual reports to Congress.

450.10 Reports to OPM Management

The IG provides periodic briefings and reports to advise the Director of OPM on OIG initiatives, and to highlight any problems which warrant management attention.

The IG will alert the Director of OPM as early as possible, consistent with requirements for confidentiality and the prosecutive system, to instances of waste or flagrant misconduct known to the OIG.

The IG will promptly report to the Director of OPM any attempts to impede an investigation, audit, or any other OIG activity. The IG will report to the Director of OPM whenever information or assistance requested is, in the judgment of the IG, unreasonably refused or not provided.

450.20 Reports to Congress

By law the OIG is mandated to provide a Semi-annual report to Congress. The Office of Investigations provides input and data concerning investigative activity for inclusion in the report. In addition, the OIG provides reports on request to the Government Accountability Office and other Federal agencies.

On occasion, a request for information or a report will be received from a congressional office. The OIG will make every effort to accommodate congressional requests for information on investigative matters that are within the oversight authority of Congress, while remaining faithful to the duty to protect confidential information.

When an inquiry from a Member of Congress is received in the OIG concerning investigative matters, a reply will be made within **one day**, acknowledging receipt of the inquiry. A full response will be prepared as soon as possible and may include interim updates.

Chapter 5

Investigative Policies and Procedures

500.00 Introduction

This chapter prescribes policies and procedures for conducting OIG investigations. These policies and procedures constitute internal OIG guidance. They do not create any legal rights (substantive or procedural) in any civil or criminal matter. They do not place limitations on otherwise lawful investigative or litigation prerogatives of the OIG.

500.10 Media Contacts and Press Releases

All news media inquiries and press coverage concerning Office of Personnel Management (OPM), Office of Inspector General (OIG), Office of Investigations (OI) complaints or investigations should be referred immediately to the OIG's Office of Legal Affairs. The OIG follows a "speak with one voice" policy when dealing with the news media. The Office of Legal Affairs, in coordination with the AIGI, will promptly respond to inquiries or requests for information from the media, and will consult with OPM's Office of Communications and Public Liaison, the Inspector General, and the Deputy Inspector General, when appropriate. In general, the news media response will recognize balancing the right of the public to be informed, an individual's right to a fair trial, and OIG's ability to further investigate matters of potential harm to the OPM. The media response will also abide by stringent confidentiality consideration to ongoing operations and investigations, OI investigative techniques, and Grand jury and tax matters. Consequently, the Office of Legal Affairs' response to media inquiries will most likely be to neither confirm nor deny ongoing investigative work.

Responsibilities and Requirements

If telephonically contacted by a member of the news media, investigative staff should respond that they are not authorized to give interviews, discuss work, or acknowledge that an investigation is being or has been conducted. Obtain the media contact's organization, name, title, telephone number, postal address, and electronic mail address. Once this information is obtained, refer the media contact to the OIG's Office of Legal Affairs. Immediately following the communication with the media contact, contact the Office of Legal Affairs and provide the details of the media inquiry.

If contacted by a member of the news media in writing or by email, do not respond. Instead, immediately forward the inquiry to the Office of Legal Affairs. The Office of Legal Affairs will respond to the media inquiry.

It is the responsibility of assigned investigative staff member to annotate the official investigative

record with the media inquiry, the Office of Legal Affairs' media response, and any additional action taken as a result of the media inquiry.

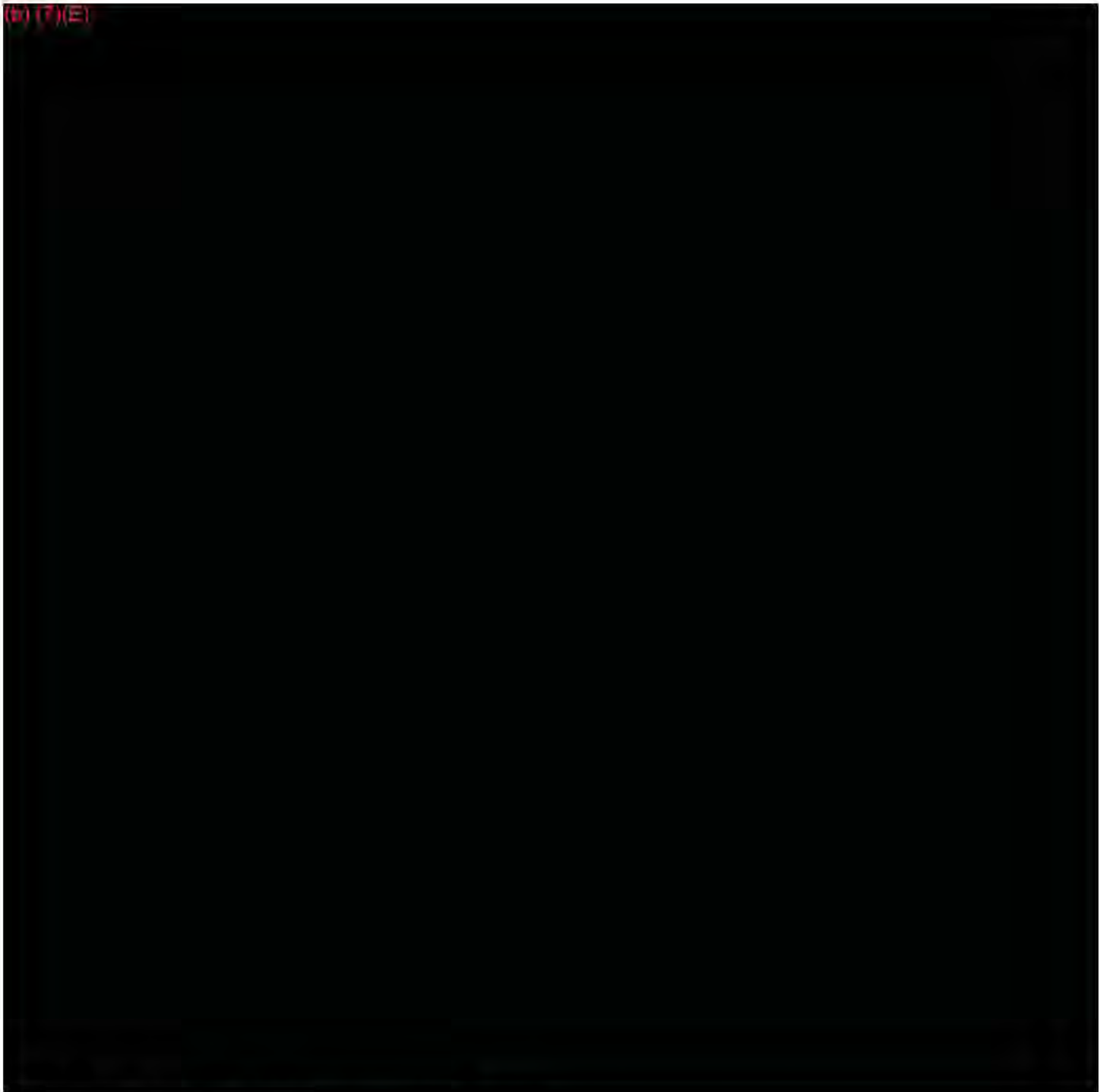
501.00 Sources of Information-Documentary Evidence

The primary function of an OIG special agent is to gather and report complete and accurate information regarding an investigation. Sources of information include statements from subjects of investigation, complainants, witnesses and informants, government officials, and others. In addition to information obtained through interviews, special agents must gather information and evidence from a variety of documentary sources. Documentary evidence, except for government records, may also be obtained by OIG subpoena. The types of information needed and the sources of information will vary from case to case. See **Appendix E** for a list of electronic databases to which the OIG has access.

501.10 OPM Sources of Documentary Information

(b) (7)(E)





502.00 Confidential Sources and Informants

This section contains policies and procedures for the establishment, management, and administrative control of confidential sources and confidential informants. The use of confidential sources and informants in law enforcement is a constitutionally acceptable method of gathering information. Subject to appropriate laws, regulations and OIG policy, special agents are encouraged to develop and use confidential informants.

502.11 Definitions

(b) (7)(E)
[Redacted text block]

[Redacted text block]

502.12 Policies

All agents will adhere to the (b) (7)(E)
[Redacted text]
Reference is also made to the (b) (7)(E)
[Redacted text], and the (b) (7)(E)
[Redacted text].

Agent-informant contacts will be handled in a strictly professional manner. (b) (7)(E)
[Redacted text]

(b) (7)(E)
[Redacted text]

(b) (7)(E)

502.13 Developing Confidential Informants

(b) (7)(E)

[Redacted text block containing multiple paragraphs of information, all obscured by black bars.]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

502.14 Payment of Confidential Informants

(b) (7)(E) [Redacted]

502.15 Reporting Violations of Criminal Law by Confidential Informants

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

(b) [REDACTED]

502.16 Protecting Identities of Confidential Informants

Protecting the identities of informants is essential. Agents will divulge the identities of informants only to authorized personnel. An informant should not be used as a witness, placed in a position where he or she might become a witness, or be identified in court without his or her permission. Agents should attempt to obtain evidence from other sources so that it is unnecessary to authorize persons to know an informant is involved in a case.

502.17 Confidential Informant Files

When an individual is designated as a confidential informant, the investigative tracking system will be used to assign a Confidential Informant (CI) number. The CI should only be identified in the investigative tracking system using the CI number and no personal identifying information will be maintained in the tracking system. (b) (7)(E), (b) (7)(F)

(b) (7)(F), (b) (7)(E) [REDACTED]

502.18 Referencing Confidential Informants in Reports

In all reports and memoranda of interview, the informants should only be referenced by their assigned control numbers. Generic wording should be used in the report without reference to race, sex, creed, or color.

Records of communication with informants are not attached to associated reports of investigation.

502.19 Protecting Confidential Informants' Identities in the Courts

If an agent is asked to disclose the identity of an informant on the witness stand, and no objection is made or sustained, the agent states that he cannot disclose the information on the grounds that it was a privileged communication to an officer of the Government (**Scher v. United States, 305 U.S. 251 (1938)**), and the agent is bound by instruction not to disclose such information. The agent maintains this position pending instructions from superiors and advice from the Assistant

U.S. Attorney. The agent's failure to disclose this information may lead to one of several possible results:

- The court may, if it thinks that no harm is done the defendant, uphold the agent;
- The court may dismiss the action;
- The agent's supervisors may release the agent from the confidentiality obligation; or
- If the agent persists in the refusal to answer, the court may find the agent in contempt.

It should be noted that information provided by confidential informants is confidential at the discretion of the government, unless such information is useful to vindicate the accused or lessen the risk of false testimony, or is essential to the proper disposition of the case (*Rugendorf v. United States* 376 U.S. 528 (1968), and *Roviaro v. United States* 353 U.S. 53 (1957)). The privilege concerns only the identity of the informant, not the information supplied by the informant. The government may waive the privilege, for example by voluntarily disclosing the informant's identity to persons who would "resent" his communication (*Mitchell v. Bass*, 252 F. 2d 513 (8th Cir. 1958)), or by calling him as a witness at trial.

503.00 Subpoenas

The IG Act empowers the OIG to obtain by subpoena all information, documents, reports, records, accounts, papers, and other data and documentary evidence necessary to perform functions assigned the OIG by the IG Act.

Generally, this subpoena power applies to four basic categories of records.

1. **Business records:** The IG Act enables the OIG to require production of any business record, even those that are not normally made available under the audit clause of a contract. Furthermore, records may be obtained from a business, subcontractor, or others who may not be subject to the audit clause of a particular contract.
2. **Personal records:** An individual can be required to produce records in his or her personal possession, including tax returns, bank statements, and employment records. For example, personal records of a corporate officer can be obtained, in addition to business records of the corporation.
3. **Financial Institution records:** Banks, saving institutions, credit unions, loan companies, and credit card companies can be required to produce their records and those of their customers. In many situations, however, the Right to Financial Privacy Act of 1978 is applicable.

Generally, the Act requires that specific advance notice of the subpoena be provided to an individual (non-corporate) customer. The notification requirements must be strictly observed in subpoenaing an individual's records from financial institutions. Delayed notification provisions are available in emergency situations to prevent the destruction of evidence or flight from prosecution. The requirements of this Act make it especially important that such cases be closely coordinated with the Counsel to the IG.

4. **Government records:** A State, municipal, or quasi-governmental body or agency can be required to produce relevant documents. The OIG subpoena power is not available to obtain records and information from other Federal agencies.

IG subpoenas are not subject to the automatic stay provisions of the Bankruptcy Code and, therefore, may be issued and enforced after a debtor petitions for bankruptcy. The issuance of an Inspector General's subpoena is exempt from the stay because it constitutes the commencement or continuation of an action or proceeding by a governmental unit to enforce such governmental unit's police or regulatory power. Investigative staff should work closely with Counsel when preparing subpoenas in bankruptcy cases.

503.10 Responsibility in OIG for Processing Subpoenas

The AIGI serves as the focal point for all matters relating to the use and issuance of OIG subpoenas. All requests for subpoenas must be processed in accordance with procedures set forth below and must be reviewed and approved by the AIGI and Counsel to the IG prior to being forwarded to the IG.

503.11 Policy on Use of Subpoenas

A subpoena should be used only after other available means of obtaining the information have been exhausted. When a document or record is available under the audit clause of a contract, or if an individual has a contractual obligation to provide certain documents, attempts are first made to obtain the documents by reference to such authority. Similarly, **the Inspector General Act, §6(a)(1)** requires OPM employees to furnish agency material and material available to the agency upon request. However, investigative staff should be aware of the ability to obtain through subpoena power information withheld despite disclosure obligations, or information that will augment, clarify, or amplify documents already obtained.

In situations where a subpoena must be used to obtain documents that should have been provided because of contractual or employment obligations, the AIGI and the Counsel to the IG may consider referral for appropriate contract or personnel action.

Normally a subpoena is not requested until information obtainable by other means has been

examined and evaluated. This enables investigative staff to more specifically define those documents that are needed. Furthermore, if the receiving party files a motion to quash the subpoena, the OIG will be able to demonstrate that the information cannot be obtained through normal procedures. However, a number of circumstances could justify the issuance of a subpoena at an earlier stage of the investigation. These circumstances include the immediate need to obtain documents to prevent their loss, alteration, or destruction. In complex investigations, numerous subpoenas may be issued, as needed, at various stages of the investigation, in order to fully develop the case.

Investigative staff should consult with their supervisors, the AIGI and the Counsel to the IG as early as possible when considering use of a subpoena. Such early discussion can help significantly in determining the appropriateness of a subpoena, considering alternative means of acquiring needed materials, and in framing and processing the subpoena request and subpoena itself.

503.12 Procedures for Requesting Subpoenas

Whenever documentary information or records needed in connection with an official OIG investigation are not otherwise provided, a subpoena request may be considered. Subpoena requests are in the form of a memorandum to the Inspector General, through the AIGI, and contain the following information:

1. **Background of Subject Matter Under Investigation**
A subpoena request must set forth a concise history of the investigation to date. It includes the authority for the investigation, an identification of the contracts or records and individuals involved, the ultimate goal of the investigation, and identification of all known agencies that may be conducting a similar or joint investigation.
2. **Description of Items**
A subpoena request must describe as precisely as possible those items that are to be obtained by the subpoena. While individual documents need not be identified, documents should be divided into certain categories, e.g., payroll records, payment invoices, bank statements, or income tax returns, and identified as completely as possible by date and party. In some cases, certain individual documents should be identified.

In consultation with the Counsel to the IG, consideration should be given to use of the phrase "including but not limited to..." to assure that both specific known documents and other relevant materials that may not be individually known or identifiable are obtained. If appropriate, the document categories are cross-referenced to a particular contract or record. Investigative staff should remember that a subpoena request need not be all inclusive. If subsequent investigation determines that other documents are needed or that other parties are involved, additional subpoenas may be issued.

3. Justification for Subpoena Request

The subpoena request must explain why the documents cannot be obtained by other means. Any lack of cooperation by the party under investigation or the holder of the records is discussed. The request specifies the particular investigative goals that will be furthered by the subpoena. In requiring the production of documents and information by subpoena, the OIG is not required to determine that there is probable cause to believe that a violation of criminal or civil statute or administrative regulations has been committed, and that the materials sought constitute evidence of such violation. The OIG needs to determine that the items sought are reasonably necessary to further proper OIG investigative activities.

4. Time and Place for Return of Service

The requestor should establish a date, time, method of delivery, and a location for the return of service. Where return of service at OPM is impractical, arrangements may be made to allow return at another appropriate Federal facility. In some circumstances, arrangements may be made to allow a return on the premises of the subpoena recipient.

503.13 Approval and Processing of Subpoenas

When a special agent, or investigative staff member determines that issuance of a subpoena is appropriate, they will prepare necessary subpoena documentation, attachments, and appendices describing the documents sought, and submit them in the ITS and use the fillable form to complete the subpoena memorandum to the IG, through the AIGI.

Subpoena requests (**Figure 500-01** and **Figure 500-02**) will be submitted in the ITS and reviewed by the appropriate SAC or ASAC, then forwarded in the ITS to the AIGI for approval. The request will then be reviewed by the OIG Office of Legal Affairs (OLA) for a determination of completeness, legality, and validity. The AIGI or OLA may require investigative staff to provide further clarification or material in support of the request, or identify additional areas of investigation that should be undertaken before a subpoena is justified.

Upon approval for legal sufficiency by OLA, subpoenas will be forwarded for approval of the Deputy IG, then forwarded to the Investigations Support group for preparation of hardcopy subpoena documents for the IG's signature.

503.14 Service of Subpoenas

Counsel, in conjunction with the requesting investigative staff member, selects a due date for compliance with the subpoena. In most cases, the date is at least 10 calendar days after the date of service. The counsel and investigative staff member determine whether the subpoena should be served personally at the corporate location or private dwelling, or sent by registered or certified mail. See **Figure 500-01** for a sample subpoena to a non-banking organization.

If service is executed by mail, the subpoena is mailed with Attachment A to the parties concerned. If personal service is chosen, the subpoena is given to the requestor to serve. The subpoena, with Attachment A, is then delivered to the addressee as expeditiously as possible.

Personal service upon a corporation is made during business hours and to the addressee. If the addressee is unavailable, a corporate officer or registered agent for service of process will suffice. If an individual other than the addressee receives the subpoena, the server obtains the recipient's signature, and then executes the remaining portions of the Certificate of Return of Service, and places it in the case file.

Cases in which the subpoenaed party seeks modifications to the subpoena, or in which the subpoenaed party is represented by counsel, are referred through the Counsel to the IG. In all cases involving a subpoena, close coordination and consultation between the requestor and Counsel are maintained. Modifications in the scope and location of return of the subpoena may be accomplished by mutual agreement between the recipient and the OIG. Prior to the date of return, the requestor may be asked to examine the documents on the premises of the recipient to verify the existence and volume of the documents sought.

503.15 Return Proceedings

The recipient of a subpoena is required to provide the requested documents on the date and time specified. The requestor should be prepared to receive the documents on the specified date and time, and have adequate personnel resources available to begin complete examination. While no precise time limits can be set for the completion of the examination of the records, the requestor will examine and analyze all records as expeditiously as possible.

Original documents are normally obtained unless the respondent can effectively demonstrate that the absence of the original documents will act as a major impediment to the operation of his or her business. In such cases, the requestor agent may accept certified copies in lieu of originals. However, the original records must be made available for verification if required by the special agent. Any questions should be referred to counsel.

A subpoena log will be maintained in the investigative tracking system for each subpoena issued. The case agent is responsible for completing the "Return" portion of the subpoena log upon receipt of the requested documents.

503.16 Handling of Subpoenaed Documents

At the outset of any examination of the documents, it may be difficult to determine which if any, of the documents will be used as evidence in a resulting civil, criminal, or administrative proceeding. Therefore, investigative staff must be aware of the need to maintain a chain of

custody for any original documents obtained through administrative subpoena. See IM Chapter 13 for guidance on the collection, preservation, and safeguarding of evidence.

Upon receipt of subpoenaed materials, Investigative staff will examine each record and determine which records are to be retained for later use, and which records may be returned to the respondent. Any record that may serve as evidence in a resulting civil, criminal, or administrative proceeding is retained until all proceedings have been exhausted. Records not needed for potential use in such proceedings will be returned to the respondent. A receipt will be obtained for all documents returned to the respondent.

503.17 Failure to Comply

When a subpoenaed party refuses to comply, fails to appear, or fails to provide documents as required by a subpoena, the requestor will inform the AIGI and Counsel to the IG immediately. Counsel is responsible for resolving such cases and for initiating subpoena enforcement actions where necessary through the appropriate United States Attorney.

503.18 Subpoena to Financial Institutions

Subpoenas requiring a financial institution to produce its customers' financial records must be processed in accordance with provisions of the Right to Financial Privacy Act of 1978, 12 U.S.C. 3401-3422, which generally requires prior or contemporaneous written notice to the customer that his or her financial records have been subpoenaed, so that the customer has an opportunity to challenge the subpoena in court (**Figure 500-02**).

The Act applies when the customer is an individual or a partnership of five or fewer individuals. It does not apply when the customer is a corporation, business trust, or partnership of six or more individuals. It also does not apply if the customers are deceased.

Because of the burdens imposed by this Act and the sanctions that may be levied for violations, investigative staff must fully document the precise nature of the business entity involved when requesting a subpoena for financial records from a financial institution. Examine appropriate public records, contracts, and other documents to confirm a business entity's status as a corporation, proprietorship, general or limited partnership, or joint venture.

When it becomes apparent that a subpoena is or may be needed for a financial institution, consult with the Counsel to the IG for guidance. There are a number of legal issues concerning advance customer authorization, notice requirements, and special limitations and requirements on transfers of records which the requestor must consider.

503.19 Reimbursement to Financial Institutions for Cost Incurred

The OIG is required to reimburse financial institutions for costs incurred in gathering, reproducing, and transporting financial records subpoenaed under the Act. The reimbursement is set at rates and conditions established by the Board of Governors of the Federal Reserve System and are outlined in 12 CFR Part 219. Photographs, films, and other materials are reimbursed at actual cost.

504.00 Search Warrants

Section 6(e) of the Inspector General Act of 1978, as amended in 2002, grants statutory law enforcement authority to OPM OIG special agents, including the authority to obtain or execute search warrants. Special agents will consult with their SAC and appropriate federal prosecutors when use of a search warrant is considered. All search warrants require an approved Operations plan by an OI SAC or other participating law enforcement agency.

504.10 Safe Execution of Search Warrants

The safety of the participating law enforcement officers and other individuals present during search warrants is paramount. Due planning and care during search warrants is required to ensure safe execution.

504.20 Handling of Seized Evidence

When the OPM OIG is taking custody of evidence seized during the execution of a search warrant, the evidence handling procedures described in IM Chapter 13 will be followed, and a receipt and inventory will be furnished to the owner of the seized property.

When the OPM OIG is a participant in the execution of a search warrant, but another law enforcement agency will be taking custody of the evidence, the evidence procedures of that agency will be followed.

504.30 Seized Firearms

(b) (7) (E)





505.00 Warnings and Rights

Special agents should exercise care to protect the rights and privacy of those involved in OIG investigations. OIG OI follows the current DOJ and legal guidelines regarding the advisement of 5th Amendment rights in criminal and administrative investigations. It is impossible to articulate and explain every circumstance and condition in which the advisement of rights is necessary. However, the following chart provides general guidelines:

Situation	Minimum Requirement
Suspect is under arrest	Full Miranda rights required
Suspect is in custody	Full Miranda rights required
Suspect is not in custody but is the “target” of a criminal investigation	Consult with the AUSA, prosecutors vary on this, generally, you may ask questions without Miranda.
Suspect is not in custody and is not OPM employee/contractor	No rights required
Suspect is not in custody and is an OPM employee/contractor in a possible criminal matter	Garrity warning may be required
Suspect is an OPM employee, and the AUSA has	Kalkines warning may be required

declined prosecution in favor of administrative action	
Witnesses who could be implicated in misconduct	No warnings required

505.10 Warnings and Rights during Custodial Criminal Investigation Interviews

A custodial interview occurs when the person being interviewed has been taken into custody or otherwise legally deprived of freedom of action. The special agent will give a Miranda Warning (**Figure 500-04**) in all custodial interviews, even if the arrest or incarceration resulted from a matter totally unrelated to the investigation.

505.11 Warnings and Assurances During Administrative Interviews

Federal employees may be compelled to answer questions regarding their job-related conduct, or face dismissal for failure to cooperate with an administrative investigation. However, if the employee also faces potential criminal liability, compelling them to answer questions during an interview violates their Fifth Amendment rights concerning self-incrimination.

There are two different administrative warnings, Garrity Warnings and Kalkines Warnings. Whenever it is necessary to interview a federal employee who is obligated to cooperate with the investigation, the agent or investigative staff member must consider how any statements obtained may be used, and use the appropriate administrative warning.

A Garrity Warning must be given prior to questioning, if the statements might be used to support criminal charges against the employee. The Garrity Warning protects the employee's Fifth Amendment rights. The Garrity Warning advises the employee that the interview is voluntary, that they do not have to answer questions, that no disciplinary action will be taken against them for refusing to answer questions, and that their statements could be used as evidence in future criminal or administrative proceedings.

A Kalkines Warning is appropriate if the employee's statements will only be used to determine whether administrative discipline is appropriate, and there is no foreseeable criminal culpability on the part of the employee. A Kalkines Warning grants use immunity, and neither the statement obtained nor the fruits thereof may be used in any criminal proceeding against the employee. Once employees are on notice that their statements cannot be used against them criminally, they have no valid Fifth Amendment privilege to invoke. Therefore, a Kalkines Warning forces employees to answer questions related to their job-related conduct, or face potential disciplinary action, up to and including termination. Since Kalkines Warnings grant use immunity, agents must be very cautious in their use. Before giving a Kalkines Warning in any instance where the allegation, if true, would have potential for prosecution of the employee interviewed, the special agent must obtain a decision from an Assistant U.S. Attorney on whether the matter should be handled administratively rather than criminally.

See **Figure 500-05** for the Garrity Warning Form and **Figure 500-06** for the Kalkines Warning Form.

506.00 Affidavits and Statements

During the course of an investigation, affidavits or written statements may be obtained from the subject of the investigation and any witnesses to the matter under investigation. The subject's affidavit or statement places admissions and statements made during the course of an interview in a written form, in the subject's own words, and under the subject's own signature. Similarly, an affidavit or statement provides a personal account that can serve to refresh recollections and dissuade a witness from changing testimony later.

The decision to take an affidavit or statement from a subject or witness depends on the nature of the investigation and the judgment of the special agent and OIG management. It should be discussed between the special agent and the SAC or ASAC during the planning phase of the investigation.

506.10 Guidelines for Preparing Affidavits

The affidavit may be prepared in narrative or question and answer format (**Figure 500-07**). It will reflect the words of the affiant and will be limited to comments directly bearing on the topic of the investigation.

When securing an affidavit in a case that may be referred for prosecution, it is particularly important to avoid inclusion of prejudicial or extraneous comments. It should set forth any defense, explanation, or other exculpatory statement furnished by a subject of a case.

When the affidavit is hand written it is preferable to have the affiant write it. If the special agent writes the affidavit, the affiant must read the full contents of the affidavit before signing it. If the affiant declines to read the affidavit, the special agent reads it to him or her. If the affiant is not literate or unable to read the affidavit because of a handicap, the special agent will 1) read the affidavit to him or her in the presence of a witness, and 2) note the affiant's inability to read on the last page of the affidavit.

Whether typed or hand written, corrections should be made in the affiant's own handwriting, initialed and dated in the margin alongside or above the correction. These corrections provide support that the affiant read and understood the statement.

The special agent administers an oath or affirmation, then the affiant initials the bottom of each page and signs the affidavit. The special agent completes the affidavit and provides the affiant a copy on request.

506.11 Authority to Administer Oath

Special agents are authorized under 5 U.S.C. 303(a) to administer oaths and affirmations to witnesses and subjects of investigations.

507.00 Interviews

Interviewing subjects and witnesses is one of the primary tools available to investigators for gathering information. Interviews should be conducted by two special agents or investigative staff members whenever possible. Interviews should also be conducted in private, away from the presence and hearing of others, to enable the interviewee to be frank and open, and to limit the risk of compromising the investigation through unauthorized disclosure of information.

The purpose of an interview is to collect information relevant to an investigation. Under no circumstances should legal advice be provided by the interviewer and no attempt should be made to answer a legal question.

507.10 Memorandum of Interview

A memorandum of interview (MOI) will be used to document interviews of subjects or witnesses. The memorandum should include the time and place of the interview, a list of all individuals present, and a discussion of the interviewee's statements and answers to questions asked. It does not have to be an exact transcript of the interview, but must be an accurate description of the topics discussed. An MOI is considered by the OIG to be an extension of the investigator's notes. The MOI should be added into the investigative tracking system within five working days of the interview, and must be reviewed and approved by an ASAC or SAC.

The MOI should contain the remarks of the interviewee, but it should not contain an analysis of his or her comments. The memorandum will be used to prepare a Report of Investigation or an Affidavit, should one become necessary at a later date. See IM 1170 for further instructions regarding the format and writing style for MOIs.

507.11 Preparation for Interview

(b) (7)(E)


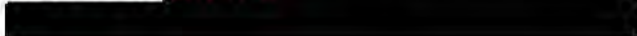


(b) (7)(E)



507.12 Time and Place of Interview

Common sense and good judgment should be used in scheduling the times and locations for interviews. (b) (7)(E)

(b) (7)(E)



507.13 Voluntary Response

(b) (7)(E)




507.14 Interview of Minors

(b) (7)(E)

A large rectangular area of the document is completely redacted with black ink, covering approximately three lines of text.


507.15 Interview of Members of the Opposite Gender

(b) (7)(E)

A single line of text is redacted with black ink.

507.16 Interview of Hostile Individuals

(b) (7)(E)

A large rectangular area of the document is completely redacted with black ink, covering approximately three lines of text.

507.17 Union Representation During Interviews

The Civil Service Reform Act of 1978 (5 U.S.C. 7114) states, in part: "An exclusive representative of an appropriate unit in an agency shall be given the opportunity to be represented at ... any examination of an employee in the unit by a representative of the agency in connection with an investigation if the employee reasonably believes the examination may result in disciplinary action against the employee; and the employee requests such representation."

Most employees of OPM are represented by a labor organization (American Federation of Government Employees, Local 32). However, supervisors, management officials, OIG employees and other categories are normally excluded from bargaining units, thus not entitled to union representation.

While the collective bargaining agreement with the American Federation of Government Employees, affecting OPM Central Office employees, does not require that an employee be advised of his or her right to union representation at an interview, some labor contracts do. Prior to interviewing employees who are stationed in OPM regional or field offices, special agents

should determine if a labor contract provision is in effect that requires the agent to notify the employee of his or her right to union representation. If an OIG agent is going to be on travel status in order to conduct the employee interview, any arrangements for union representation should be finalized prior to the agents' departure.

OPM employees who are covered by the bargaining unit are entitled to union representation in administrative matters. However, if an OPM employee agrees to speak with OIG agents regarding a criminal matter, union representation is NOT permitted. Union Representatives are not qualified to give advice in criminal matters. (b) (7)(E)

OPM Supervisors and other employees not covered by the bargaining unit are (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

A copy of the OIG report will be forwarded to the deciding official as well as OPM Human Resources.

507.18 Confidentiality During Investigative Interviews

(b) (7)(E) [Redacted]
[Redacted]
[Redacted] (b) (7)(E)
[Redacted] (See IM 310.11).

508.00 Special Investigative Procedures

Special investigative procedures such as a polygraph examination, surveillance, or other techniques may be used in an investigation when appropriate to the circumstances and the objectives.

508.10 Polygraph Examinations

(b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

508.11 Requesting Polygraph Examinations

To request a polygraph the special agent submits a written request to the SAC. The request includes the case number, case title, and a brief explanation of the purpose of the polygraph examination, including the name of the person to be examined.

If the SAC concurs with the request, arrangements are made for a polygraph through another federal law enforcement agency.

508.20 Surveillance

Surveillance requests must be submitted in writing to the SAC, and approved by the AIGI. Surveillance decisions, including assignment of agents, methods, and documentation, are made by the AIGI in accordance with applicable laws.

A spot surveillance or drive-by surveillance may be conducted to verify such things as the subject's going to or from work, or to verify a place of business, and may be conducted on the special agent's own initiative without written approval.

A physical surveillance is an investigative technique consisting of the discreet observation of persons, vehicles, places, or objects to obtain information about activities, operations, and contacts. It is conducted in public areas so not to give rise to the question of trespass or invasion of privacy.

Items such as binoculars or telephoto cameras may be used to enhance observation. Photographs and videotapes of the subject during the surveillance are acceptable legal evidence of the activities, operations, or contacts observed.

508.21 Electronic and Video Surveillance

Electronic surveillance includes interception of wire, oral, and electronic communications; tracking the movement of vehicles or other objects; the tracing of telephone calls and electronic communications. This section also addresses video-only surveillance.

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title 18 U.S.C. 2510 et seq. prohibits the warrantless, non-consensual interception of wire or electronic communications, and also prohibits using a device to intercept oral communications where there is a reasonable expectation of privacy and none of the participants in the oral communications has consented to monitoring. Such intercepts may be lawfully done only with a Title III Court Order.
- Exemptions to the requirement for a Title III Court Order include: 1) where there is no reasonable expectation of privacy in an oral communication; and 2) where at least one party to the conversation has given consent to interception of the communication (also known as consensual monitoring). See IM 508.30 through 508.34 for information on consensual monitoring.
- A Title III Court Order is not required to intercept the following types of electronic communications: (b) (7)(E)

See IM 508.22 for information on the use or electronic tracking

devices.

(b) (7)(E)

However, Federal courts are currently divided on the type of court order required. Therefore, consultation with a local AUSA is required to determine the appropriate type of court order needed in order to track a cellular telephone in the relevant judicial district.

508.22 Electronic Tracking Devices

Title 18 U.S.C. §3117 discusses the use of “electronic or mechanical device(s) which permit the tracking of the movement of a person or object.” The most commonly used tracking devices are beepers, transponders, and GPS devices. The Fourth Amendment, not Title III, regulates the installation and monitoring of electronic tracking devices. If a reasonable expectation of privacy is implicated in *either* the installation or the monitoring, a warrant (or an exception, such as consent) is required. Prior to using any electronic tracking device, the special agent must consult with an AUSA and obtain the written approval of the DAIGI or AIGI.

508.23 Pen Registers and Trap and Trace Devices

(b) (7)(E)

508.24 Video-Only Surveillance

In all circumstances, video-only surveillance requires the written approval of the AIGI or DAIGI.

Using video-only surveillance to record activity in an area where a reasonable expectation of privacy exists is governed by the Fourth Amendment. If there is a reasonable expectation of privacy, either a search warrant or consent is required. This includes the installation of cameras in public areas, where the camera is positioned to record activities occurring on the target’s curtilage or other private place. Agents must consult with an AUSA regarding the preparation of search warrant affidavits for video-only surveillance, as the requirements may vary by judicial district. Agents are also reminded that in some circumstances it is possible for a reasonable expectation of privacy to be established within a Government-owned workspace.

If the video camera is installed in a public area, and monitors only activities in a location where no reasonable expectation of privacy exists, no search warrant is required. Agents should consult with an AUSA regarding whether there is a reasonable expectation of privacy in the location where the camera is installed, and in the area to be monitored.

508.25 Stored Electronic Communications

The Stored Communications Act (SCA), found at 18 U.S.C. §§ 2701-12 controls government access to electronic communications stored by publicly accessible internet service providers (ISP). There are three types of information stored by ISPs which may be relevant to investigations: 1) basic subscriber information; 2) transactional records; and 3) the contents of stored communications.

- A subpoena is required to obtain basic subscriber information. Basic subscriber information includes the name; address; local and long distance telephone connection records, or records of session times and durations, length of service; types of services utilized; telephone or instrument number, or other subscriber number or identity, to include temporarily assigned network addresses, and the means and source of payment of a subscriber or customer of the ISP service.
- A court order is required for transactional records. Transactional records include historical data on past activity on the ISP account, such as web sites visited, cell-site data for cellular telephone calls, or email addresses of those with whom the account holder corresponded.

The actual contents of wire or electronic communications held in storage by the ISP may require a search warrant, a court order, or a subpoena, depending on the time and retrieval status. Agents should consult with an AUSA to ensure the appropriate legal method is used.

508.30 Consensual Monitoring

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title 18 U.S.C. 2510 *et. seq.*), as amended, permits government agents, acting with the consent of a party to a communication, to engage in warrantless monitoring of wire (telephone) and oral, non-wire communications. Similarly, the Constitution and federal statutes permit federal agents to engage in warrantless monitoring of oral, non-wire communications when the communicating parties have no justifiable expectation of privacy. While these techniques are lawful and helpful, their use in investigations is frequently sensitive, so they must remain the subject of careful, self-regulation by the agencies employing them.

Special agents are required to first obtain approval from the local AUSA and subsequently secure the express consent of the AIGI prior to any monitoring activity. Authorization will be requested through the SAC via memorandum. In urgent situations, the SAC may seek approval by telephone.

508.31 Request for Approval of Consensual Monitoring

The request for approval of consensual telephone monitoring and the authorization to use electronic equipment for consensual monitoring will be submitted through the SAC to the AIGI with the following information:

1. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

b(7)(E)

Requests for extensions or renewals should be submitted in the same manner as the original request.

[REDACTED]

508.32 Execution of the Consensual Monitoring

1. A signed consent will be obtained from the consenting party prior to the special agent engaging in consensual telephone monitoring.
2. Records generated by consensual monitoring must be incorporated into the relevant investigation file.
3. After completion of each monitoring period, the special agent will complete a Consensual

Monitoring Report detailing the names of all individuals involved, dates monitored, time, location, and a summary of information obtained pertinent to the investigation. This report must be added to the investigative tracking system, where it shall be reviewed and approved by the supervisor.

508.33 Obtaining Monitoring Equipment

SACs may make arrangements to obtain the necessary equipment from OPM-OIG headquarters, or, when needed on a loan basis from local, state, and Federal agencies. Issued or borrowed equipment is to be secured and safeguarded to prevent unauthorized access or use.

508.34 Safeguarding Materials

All recordings and records of information obtained through interception activities, to include consensual monitoring, as well as video or electronic surveillance, shall be safeguarded to preclude unauthorized access, theft, or use. Both the interest of the Government and the rights of private individuals involved shall be considered in the development of safeguarding procedures.

Records and recordings of interceptions shall be retained as appropriate in accordance with the policies and procedures outlined for maintaining evidence.

SACs will ensure that an inventory of all monitoring equipment and its location is conducted annually, if applicable.

509.00 Undercover Techniques

The OI may use undercover techniques, or participate in joint undercover activities or operations with other law enforcement agencies, as appropriate to carry out its law enforcement responsibilities. However, undercover techniques inherently involve an element of deception and may require cooperation with persons whose motivation and conduct are open to question, and so should be carefully considered and monitored. The objective in utilizing undercover techniques is to obtain needed evidence against suspected criminals; and/or to advance an investigation or preliminary inquiry to higher or wider scale; and, to reduce time and expenses involved in the completion of an investigation.

(b) (7)(E)
[Redacted]

[Redacted]

(b) (7)(E)

509.01 Definitions of Undercover Terms

“Undercover Activity” - any investigative activity involving the use of an assumed name or cover identity by an OI employee or another Federal, state, or local law enforcement organization working with the OIG. (b) (7)(E)

(b) (7)(E) For the purposes of this section, the following investigative procedures are not considered undercover activities: placing pretext telephone calls; and, using a temporary cover while on surveillance.

“Undercover Operation” - a series of related undercover activities over a period of time. A “series of related undercover activities” generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. (b) (7)(E)

(b) (7)(E)

Sensitive Circumstances are fully defined in the *CIGIE Guidelines* (See **Appendix I**). Examples of Sensitive Circumstances include investigations involving the following: certain public officials; religious, political, or news organizations; a significant risk of violence; authorized criminal activity on the part of the undercover operative; operation of a proprietary business; requests to certain individuals, such as attorneys or physicians, for information that would ordinarily be privileged; and, the risk for significant civil liability.

509.10 Authorization to use Undercover Techniques

Under no circumstances will special agents (SA) engage in undercover activities or operations without proper authorization. SAs must submit a written request in a memorandum format prior to utilizing any undercover technique. A copy of the request memorandum, bearing the signature(s) of the proper level of authority, if approved, must be maintained in the case file.

When exigent circumstances exist, approval may be obtained verbally and a written request submitted as soon as possible, but not later than three working days. “Exigent circumstances” are those where there is a potential threat to life or of bodily injury, or where failure to act could mean the destruction of essential evidence or the escape of a fleeing offender.

509.11 Undercover Memoranda of Request, OPM/OIG Lead Agency

When the OPM/OIG is the lead agency for the proposed undercover activity or operation, the memorandum requesting approval must include the following information set forth in the *CIGIE Guidelines* (See **Appendix J** for more detail and referenced sections or subparts):

1. APPLICATION/PROPOSAL TO THE UNDERCOVER REVIEW COMMITTEE

- a. Application for any undercover operation shall include:
 - i. A description of the proposed operation and the particular identity cover to be employed; any informants or other cooperating persons who will assist in the operation including background information, arrest record, and plea agreements; the particular offense or criminal enterprise under investigation; and any individuals known to be involved;
 - ii. A statement of the period of time for which the operation would be maintained;
 - iii. A description of how the requirements concerning any inducements to be offered as discussed in Section V, Subpart B below have been met;
- b. Applications for approval of undercover operations involving sensitive circumstances listed in Section IV, Subpart B shall also include the following information:
 - i. A statement of which circumstances are reasonably expected to occur, what the facts are likely to be, and why the undercover operation merits approval in light of the circumstances, including:
 - a) For undercover operations involving sensitive circumstance, a statement why the participation in otherwise illegal activity is justified under the requirements of Section IV, Subsection H; and 1
 - b) For undercover operations involving sensitive circumstance (I), a statement why the infiltration or recruitment is necessary, a description of procedures to minimize any acquisition, retention, and dissemination of, information that does not relate to the matter under investigation or other authorized investigative activity, and an explanation of how any potential constitutional concerns and any other legal concerns have been addressed.
- c. A letter from the appropriate prosecutor indicating that he or she has reviewed the

proposed operation, including the sensitive circumstances reasonably expected to occur, agrees with the proposal and its legality, and would anticipate prosecuting any meritorious case that is developed. The letter should include a finding that the proposed investigation would be an appropriate use of the undercover technique and that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm.

In addition to the *CIGIE Guidelines* please include the following information:

1. An indication of whether the undercover would be conducted jointly with another law enforcement agency, and the contributions each agency would make.
2. A description of any technical equipment, such as monitoring or recording devices, which would be used.
3. A statement of proposed expenses, including any anticipated charges to OPM-administered programs.
4. An evaluation of the risk to the undercover operative, including risk management/contingency plans.
5. Signature lines for recording the necessary approvals.

509.12 Undercover Memoranda of Request, Other Agency Lead

A memorandum requesting approval with signature lines for recording the necessary approvals is also required (b) (7)(E)

It is permissible for the OIG memorandum requesting approval to take the form of a cover document referencing an attached copy of the lead agency's undercover approval documentation, provided that the combination of the memorandum and its attachment(s) address all of the items detailed in the section above.

509.13 Task Force Assistance

An SA may, as a member of a joint Task Force, help another law enforcement agency monitor or provide physical security for that agency's approved undercover activity/operation. The formal approval process described in this section is not required in such circumstances, provided that the SA is not in an undercover role, no OPM-administered program is affected by the other agency's

undercover activity/operation, and the other agency's undercover activity/operation has been properly approved under the other agency's policies.

509.14 Scope and Duration

An approved undercover activity or operation may not continue longer than necessary to achieve the objectives or beyond the time frame/number of encounters initially specified, without further authorization. An application for the extension or renewal of an undercover operation should describe the results obtained from the operation or explain any failure to obtain significant results and, where sensitive circumstances are involved, should include a letter from the appropriate prosecutor favoring the extension or renewal of authority.

509.20 Approval Authority for Undercover Techniques

(b) (7)(E) [Redacted]

- [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

509.30 FBI Notification

Prior to conducting any undercover operation lasting longer than six months, or involving any of

the sensitive circumstances set forth in the FBI Undercover Guidelines, the OPM/OIG must first notify the FBI. If the FBI opts to join the case, the undercover operation will be subject to review by the Criminal Undercover Operations Review Committee of the FBI. If the FBI opts not to join the case, the undercover operation will be reviewed by the CIGIE's Undercover Review Committee. No undercover operation involving Sensitive Circumstances may be conducted without the approval of one of these committees.

509.40 Coordination with Prosecutors

Upon initiating and throughout the course of any undercover activity/operation, the SA shall consult on a continuing basis with the appropriate Federal or State prosecutor, particularly with respect to the propriety of the operation and the legal sufficiency and quality of evidence that is being produced by the activity.

509.50 Conduct of Undercover Activities/Operations

(b) (7)(E)



509.60 Considerations in Health Care Fraud Undercover Operations

(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



510.00 Investigative Equipment

All investigative equipment will be inventoried, such as cell phones, firearms, handcuffs, badges, commission books, etc. Investigative equipment issued to personnel will be inventoried in the investigative tracking system. Equipment returned to the property officer will also be described with the employee documenting and dating the return in the investigative tracking system. The property officer (in Washington, D.C.) and/or assigned supervisors will inventory issued and non-issued equipment annually and prepare a memorandum to the AIGI certifying the results of the inventory.

511.00 Use of Email for Case Related Communication

The OIG is required to retain and, in certain circumstances, produce in discovery substantive emails between OIG staff, between OIG staff and prosecutors and between OIG staff and victim/witnesses. Moreover, emails sent to others, particularly to multiple recipients, may be inadvertently or intentionally disseminated outside the office. Although email is a valuable, time-saving and effective tool that can make communication faster and more convenient, it may have significant, possibly adverse, consequences if not used thoughtfully. Moreover, the use of email to communicate substantive case-related information in criminal and parallel criminal/civil cases may trigger our responsibilities under the Jencks Act, Federal Rules of Criminal Procedure Rules 16 and 26.2, *Brady v. Maryland* and *Giglio v. United States*, United States Attorney's Manual 9-5.001 (issued October 19, 2006), and the Federal Records Act (44 U.S.C. 3301, and 36 CFR 1234.2).

OI employees must be circumspect and professional in email communications. Professional investigative organizations must gather and report evidence in an unbiased, impartial, and independent manner. Case related emails must reflect that standard, and be written with the same level of due professional care as other written work product.

OI employees should avoid using email to communicate substantive case-related information in criminal and parallel criminal/civil cases whenever possible. Because email communications may not be as complete as investigative reports, and may have the unintended effect of circumventing

established procedures for writing and reviewing reports, all substantive written communications with other agents or agency personnel, prosecutors or other Department of Justice personnel should be in the form of a formal investigative report or formal letter, and not in the form of electronic mail. “Substantive” communications include reports about investigative activity, discussions of the relative merits of evidence, characterizations of potential testimony, interviews of or interactions with witnesses/victims, and issues relating to credibility.

Email may be the most efficient and appropriate method to communicate regarding case strategy, case organization, case-related tasks that need to be conducted in anticipation of litigation, or to seek or provide legal advice on a pending investigation or case. Such emails are “potentially privileged” and as such may be protected from discovery. However, emails from an agent or other agency personnel to a prosecutor or other Department of Justice personnel in response to “to-do” list emails could possibly fall within the “substantive” communications that may not be privileged.

If email is used to communicate substantive or potentially privileged case-related information between agents, between agents and agency personnel, prosecutors or any Department of Justice personnel, or between victims/witnesses and the agent, the email must be retained in the investigative tracking system, and provided to the prosecutor along with formal reports.

OI employees should make every effort to limit email exchanges with victim/witnesses to non-substantive matters, such as the scheduling of interviews or notification of dates and times of hearings. Any substantive information received from a victim or witness should be considered potential Jencks Act material and maintained for Brady/Giglio review.

Email may be used to send formal investigative reports as attachments, or to communicate efficiently regarding non-substantive issues such as scheduling meetings, interviews, and court appearances.

Emails should never contain unprofessional language.

Figure 500-01 – Subpoena Memorandum Request Form Format (Non-Financial)

Date

MEMORANDUM FOR PATRICK E. McFARLAND
Inspector General

THROUGH: MICHELLE B. SCHMITZ
Assistant Inspector General for Investigations

FROM: JOHN DOE
Special Agent, D.C. Metro Region

SUBJECT: Request for Issuance of a Subpoena

We request a subpoena be issued in the matter described below:

1. Authority: Inspector General (IG) Act of 1978, 5 U.S.C. App.
2. OIG file No.: I-14-XXXXXX
3. Nature of the inquiry: Investigation
 Joint audit/investigation
 Other
4. U.S. Office of Personnel Management (OPM): Federal Employees Health Benefits Program (FEHBP).
5. Suspect(s)/Focus of inquiry: Dr. Jane Doe
6. Name(s) of person(s) (and title, if the person to be subpoenaed is in representative capacity) or entity to be subpoenaed: Nurse Smith, RN, JD, CPHRM.
7. Address: Nurse Smith, RN, JD, CPHRM
Director of Risk Management, Safety & Compliance
Washington, DC

8. Relationship of person(s)/entity to be subpoenaed to subject of inquiry:

The Hospital is the custodian of records for medical services provided to FEHBP beneficiaries by Dr. Jane Doe at the Hospital.

9. Background: See Appendix I.

10. Purpose of subpoena: To determine whether Dr. Jane Doe submitted fraudulent health insurance claims to the FEHBP insurance plans.

11. Description of records sought: See Appendix A.

12. Are records available under statute, regulation, or audit access clause of a contract or other agreement?

Yes No

If yes, describe:

13. Have efforts been made to obtain records by means other than subpoena?

Yes No

If so, how and with what results?

If not, why not? (b) (7)(E)

14. Is the subpoenaed information protected by the Right to Financial Privacy Act? Yes No

If so, list the name(s) and address(es), including the county of the individual(s) who should receive a customer notification letter:

Not applicable.

14. Is the person(s)/entity to be subpoenaed the subject of any other law enforcement investigation or any civil, criminal, or administrative proceeding?

15. Yes Unknown

If so, describe:

16. Has the subject(s) of this inquiry been discussed with the FBI, a United States Attorney's Office, or the Department of Justice in Washington, D.C.?

Yes No

If yes, explain: This case has been accepted by the U.S. Attorney's Office for Maryland.

17. Method of service (e.g., mail, hand-delivery, etc.): Hand-Delivery

18. OIG employee to receive the information:

Special Agent (SA) John Doe
U.S. Office of Personnel Management
Office of the Inspector General-Office of Investigations
6400 Baltimore National Pike, Suite 322
Catonsville, Maryland 21228

19. Location for in-person production of records: SA John Doe will pick up the records from the Hospital.

20. Recommendation for permitting production of records by mail:

Yes No

If yes, explain:

21. Date and time for production: As soon as possible after the receipt of this subpoena but not more that fourteen days after receipt.

FOR HEADQUARTERS USE

22. Approved by AIGI: [] Yes [] No
Initials and date:

Comments, if any:

23. Cleared by Counsel: [] Yes [] No
Initials and date:

Comments, if any:

24. Approved by IG or Deputy IG: [] Yes [] No
Initials and date:

Comments, if any:

APPENDIX I

A. Purpose of the inquiry: To determine whether Dr. Doe submitted fraudulent health insurance claims to the FEHBP insurance plans.

B. Summary of known facts: (b) (7)(E)

[Redacted text block containing multiple paragraphs of information obscured by black bars.]

APPENDIX A

The Hospital is requested to provide the following:

1. Original and complete patient medical records for each of the below-listed patients insured by the Federal Employees Health Benefits Program (FEHBP), to include but not limited to: (b) (7)(E)
[REDACTED]
2. All claims for reimbursement submitted to the FEHBP program with respect to the below-listed FEHBP patients, (b) (7)(E)
[REDACTED].
3. All (b) (7)(E) [REDACTED] for the FEHBP patients listed below.

Please contact Special Agent John Doe to arrange for pick-up of the requested medical records. His contact information is as follows:

John Doe
Special Agent
U.S. Office of Personnel Management
Office of the Inspector General
6400 Baltimore National Pike, Suite 322
Catonsville, Maryland 21228-3915

Figure 500-02 – Subpoena Memorandum Request Form Format (Financial Institution)

Date

MEMORANDUM FOR PATRICK E. McFARLAND
Inspector General

THROUGH: MICHELLE B. SCHMITZ
Assistant Inspector General for Investigations

FROM: (b) (7)(C), (b) (7)(E)
Special Agent

SUBJECT: Request for Issuance of a Subpoena

We request that a subpoena be issued in the matter described below:

1. Authority: Inspector General (IG) Act of 1978, 5 U.S.C. App.
2. OIG file No.: I-14-XXXXXX
3. Nature of the inquiry: Investigation
 Joint audit/investigation
 Other
4. U.S. Office of Personnel Management (OPM) Program: Civil Service Retirement System (CSRS), Center for Retirement and Insurance Services (CRIS).
5. Subject(s)/Focus of inquiry: Jonathan Doe.
6. Name(s) of person(s) (and title, if person to be subpoenaed is in representative capacity) or entity to be subpoenaed: US Bank, N.A.

7. Address: US Bank, N.A.
800 Nicollet Mall
Legal Department – Subpoena Processing
21st Floor
Minneapolis, MN 55402
8. Relationship of person(s)/entity to be subpoenaed to subject of inquiry: US Bank, N.A. may hold the personal account information of the subject(s) under investigation.
9. Background: See Appendix I.
10. Purpose of Subpoena: To determine who fraudulently obtained and utilized CSRS survivor annuity payments in the amount of \$59,622.65, issued to deceased Federal survivor annuitant Jane Doe, CSRS claim number XXXXXXXXW, after her death on October 18, 1995.
11. Description of records sought: See Appendix A.
12. Are records available under statute, regulation, or audit access clause of a contract or other agreement?
 Yes No
- If yes, describe:
13. Have efforts been made to obtain records by means other than subpoena?
 Yes No
- If so, how and with what results?
- If not, why not? The Right to Financial Privacy Act precludes banking institutions from providing customer account information without a subpoena.

14. Is the subpoenaed information protected by the Right to Financial Privacy Act?
 Yes No

If so, list the name(s) and address(es), including the county of the individual(s) who should receive a customer notification letter:

Jonathan Doe
3953 San Juan Ave.
Carmichael, CA 95608-2639
Sacramento County

15. Is the person(s)/entity to be subpoenaed the subject of any other law enforcement investigation or any civil, criminal, or administrative proceedings?
 Yes Unknown

16. Has the subject of this inquiry been discussed with the FBI, a United States Attorney's Office, or the Department of Justice in Washington, D.C.?
 Yes No

If yes, explain:

17. Method of service (e.g., certified mail, hand-delivery, etc.): Certified Mail.

18. OIG employee to receive the information:

Special Agent Tom Jones
U.S. Office of Personnel Management
Office of the Inspector General
800 NE Tenney Rd., Ste 110 PMB 438
Vancouver, WA 98685

19. Location for in-person production of records: N/A

20. Recommendation for permitting production of records by mail:
 Yes No

If yes, explain: The location of bank makes production of records by mail preferable.

21. Date and time for production: Fourteen (14) days from the date of the subpoena.

FOR HEADQUARTERS USE

22. Approved by AIGI: [] Yes [] No
Initials and date:

Comments, if any:

23. Cleared by Counsel: [] Yes [] No
Initials and date:

Comments, if any:

24. Approved by IG or Deputy IG: [] Yes [] No
Initials and date:

Comments, if any:

APPENDIX I

A. Purpose of the inquiry: To determine who fraudulently received and utilized CSRS survivor annuity benefit payments in the amount of \$59,622.65, issued to deceased Federal annuitant Jane Doe, CSRS claim number CSFXXXXXXXXXW, after her death on October 18, 1995, and to determine if the US Bank, N.A. is liable for losses sustained by the Government.

B. Summary of known facts: (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E)



APPENDIX A

(b)(7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)




Figure 500-03 – "Tracing of Firearms in Connection with Criminal Investigations"

(b) (7)(E)



(b) (7)(E)



Figure 500-04 – Miranda Warning



OFFICE OF
THE INSPECTOR GENERAL

**UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100**

WARNING AND WAIVER OF RIGHTS

Location: _____

Date: _____ Time: _____

WARNING

BEFORE YOU ARE ASKED ANY QUESTIONS, YOU MUST UNDERSTAND YOUR RIGHTS.

- You have a right to remain silent.
- Anything you say can be used against you in court.
- You have the right to talk to a lawyer for advice before we ask you any questions and to have him with you during questioning.
- If you cannot afford a lawyer, one will be appointed for you before any questioning if you wish.
- If you decide to answer questions now without a lawyer present, you will still have the right to stop answering questions at any time. You have the right to stop answering questions at any time until you talk to a lawyer.

I have read this statement of my rights (This statement of my rights has been read to me) and I understand what my rights are.

(Date) (Time) (Print Name) (Signature)

WAIVER

I am willing to discuss subjects presented and answer questions. I do not want a lawyer at this time. I understand and know what I am doing. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

(Date) (Time) (Signature)

Witnessed by: _____
Title: _____

Witnessed by: _____
Title: _____

Figure 500-05 – Garrity Warning



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

**WARNINGS AND ASSURANCES
TO EMPLOYEE REQUESTED TO PROVIDE INFORMATION
ON A VOLUNTARY BASIS (GARRITY)**

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General into alleged misconduct and/or improper performance of official duties. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

This is a voluntary interview. Accordingly, you do not have to answer questions. No disciplinary action will be taken against you solely for refusing to answer questions.

Any statement you furnish may be used as evidence in any future criminal proceeding or agency disciplinary proceeding, or both.

ACKNOWLEDGEMENT

I understand the warnings and assurances stated above and I am willing to make a statement and answer questions. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

Office of Inspector General
Special Agent

Employee's Signature

Witness: _____

Date: _____

Time: _____

Location: _____

Figure 500-06 – Kalkines Warning



**United States
Office of
Personnel
Management**

OFFICE OF INSPECTOR GENERAL

Notification of Your Rights and Obligations

Before I ask you any questions, or request a statement, I must advise you of the following:

You are going to be asked a number of specific questions concerning the performance of your official duties.

You have a duty to reply to these questions and agency disciplinary proceedings may be instituted as a result of your answers. However, neither your answers nor anything gained as a result of such statements can be used against you in any criminal proceeding (except you may be criminally prosecuted for knowing and willfully providing false statements or information in your answers).

I have read or have had read to me the above statement of my rights and obligations as an employee of the U.S. Office of Personnel Management. I understand what these rights and obligations are.

Employee Signature

Date

Time

Witnessed By

Special Agent
Office of Personnel Management
Office of Inspector General

Witnessed By

Figure 500-07 – Sworn Statement



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

Sworn Statement

Date: _____

Time: _____

Case #: _____

Place: _____

I, _____, residing at

having been duly sworn as provided by law, make the following statement freely and voluntarily to _____, a Special Agent of the U.S. Office of Personnel Management, Office of the Inspector General:

Sworn Statement of (Sign): _____ Date: _____

Witnessed By (Sign): _____ Date: _____

ATTACHMENT A

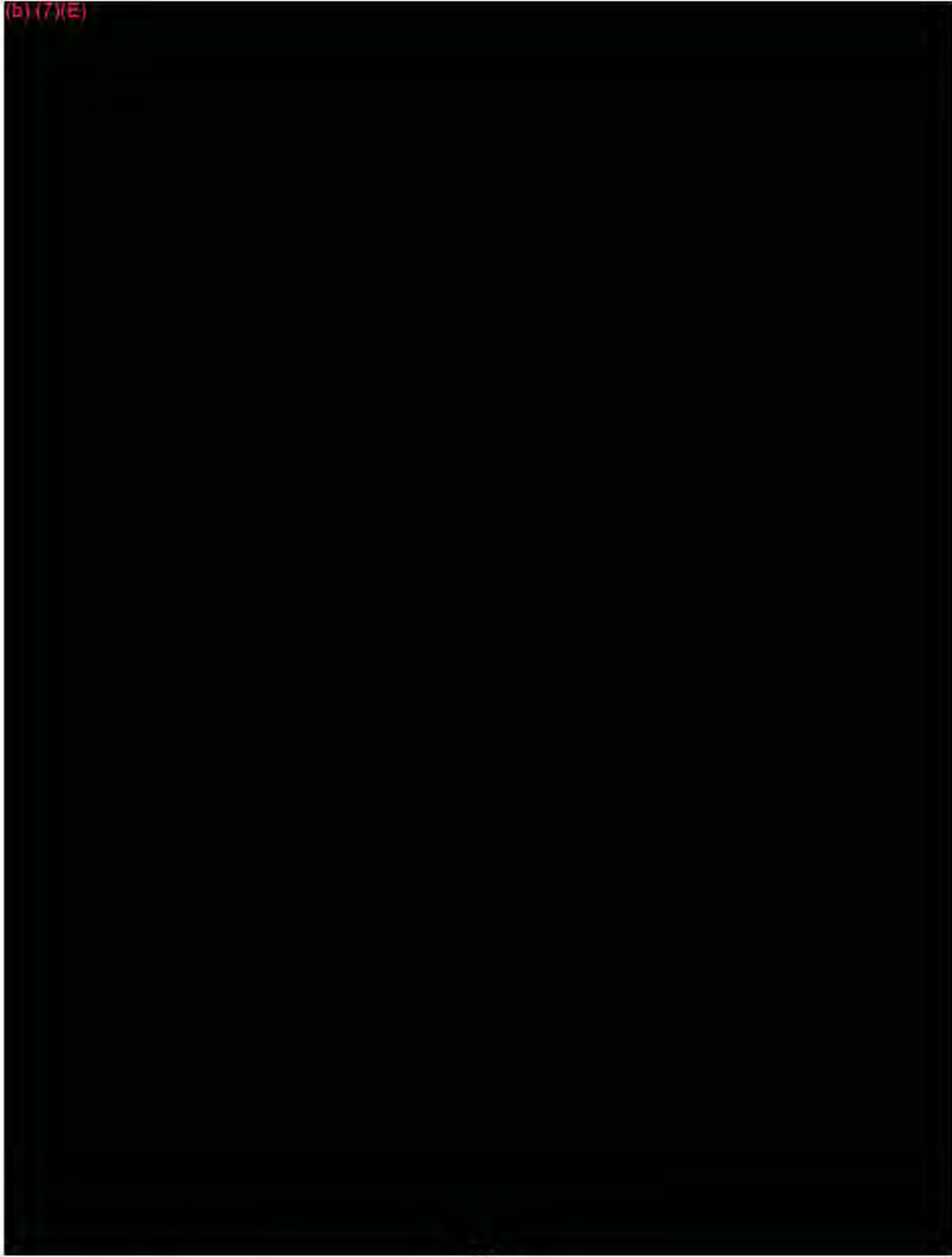
Oath:

Do you solemnly swear that the information you have provided in the form of this written statement is the truth, the whole truth, and nothing but the truth?

Affirmation:

Do you solemnly affirm, under the penalties of perjury, that the information you have provided in the form of this written statement is the truth, the whole truth, and nothing but the truth?

(b) (7)(E)



Chapter 6

Health Care Fraud Investigations

600.00 Introduction

One of the primary responsibilities of the Office of Personnel Management (OPM), Office of Inspector General (OIG), Office of Investigation (OI) is to investigate fraud against the Federal Employees Health Benefits Program (FEHBP). The FEHBP was established by the Federal Employees Health Benefits Act (Public Law 86-382) on September 28, 1959. The provisions of the Act are implemented by the OPM through regulations codified in Chapter 1, Part 890, of Title 5, Code of Federal Regulations. The FEHBP is a Federally funded medical insurance program that was created to provide health insurance benefits for federal employees, annuitants, and their spouses and dependent unmarried children under the age of twenty-two.

The FEHBP is the largest, employer-sponsored health insurance program in the world. The FEHBP serves as an insurance purchaser by contracting with several hundred health plans to offer benefits to around 9 million eligible individuals. FEHBP administrators negotiate premiums and benefits with participating health plans, including both fee-for-service plans and health maintenance organizations.

The Federal government contributes approximately 70% of the insurance premiums, with Federal employees and annuitants paying the rest. All premium payments, both from the government and from individuals, are deposited into the FEHB Fund, which is held at the US Treasury and administered by OPM.

600.10 Types of Health Care Fraud

The OI participates in criminal, civil, and administrative investigations affecting the FEHBP. Fraud schemes affect the delivery of and payment for nearly every service or product associated with modern health care. (b) (7) [REDACTED]

(E)

601.0 Federal Statutes Used to Prosecute Health Care Fraud Matters

- (a) Title 18 Section 201 - Bribery, Graft and Conflicts of Interest
- (b) Title 18 Section 286 - Conspiracy to Defraud the Government
- (c) Title 18 Section 287 - False, Fictitious or Fraudulent Claims
- (d) Title 18 Section 371 - Conspiracy to Commit Offense or Defraud the United States
- (e) Title 18 Section 664 - Theft or Embezzlement from Employee Benefit Plan
- (f) Title 18 Section 666 - Theft or Bribery Concerning Programs Receiving Federal Funds
- (g) Title 18 Section 669 - Theft or Embezzlement in Connection with Health Care
- (h) Title 18 Section 1001 - Making False Statement
- (i) Title 18 Section 1035 - False Statements relating to Health Care Matters
- (j) Title 18 Section 1341 - Mail Fraud
- (k) Title 18 Section 1343 - Fraud by Wire, Radio or Television
- (l) Title 18 Section 1347 - Health Care Fraud
- (m) Title 18 Section 1518 - Obstruction of Criminal Investigations
- (n) Title 18 Section 1956 and 1957 - Money Laundering
- (o) Title 18 Section 1028A - Aggravated Identity Theft

602.00 Jurisdiction/Venue

For prosecution purposes, the venue of health care fraud investigations includes any district in which a provider, health care plan, or beneficiary is located; where a service is provided or received; or where claims originated, are processed, and/or paid.

603.00 Investigative Techniques

(b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

604.00 Sharing of Information with Other Agencies

The Health Insurance Portability and Accountability Act (HIPAA) encourages the use of multi-agency working groups and task forces to address health care fraud. The guidelines also encourage the sharing of information with the private sector. The OI encourages the sharing of information permitted by HIPAA with the members, both public and private, of various health care fraud working groups.

Each field office will establish liaison with health care insurance carriers and all other federal, state, and local law enforcement agencies that are investigating health care fraud.

605.00 Prioritization

Health care fraud referrals will be prioritized based upon the potential for patient harm, the extent of the potential financial damages to the FEHBP, and the credibility of the allegation.

605.10 Evaluation of Health Care Fraud Allegations

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

606.00 Desk Review

(b) (7)(E) [Redacted]



607.00 Presenting the Case for Prosecution

1. Health care fraud cases are presented to the United States Attorney's Office in the relevant judicial district. Agents should present all aspects of the case, and let the prosecutor determine the strengths and weaknesses of the case.
2. If the United States Attorney's Office declines the case, the agent should attempt to obtain a declination letter. If the United States Attorney's Office fails to provide a declination letter, the agent should send a written message to the relevant Assistant United States Attorney confirming the conversation during which the case was declined.
3. If the case is declined Federally, agents are encouraged to present cases to state or local prosecutors. However, a declination from the United States Attorney's Office is required first. Agents should consider all available remedies, including civil action and administrative sanctions.

608.00 Approval for Civil Settlements

Settlements of cases involving health care providers or suppliers under the FEHBP must be approved and signed by OPM's Assistant Director for Federal Employee Insurance Operations. If the settlement debars, suspends, or imposes a civil monetary penalty, or agrees not to do so, the Debarring Official must also approve and sign the settlement. Special agents may not approve a settlement on behalf of OPM, and are not to send draft or final settlement agreements directly to the Office of Healthcare and Insurance. Rather, special agents must notify the Counsel to the IG or the Assistant IG for Legal Affairs prior to the completion of settlement discussions. The Counsel to the IG or the Assistant IG for Legal Affairs will work with OPM's Office of General Counsel to obtain the necessary legal review and agency approval.

609.00 Recoveries to the FEHB Trust Fund

Any financial recoveries to the FEHB Trust Fund as a result of OI cases must be reported, in writing, to OPM's Office of the Chief Financial Officer and to Federal Employee Insurance Operations via memorandum from the agent, through the DAIGI. The memorandum must specify

the total dollar amount of the recovery, and break down the amount of the recovery attributable to each FEHBP insurance carrier by both percentage and dollar amount. This memorandum is required in order for proper accounting of recoveries to carrier trust fund reserves (**Figure 600-01 and Figure 600-02**).

610.00 Other OPM Administered health care programs

While the majority of the health care fraud investigations conducted by the OI concern the FEHBP, it should be noted that OPM does administer other programs with vulnerability to health care fraud schemes, such as the Federal Long Term Care Insurance Program (FLTCIP), the Federal Employees Dental and Vision Insurance Program (FEDVIP), the Federal Flexible Spending Account Program (FSAFEDS), and disability retirement. The OIG investigates allegations of fraud within or affecting these programs.

620.00 Multi-State Plan Program

OPM also contracts with private health insurers pursuant to the Multi-State Plan (MSP) Program established under the Affordable Care Act. The OIG will investigate allegations of contract fraud by an MSP insurer under contract with OPM. However, the Multi-State Plan Program is administered by the Department of Health and Human Services (HHS) and premium payments to MSPs do not flow through OPM controlled accounts at the Department of the Treasury. Therefore, provider and enrollee frauds affecting the MSPs are outside the investigative jurisdiction of the OIG, and are referred to other law enforcement agencies, such as the Federal Bureau of Investigation and HHS OIG.

Figure 600-01 – Health Care Fraud Restitution Memo (Criminal)



OFFICE OF
THE INSPECTOR GENERAL

**UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100**

October 1, 2013

MEMORANDUM FOR

(b) (6), (b) (7)(C)

Supervisor, Financial Management Specialist
Office of the Chief Financial Officer

(b) (6), (b) (7)(C)

Accountant
Office of the Chief Financial Officer

(b) (6), (b) (7)(C)

Program Analyst
Health Insurance, Federal Employee Insurance

Operations

THROUGH:

(b) (6), (b) (7)(C)

Deputy Assistant Inspector General for Investigations
Office of the Inspector General

FROM:

YOUR NAME
Special Agent
Office of the Inspector General

SUBJECT:

Investigative Recoveries-
OIG Case Name: XXXX
OIG Case Number: I XX XXXXX

Pursuant to our criminal investigation, **Subject Name** was convicted and sentenced to **X months of incarceration (if ordered), X months of supervised release (if ordered), and ordered to pay restitution in the amount of \$X,XXX.xx** to the Federal Employees Health Benefits Program (FEHBP). The restitution will be paid in a lump sum or paid in multiple installments through the IPAC System or by US Treasury Check(s)/state Check(s). The funds should be distributed as follows:

Carrier	Percentage	Dollars
APWU (Plan Code 47)	xx.xx%	\$xxx.xx
BCBS (Plan Code 10)	xx.xx%	\$xxx.xx
CVTY (Plan Code 45)	xx.xx%	\$xxx.xx
GEHA (Plan Code 31)	xx.xx%	\$xxx.xx
NALC (Plan Code 32)	xx.xx%	\$xxx.xx
SAMBA (Plan Code 44)	<u>xx.xx%</u>	<u>\$xxx.xx</u>
Total	100.00%	\$x,xxx,xx.xx

Please feel free to contact me at **Your Phone Number** or by e mail at **Your Email Address** should you have any questions. Thank you.

cc: Drew Grimm, (b) (6), (b) (7)(C)

Figure 600-02 – Health Care Fraud Restitution Memo (Civil)



OFFICE OF
THE INSPECTOR GENERAL

**UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100**

October 1, 2013

MEMORANDUM FOR

(b) (7)(C), (b) (6)

Supervisor, Financial Management Specialist
Office of the Chief Financial Officer

(b) (7)(C), (b) (6)

Accountant
Office of the Chief Financial Officer

(b) (6), (b) (7)(C)

Program Analyst
Health Insurance, Federal Employee Insurance

Operations

THROUGH:

(b) (7)(C), (b) (6)

Deputy Assistant Inspector General for Investigations
Office of the Inspector General

FROM:

YOUR NAME
Special Agent
Office of the Inspector General

SUBJECT:

Investigative Recoveries-
OIG Case Name: XXXX
OIG Case Number: I XX XXXXX

Our civil investigation of **Subject Name** has resulted in a civil settlement. As part of the civil settlement, the Federal Employees Health Benefits (FEHBP) was awarded **\$xx,xxx.xx**, minus the 3% DOJ allocation of **\$xx.xx**, leaving a net recovery to the FEHBP of **\$xx,xxx.xx**. The restitution will be **paid in a lump sum or paid in multiple installments** through the IPAC System or by US Treasury Check(s)/State Check(s). The funds should be distributed as follows:

Carrier	Percentage	Dollars
AFSPA (Plan Code 40)	xx.xx%	\$xxx.xx
Aetna (Plan Code 22)	xx.xx%	\$xxx.xx
BCBS (Plan Code 10)	xx.xx%	\$xxx.xx
CVTY (Plan Code 45)	xx.xx%	\$xxx.xx
GEHA (Plan Code 31)	xx.xx%	\$xxx.xx
RCBP (Plan Code 38)	xx.xx%	\$xxx.xx
SAMBA (Plan Code 44)	<u>xx.xx%</u>	<u>\$xxx.xx</u>
Total	100.00%	\$x,xxx,xxx.xx

Please feel free to contact me at **Your Phone Number** or email at **Your Email Address** should you have any questions. Thank you.

cc: Drew Grimm, (b) (7)(C), (b) (E)

Chapter 7

Retirement Fraud Investigations

700.00 Introduction

One of the responsibilities for the Office of Personnel Management (OPM), Office of the Inspector General (OIG), Office of Investigations (OI), is to investigate fraud against the two federal retirement systems maintained by OPM.

700.10 OPM's Two Federal Retirement Systems

OPM is authorized under Title 5, U.S.C. to administer and oversee two federal retirement systems, the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS). The Civil Service Retirement and Disability Fund (CSRDF) is the source of benefits for both systems. The OPM/OIG is responsible for investigating and auditing incidences of fraud, waste and abuse within these two retirement systems.

Federal employees hired on or before December 31, 1983 are covered under CSRS. Employees hired since December 31, 1983, with less than five years of civilian federal service under CSRS, were automatically converted to FERS coverage on January 1, 1987, the date FERS was established. In addition, CSRS employees not automatically transferred to FERS were given an opportunity to elect FERS during an open enrollment period from July 1, 1987 through December 31, 1987, and during a second open enrollment period from July 1, 1998 through December 31, 1998.

700.20 Retirement Services (RS)

Retirement Services (RS) is the OPM program office responsible for administering the federal retirement systems. RS has two locations which process the retirement workload, the Theodore Roosevelt Building in Washington, D.C. and the Retirement Operations Center in Boyers, PA. The Retirement Operations Center collects and stores most retirement records and files and processes applications for retirement benefits. The Washington Office, the headquarters for RS, processes more complex retirement claims and addresses many of the issues associated with annuity roll maintenance. Both claims groups process pending retirement cases and post retirement changes. Claims 1 Group (DC) processes all disability cases and Claims 2 Group (Boyers) processes all survivor cases.

701.00 Various Types of Retirement Fraud

(b) (7)(E)

[Redacted text block containing approximately 20 lines of blacked-out content]

702.00 Federal Statutes Used to Prosecute Retirement Fraud

- (a) Title 18 Section 286- Conspiracy to Defraud the Government
- (b) Title 18 Section 287- False, Fictitious or Fraudulent Claims
- (c) Title 18 Section 371- Conspiracy to Commit Offense or Defraud the United States
- (d) Title 18 Section 666- Theft or Bribery Concerning Programs Receiving Federal Funds
- (e) Title 18 Section 1001- Making False Statements
- (f) Title 18 Section 1341- Mail Fraud

(g) Title 18 Section 1343- Fraud by Wire, Radio or Television.

(h) Title 18 Section 1028A – Aggravated Identity Theft.

703.00 Jurisdiction/Venue

For Federal prosecution purposes, the venue of retirement fraud investigations include the district where the fraud was committed and the districts where the claims originated, are processed, and/or paid.

704.00 Investigative Techniques

(b) (7)(E) [Redacted]

[Redacted]

704.10 Steps Needed to Investigate an Annuity Overpayment

(b) (7)(E) [Redacted]

- ▶ [Redacted]
- ▶ [Redacted]
- ▶ [Redacted]
- ▶ [Redacted]

[Redacted]

(b) (7)(E)



(b) (7)(E)



704.20 Check Copies

In annuity fraud cases involving hard copy checks, (b) (7)(E)



704.30 Subpoenas

Two types of OIG subpoenas are used in developing account information from relevant financial institutions. The first subpoena is sent to establish basic account holder information. The identities and addresses of all account holders are obtained first, because that information is required in order to comply with the Right to Financial Privacy Act prior to obtaining more detailed information. A second subpoena is used to request detailed account information. In these subpoenas, it is important that certain language appears in Appendix I as justification for the OIG subpoena. (b) (7)(E)



Current sample subpoenas are maintained in the investigative tracking system standard forms section. See IM 503 for more information regarding OIG administrative subpoenas.

705.00 Testifying and the Use of Expert Witnesses

The current procedure to request expert witnesses for testifying in a retirement case requires that the agent contact OIG counsel which submits the request to the OPM Office of General Counsel (OGC). OGC will contact the management of the respective program office and a witness will be made available. In addition, the investigative analysts in the OIG's Investigations Support Group are available to answer questions, collect data and give direction to the case agents and the prosecutors.

706.00 Case Closing Procedures

In all cases, the Office of the Chief Financial Officer and RS must be notified in writing of the conclusion and disposition of investigations and complaints. The assigned case agent is responsible for preparing a memorandum to the OCFO providing a brief synopsis of the case and communicating the final outcome of investigative work. The memorandum should also include information about cases that have been declined for prosecution by a federal, state, or local prosecutor. If the OIG-OI declines to investigate, this information, with an explanation, should be included in the memorandum.

Prompt notification enables the OCFO to accurately account for, collect, and monitor repayments to ensure the conditions of court orders or payment agreements are met. In addition, the OCFO will be able to take appropriate action to collect the overpayment when investigative actions have been unsuccessful (e.g. subject/debtor has died, there is no identifiable suspect, prosecution is declined, or defendant is found not guilty).

The establishment of an off-roll collection payment schedule is a multi-stage process that involves two separate offices within the OCFO. The Trust Funds Financial Branch is responsible for closing out the reclamation and establishing an off-roll account for collecting the overpayment. The Funds Management Branch is responsible for posting payment receipts to the established off-roll account, and monitoring the collection process. Questions regarding the collection process should be directed to either the Chief of the Receivables Management Section at 202-606-0716 or via email to the Funds Management Branch, at FundsManagement-TrustFunds@opm.gov. (b) (6), (b) (7) may be contacted at (b) (6), (b) (7) or (b) (7)(C), (b) (6) if no timely response is received from the Funds Management Branch via the group email address.

1. **Procedures:** The following guidelines provide direction for handling repayments to the retirement trust fund, notifying the OCFO of the final outcome of OIG-OI investigative work, documenting the investigative tracking system, and the final disposition of the RS retirement annuity case file.

a. Repayments by Hard Copy Check

A hardcopy check must:

- i. Be payable to the U.S. Office of Personnel Management;
- ii. Include the RS retirement CSA or CSF claim number;
- iii. Include the name of the annuitant or survivor annuitant whose annuity benefit was overpaid;
- iv. Be sent directly to the OPM at the following address so that the money can be applied to the appropriate accounts receivables account.

**U.S. Office of Personnel Management
Attention: Kenneth Harris - Chief of Trust Funds
Office of the Chief Financial Officer
1900 E Street, NW, Room 3H25
Washington, DC 20415**

b. Department of Justice Electronic Payments

In some cases involving repayments, a restitution order may require the convicted individual to make recurring payments (usually monthly) to the court. These payments are in turn sent electronically, through the Intra-Governmental Payment and Collection (IPAC) System, to OPM by the U.S. Department of Justice's Debt Management System. In these instances, the case agent will notify the court that payments must:

- i. Be identified by the debtor's name; and
- ii. Include the RS retirement CSA or CSF claim number.

The assigned case agent should include information regarding the method of repayment in the memorandum to the OCFO.

c. Notifying the OPM-OCFO of Investigative Outcome

In addition to ensuring that payments are correctly identified and sent to the appropriate location, it is necessary for the assigned case agent to prepare a memorandum to the OCFO and RS providing a brief synopsis of the investigation, investigation outcome, and any anticipated repayments to the trust fund. A memorandum is required in all retirement fraud cases regardless of the investigation outcome.

707.00 Investigation/Complaint Case Close-Out

The OIG-OI investigation or complaint case file should include a copy of the memorandum with the attachments sent to the OCFO and RS, and actions documented in the investigative tracking system. In cases involving restitution to the retirement fund, the case agent should not close the investigation until confirmation is received from OCFO that the collection process has been established. Once confirmation is received from the OCFO, the case agent should file the e-mail confirmation in the investigation or complaint file.

Chapter 8

Federal Investigative Services, Computer Forensics, and Combined Federal Campaign Investigations

800.00 Federal Investigative Services

801.00 Federal Investigative Services Investigations

In April 1953, President Eisenhower signed Executive Order 10450, which gave the U.S. Civil Service Commission (CSC), the predecessor to OPM, the authority and responsibility to manage the Federal government's personnel security program. While this required CSC/OPM to conduct background investigations on government employees, the Department of Defense (DOD) also retained independent authority to do likewise for DOD employees and military personnel through the Defense Security Service (DSS). The majority of the background investigators working for CSC/OPM were Federal employees until OPM privatized its background investigative function in July 1996.

In February 2005, the DSS' personnel security investigations mission was transferred to OPM, along with approximately 1800 DSS background investigators. This transfer was authorized by the Defense Authorization Act of FY 2004 and was implemented under an agreement between OPM and the Department of Defense. As of Fiscal Year 2013, FIS had a workforce of approximately 2517 Federal employees and 7091 contract investigators working throughout the United States and overseas.

FIS conducts background investigations for most Federal agencies and their contractors, and supports approximately 95% of all government security clearance investigations. Agencies use FIS's background investigation products to determine individuals' suitability for Federal civilian, military or Federal contract employment, as well as their eligibility for access to classified national security information. As such, these background investigations are essential to our nation's security. If a background investigation contains incorrect or fraudulent information, a qualified candidate may be wrongfully denied employment or an unsuitable person may be cleared and allowed access to Federal facilities or classified information.

FIS's Integrity Assurance performs quality assurance reviews on background investigations, through which potential fabrications of background investigation work products are identified and referred to the OIG for investigation.

801.10 Advisement of Rights and Administrative Warnings

The most common Federal Criminal Statutes used to prosecute FIS fabrication case are:

- Title 18 U.S.C. 1001 - False Statements
- Title 18 U.S.C. 1510 - Obstruction of criminal investigations

801.20 Major FIS Contractors

- KeyPoint
- CACI International, Inc

801.30 FIS Investigations

(b) (7)(E)



802.00 Computer Crimes Investigations

802.10 Authorized Computer Forensic Examinations

Computer forensic examinations may be authorized in any case where the crime under investigation is an offense punishable under Federal law, or the violation is otherwise under

investigation by OPM/OIG. This includes joint investigations with other law enforcement agencies.

802.20 Computer Forensics Training

OPM/OIG policy is that any electronic media considered to have evidentiary value must be examined only by personnel from a law enforcement agency who have the required specialized training. Attempts to “examine” electronic media without proper training and experience could lead to the alteration of crucial evidence. Computer forensics examinations shall only be conducted by individuals who have completed the Seized Computer Evidence Recovery Specialist course at the Federal Law Enforcement Training Center (FLETC) or equivalent training. When the need for a computer forensic examination is identified, the specific requirements of the examination shall be considered and a determination made as to whether the OIG has appropriately trained staff available to perform the examination, or whether assistance shall be requested from another agency.

802.30 Computer Forensic Examination Responsibilities

The success of a computer forensic examination often depends upon the professional capabilities of the case agent. The case agent is responsible for establishing probable cause to seize electronic media, and he/she is responsible for selecting and articulating the legal basis for any seizure. Computer forensic personnel can assist the case agent by explaining the technical issues and potential problems; providing expertise that can be used in an affidavit; and providing language that will explain technical issues in non-technical language. Reference is made to the published Department of Justice Federal Guidelines for Searching and Seizing Computers and the *Quality Standards for Digital Forensics* from the Council of the Inspectors General for Integrity and Efficiency (**Appendix K**).

The role that any computer or electronic media may play in the investigation needs to be fully articulated prior to examination. The computer or storage media can be an instrument of the crime, or it can merely be a repository for evidence. In the former case, if the case agent can show that the computer was an essential part of the commission of the crime, then he/she will be better able to justify the seizure of the computer/electronic media to a court. If the computer is only used as a repository for records, then an image of the computer’s hard-drive may be sufficient, and seizure of the computer may not be approved unless there are significant reasons that such seizure is necessary.

If a case has been investigated properly, a computer forensic examination can contribute to the successful conclusion of the investigation. The case agent must understand that the computer forensic examination is a tool for their investigation and that a thorough field investigation must be conducted, aimed at securing competent evidence to prove or disprove an offense or allegation.

Effective computer forensic examinations require intelligence concerning what is to be seized and what evidence is expected to be contained in the computer or electronic media. The case agent must articulate the purpose of the examination and what information needs to be developed.

Computer forensic personnel can conduct a number of different types of computer forensic examinations on a given piece of electronic media. They can also use a variety of tools with different parameters. The type of examination and the tools to be used are chosen based upon the examination goals as set by the case agent and the computer forensic examiner.

The AIGI has the overall responsibility for the formulation and implementation of all policy and procedures relating to computer crime investigations. The AIGI also has the ultimate responsibility for the procurement of computer forensic assistance from other agencies, when required.

802.40 Computer Crime and Forensic Assistance Request Procedures

(b) (7)(E)



(b) (7)(E)

802.50 Request for Examinations on Previously Collected Evidence

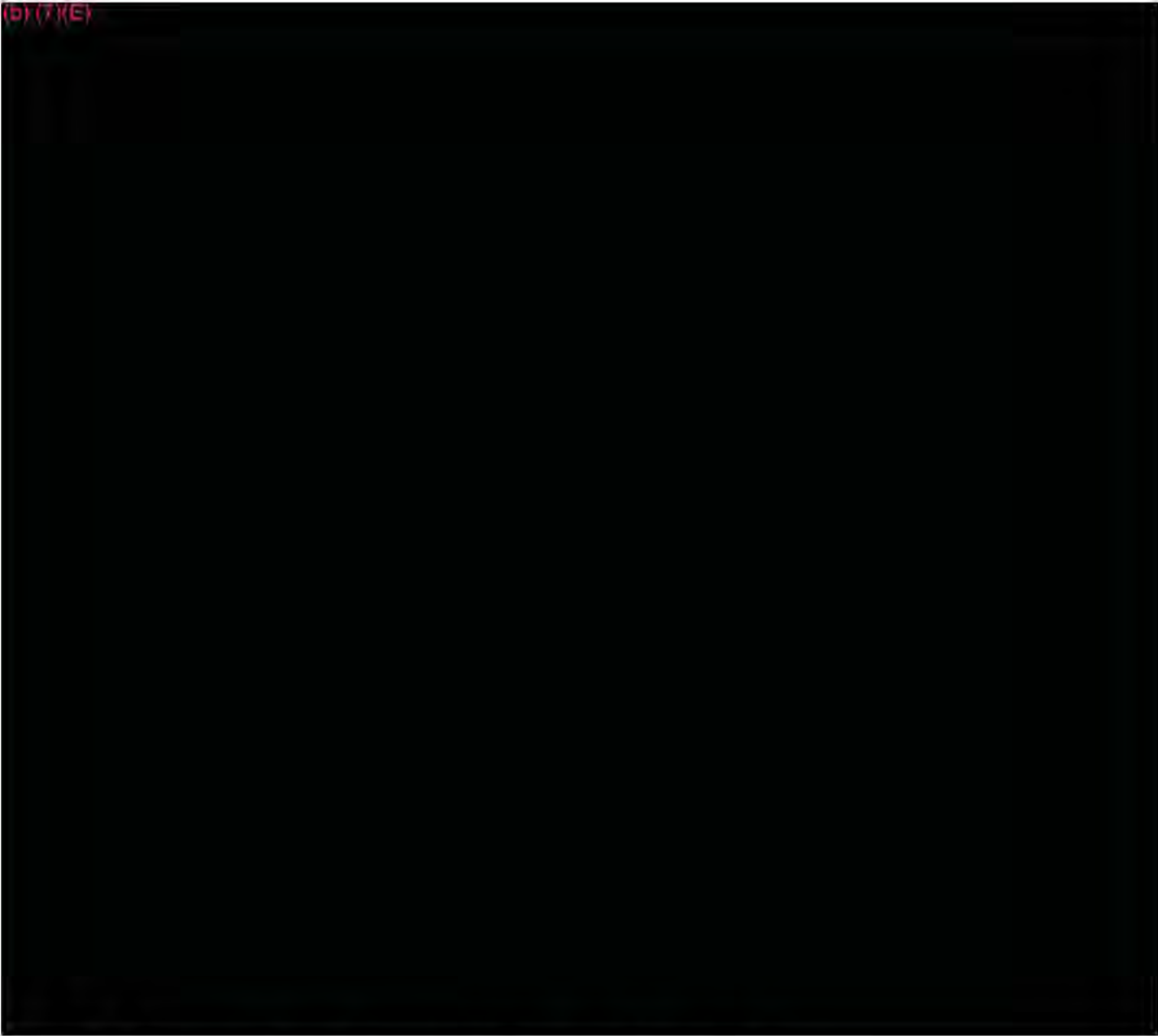
Appropriate authorizations must accompany requests for computer forensic examinations of electronic media that is already in an agent's possession. When written consent to search a computer is granted, a copy of the written consent form or the proof of implied consent through the production of user agreements, printout of properly worded log on banners, or other relevant documentation must be attached. Each item to be examined must be inventoried on an appropriate evidence form. Chain of custody issues must be resolved prior to the computer forensic examination. Due to a variety of legal issues and constraints, search warrants are often required prior to conducting forensic examinations (e.g., unopened emails, personally owned computers, etc.). If neither actual nor implied consent to search is obtained by investigators, case agents should make appropriate inquiries regarding the need to secure a search warrant before requesting examination of a computer.

802.60 Handling of Digital Evidence During Computer Forensics Examinations

This section provides guidance for the handling of digital evidence during computer forensics examinations by trained computer forensic staff. Each forensic examination of digital evidence is unique and may not be conducted in the exact same manner. Any variations from the guidance in this section must be forensically sound and generally accepted within the law enforcement forensic community.

Evidence receipts and logs for digital evidence shall be used in accordance with Chapter 13 of this manual.

(b) (7)(E)



802.70 Computer Forensic Examination Reporting Procedures

After the computer forensic examination is completed, but before the examination report is prepared, the examiner will contact the OPM/OIG case agent to discuss the findings. As a result of this conversation, the case agent may make additional requests. In the event that there are no additional requests concerning the examination, the computer forensic staff will prepare a Forensic Examination Report concerning the examination. The Case Agent shall be provided with copies (either hard copy or electronic) of discovered evidence and a signed Forensic Examination Report.

803.00 Combined Federal Campaign

803.10 Combined Federal Campaign Investigations

In 1961 Executive Orders 12353 and 12404 authorized the United States Office of Personnel Management (OPM) (at the time called the Civil Service Commission) to prescribe rules and regulations to facilitate fund raising on behalf of charitable organizations through on-the-job solicitation of Federal employees and military personnel, and to ensure that recipient agencies are responsible in the use of the funds raised. As a result, OPM created the Combined Federal Campaign (CFC).

The CFC rules, regulations and standards can be found in Title 5, Part 950 of the Code of Federal Regulations (CFR). The CFR outlines the CFC program's organizational structure, solicitation methods, expense reimbursement, contribution disbursement, and reporting requirements. On April 17, 2014, OPM significantly revised 5 CFR 950, with the changes effective beginning in the 2016 Combined Federal Campaign.

The OPM/OIG is responsible for the prevention, detection, and investigation of theft, embezzlement, and fraud concerning the CFC.

The OIG maintains an audit and oversight function of the collected CFC funds to safeguard the program from theft, embezzlement, fraud and misappropriation of the CFC funds. Although the CFC funds are not technically "Federal Funds" because the collected contributions come from Federal employees and Military personnel and not from congressional funding, any intentional misappropriation, theft, and/or embezzlement of these funds may be considered a criminal violation.

803.20 Criminal Statutes

The most common Federal Criminal Statutes used to prosecute CFC cases are:

- Title 18 U.S.C. 641 - Theft / Fraudulent Conversion of Government Property
- Title 18 U.S.C. 1341 - Mail Fraud
- Title 18 U.S.C. 1343 - Wire Fraud
- Title 18 U.S.C. 1001 - False Statements

803.30 Definitions

- "LFCC" or the Local Federal Coordinating Committee: The LFCC is a group of

designated Federal employees, usually supervisors, and representatives of local unions who are designated by their agencies to conduct the CFC in a local area. Prior to 2016, the LFCC selected the Principle Combined Fund Organization (PCFO) on a yearly basis. After 2016, the LFCC is no longer responsible for selecting a PCFO, but its other responsibilities remain the same. These responsibilities include providing oversight of the local campaign; approving local charity applications; and reviewing collections, disbursements, and expenses at the end of each campaign cycle.

- “PCFO” or the Principle Combined Fund Organization: PCFOs were the fiscal agents that administered the campaign in each local CFC area in years prior to 2016. The PCFO was most commonly a local United Way organization, but could also be a private non-profit company. The PCFO was responsible for all aspects of the campaign planning, organizing, and administration, including the disbursement of designated contributions to specific charities. The PCFO was also reimbursed for 100% of the expenses related to the administration of the CFC up to an agreed upon limitation. In most cases, when the United Way was the PCFO, they had a designated employee who directed all aspects of the CFC program.
- “CCA” or Central Campaign Administrator: Effective January 1, 2016, the PCFOs for local campaigns were eliminated and replaced by one or more CCAs, in an effort by OPM to centralize the CFC’s fiscal administration functions. The CCA may either perform all fiscal administration functions itself or set up regional receipt and disbursement centers.
- Outreach Coordinator: Outreach coordinators were also created effective in 2016. They are hired by the LFCC and perform the marketing functions previously performed by PCFOs.

803.40 CFC Investigations

(b) (7) (E)



804.00 Bribery/Kickback Investigations

This section establishes OPM OIG policy regarding bribery and kickback investigations. The Federal Bureau of Investigations has investigative jurisdiction in **significant** instances of bribery being investigated under Title 18, U.S.C..

804.10 Authority

Although there are a number of Federal statutes prohibiting bribery of Federal officials, the most frequently employed and most important statute is 18 U.S.C. 201. It provides in part:

“Whoever, directly or indirectly, corruptly gives, offers or promises anything of value to any public official...with intent...to influence any official act; or...to influence such official...to commit or aid in committing...or allow, any fraud...on the United States...,” shall be guilty of an offense against the laws of the United States.

Other provisions of 18 U.S.C. are:

1. Offering a bribe, 18 U.S.C. 201 (b)
2. Seeking or accepting a bribe, 18 U.S.C. 201 (c)
3. Offering a bribe to a witness, 18 U.S.C. 201 (d)
4. Offering gratuities or graft to a public official, 18 U.S.C. 201 (f)

5. Graft, soliciting or accepting illegal gratuities, 18 U.S.C. 201 (g)

Offering a bribe (18 U.S.C. 201 (b)) – Elements of the offense:

1. That the subject gave, offered or promised, directly or indirectly, to give something of value;
2. To a public official or a person who has been selected to be a public official;
3. That the subject acted corruptly;
4. That the subject made the offer or promise with the intent to:
 - a. Influence some official act of the official or
 - b. Induce a breach of official duty or
 - c. Induce the official to commit or permit a fraud on the United States.
5. The thing of value need to actually be given. The offense is complete upon making the offer. The public official need not actually be influenced. He may refuse the offer, yet the offense is complete. Nor does the item or thing of value personally have to benefit the public officials. However, the offer must be made to the public official, either directly or indirectly.
6. The bribe must relate to an official act, not a private matter. For example, an offer of payment to a public official to place an illegal wager would not constitute bribery since gambling is not part of the public official's duty.

The Comprehensive Crime Control Act of 1984 added a new section applicable to bribery investigations: 18 U.S.C. 666 (a) of the statute makes it a crime for an agent of any organization, state or local Government agency that receives benefits of \$10,000 or more in any year, under a "Federal program involving a grant, contract, subsidy, loan, guarantee, insurance or another form of Federal assistance," to steal, embezzle, obtain by fraud or otherwise knowingly convert without authorization, property of the organization valued at \$5,000 or more. Subsection (b) makes it a crime for such an agent to solicit or accept anything of value from anyone other than his employer because of the agent's conduct in any transaction involving \$5,000 or more concerning the affairs of the organization. Finally, subsection (c) makes it a crime to offer a bribe to an agent because of the agent's conduct in transactions concerning the organization, again where the transactions involve \$5,000 or more. All three offenses are punishable by up to 10 years imprisonment and a fine of either \$100,000 or twice the value of the property stolen (subsection a) or twice the amount of the bribe (subsections b and c), whichever is greater.

804.20 Definitions

1. **Corruption:** Wrongful activity or some aspect of a wrongful pattern of activity committed in part by an individual holding a position of trust by the use of deception in order to obtain something of value or to obtain a personal advantage.
2. **Gratuity:** “Any gift, favor, entertainment, hospitality, transportation, loan, and any benefit, for example discounts, passes etc., given or extended to or on behalf of OPM personnel, their immediate families, or households for which fair market value is not paid by the recipient or the U.S. Government.” Gratuities are distinguished from bribes in that there is usually no request for specific improper action in exchange for what is being offered. Gratuities are generally given to enhance the relationship between the offerer and the Government employee.
3. **Bribe:** Anything of value provided, solicited or demanded, directly or indirectly, by or to any OPM employee, or person selected to be an OPM employee to influence any official act, to influence such employee to commit or aid in committing a fraud against the United States, or to omit to do any act in violation of the lawful duty of such employee.
4. **Entrapment:** Acts of officers of the Government in inducing a person to commit a crime not contemplated by the person in order to initiate a criminal prosecution. The inducement may consist of:
 - a. Appeals to sympathy
 - b. Playing on emotions
 - c. Overzealous persuasion
 - d. Persistence (wearing down resistance)
 - e. Pressure, coercion, and threats.

804.30 Methods of Payment

Bribery payments can be in many forms and are limited only by the ingenuity of the persons involved in the crime. Some of the more common types of payments include:

(b) (7)(E)



(b) (7)(E)



804.40 Indicators of Bribery Payments

Although not inclusive, the following are some indicators of possible bribery payments the OPM OIG agent should be familiar with:

(b) (7)(E)



804.50 Bribery Investigations

(b) (7)(E)



(b) (7)(E)



Chapter 9

Arrest Procedures

900.00 Arrest Procedures

This section establishes the Office of Personnel Management (OPM), Office of the Inspector General (OIG) policy relating to arrests and prisoner processing by OPM OIG special agents and provides implementing guidelines and procedures..

900.10 Statutory Provisions and References

OPM OIG special agents need to follow policies and procedures for making arrests with or without a warrant. The policies and procedures are in accordance with the following references:

- Federal Rules of Criminal Procedures, Rule 3, The Complaint; Rule 4, Arrest Warrant or Summons upon Complaint; Rule 5, Initial Appearance Before the Magistrate; and Rule 9, Warrant or Summons upon Indictment or Information.
- Title 28, U.S.C., Section 2671(b), popularly known as “The Law Enforcement Officers’ Good Samaritan Act.”

(b) (7)(E)
[Redacted text block]

Warrantless arrests should be made only under exigent circumstances.

900.11 Authority

Section 6 (e) of the Inspector General Act of 1978, as amended in November 2002 by the Homeland Security Act, granted statutory law enforcement authority, including the authority to make arrests with or without warrants, to 24 Offices of Inspectors General, including special agents in the OPM Office of Inspector General.

900.12 Definitions

1. **Custody:** The placing of an individual under arrest, or otherwise restricting the individual's freedom of action in any significant way.
2. **Interrogation:** Any formal or informal questioning in which an incriminating response is either sought or is a reasonable consequence of such questioning; typically the questioning of a suspect.
3. **Interview:** The questioning of an individual who either has or is believed to have factual information, not self-incriminating, that is of interest to the agent. An interview is the questioning of a witness, as compared to an interrogation, which is used to question subject/suspect. See IM 507, Interviews, for further policy and guidance.
4. **Juvenile:** A person under 18 years of age.
5. **Juvenile Delinquency:** A violation of a law of the United States committed by a person prior to his or her 18th birthday that would have been a crime if committed by an adult. A person over 18 years of age but less than 21 years of age is also accorded juvenile treatment if the act of juvenile delinquency occurred prior to his or her 18th birthday.
6. **Minor:** A person under 18 years of age.
7. **Subject/Suspect:** A person whose involvement in the commission of some violation of existing law is considered, on reasonable grounds, to be a practical possibility.

900.13 Training

Prior to being authorized to make arrests, OPM OIG special agents must have completed the entry level training specified at IM 220.10.

900.14 Use of Force

(b) (7)(E)



900.15 Obtaining Arrest Warrants

An arrest warrant may be obtained by filing a complaint or may be issued as a direct result of an indictment or information. Generally, when seeking an arrest warrant, special agents should prepare a complaint and provide it for review, if appropriate, to the Assistant U.S. Attorney (AUSA) assigned to the case. The complaint is then filed before a U.S. magistrate, who will determine if sufficient probable cause exists to issue the warrant.

A complaint is a written statement of the essential facts constituting the offense(s) charged. It is prepared by the complainant, who must swear to its truthfulness while under oath before a magistrate. A complaint contains the following:

1. Name of the suspect.
2. Statutory language of the offense charge.
3. Facts of complainant's charge (a brief synopsis of the investigation explaining how the facts of the case became known to the agent. An affidavit may be used if the synopsis is lengthy).

An arrest warrant contains the following:

1. Name of the defendant. (If unknown, a complete description by which the suspect can be identified with reasonable certainty.)
2. Description of offense.
3. A command that the suspect be arrested and brought before a magistrate.
4. Signature of the magistrate.

An agent need not have a warrant in his/her possession when effecting the arrest, but the agent must show the warrant to the suspect as soon as possible after the arrest and advise the suspect of the charges leading to the arrest.

900.16 Execution of Arrest Warrants

Supervisory Responsibilities:

1. Upon request of a subordinate agent, discuss and approve, if appropriate, the request to seek an arrest warrant. Determine whether the Office of Personnel Management nexus and probable cause exist and, if so, authorize the agent to seek a warrant.
2. Ensure the execution of every arrest warrant is coordinated with the appropriate prosecutor and that it is carefully planned, particularly with regard to the safety of agents, subjects and uninvolved parties.

Special Agent Responsibilities:

1. When the facts of an investigation support a finding of probable cause, discuss the issue with your supervisor to gain his or her approval to obtain an arrest warrant. All arrest warrants must have an operations plan approved by your supervisor or other law enforcement agency.
2. Special agents should make arrests without warrants ONLY when absolutely necessary; e.g., if you are assaulted or if a felony violation occurs in your presence.
3. Determine and comply with procedures of the local U.S. Attorney, U.S. Marshal, and U.S. District Court regarding arrests. When applicable, consult with the prosecutor to determine the timing of the arrest.
4. Plan carefully all arrest situations considering the following:
 - a. Agent safety.
 - b. Public safety.
 - c. Prisoner safety.
 - d. Secure transportation of the prisoner to the magistrate.
5. Contact the local U.S. Marshal Service office to determine the location of and obtain directions to the nearest medical facility that has an authorized ward to hold Federal prisoners in case the arrestee requires medical treatment.
6. Coordinate with local law enforcement agencies.

7. Consider the need for foreign or sign language interpreters and/or an agent of the same sex as the arrestee to conduct a search incident to arrest.
8. Identify yourself by displaying your badge and credentials at the earliest possible opportunity, consistent with safety during the arrest process.
9. Advise the arrestee of his/her constitutional rights if you intend to question the arrestee.

900.17 Search Incident to Arrest

(b) (7)(E) [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted] The term "evidence" includes drugs, drug paraphernalia, stolen property, papers, notes or anything else that could implicate the subject's complicity in a violation of law. The term "contraband" means anything that is inherently illegal (e.g., illicit narcotics, untaxed liquor, counterfeit money, etc.).

Arrest of Opposite Gender Defendants

(b) (7)(E) [Redacted text block]

[Redacted text block]

(b) (7)(E) [Redacted text block]

Arrest within a Dwelling

(b) (7)(E) [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED] (b) (7)

1. **Arrest without a warrant.**

- a. (b) (7)(E) [REDACTED]

2. **Arrest with a warrant.**

- a. (b) (7)(E) [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

900.18 Arrest and Search in/near a Vehicle

(b) (7)(E) [REDACTED]

(b) (7) (E)

900.19 Inventory

Inventory the personal property of the prisoner at the first appropriate opportunity. If the prisoner was arrested in or near a motor vehicle, secure it at the scene or arrange for its safe storage with the local law enforcement agency. Vehicles should be stored at a secure location or a facility used by other law enforcement agencies. If adequate facilities are unavailable, contact the U.S. Marshal to arrange for storage. Make every effort to avoid assuming custody of vehicles, unless warranted by circumstances of the arrest.

Inventory all vehicles and their contents, and all other property taken into custody. Conduct an inventory to:

- Protect the owner's property while in Government custody.
- Protect the Government against claims of lost, stolen, or vandalized property.
- Protect OPM and other personnel from potentially dangerous items.

The inventory shall be conducted at the time of the arrest, or as soon thereafter as circumstances allow, and shall consist of opening all compartments, including locked or closed containers, and cataloging all items found. An inventory list shall be prepared.

1. Vehicle inventory lists should include, but not be limited to, the following:
 - a. Description of the vehicle (year, make, model, color, vehicle identification number, license number).
 - b. Description of all valuables secured from a vehicle for safekeeping.
 - c. List of all accessories, tools, and unattached parts left in the vehicle.
 - d. Notation describing the condition of the body and upholstery (specifically naming the damage or deteriorated areas and briefly stating the extent of the damage).
 - e. List of all missing items such as keys, motor, radio, battery, spare tire, etc.

2. Place the original inventory list in the investigative case file with a copy attached to or left with the property, a copy provided to the representative of the storage facility, an a copy provided to the person from whom the property was seized.
3. Minimize damage to a container or its contents while gaining access, in the event a container or vehicle compartment is locked or sealed.
4. Seize all property discovered in the course of a property inventory that constitutes contraband or evidence of a crime. Follow proper evidence handling, inventory and receipt procedures for any evidence or contraband seized.

900.20 Prisoner Processing

Custody of Prisoners: Special agents making an arrest are responsible for the protection and safe custody of defendants until custodial transfer to another agency has been completed. It is important to keep a record of the movement and detention of prisoners and any unusual circumstances occurring during this time.

1. Handcuffing prisoners

- a. (b) (7)(E) [REDACTED]
- b. (b) (7)(E) [REDACTED]

2. Medical treatment

- a. (b) (7)(E) [REDACTED]
- b. (b) (7)(E) [REDACTED]

(b) (7)(E)
[Redacted]

3. Processing Prisoners

a. (b) (7)(E)
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) [REDACTED]
(7)(E)

[REDACTED]

[REDACTED]

910.00 Juveniles

(b) (7)(E) [REDACTED]

1. Arrests

a. (b) (7)(E) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

2. Interviews and Interrogations

(b) (7)(E)

[Redacted]

[Redacted]

[Redacted]

a. Interviews

[Redacted]

b

(b) (7)(E) [Redacted text block]

b. Interrogations

(b) (7)(E) [Redacted text block]

3. Juvenile Witnesses

(b) (7)(E) [Redacted text block]

4. Parental Notification

a. (b) (7)(E) [Redacted text block]

(b) (7)
(E) [Redacted]

5. Photographing and Fingerprinting

a. (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

6. Polygraph Examination

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

7. Publicity

- a. Press releases and other publicity identifying a juvenile directly or indirectly are not permitted under 18 U.S.C. § 5038.
- b. If a person is belatedly determined to be a juvenile (after publicity or indictment) and if a hearing on a motion to transfer the juvenile to adult status is not imminent, all efforts should be made to minimize further publicity.

8. Release of Information

(b) (7)(E)
[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

9. Search and Seizure

As a general rule, parents may consent to the search of a family dwelling directed against juveniles residing therein and being supported by the parents. On the other hand, since Fourth Amendment protection belongs to the parents, juveniles may not relinquish the parents' rights by consenting to a search of the family home directed against them.

10. Sources

- a. The use of sources in law enforcement is both a time honored and constitutionally accepted method of collecting information and identifying substantive criminal activities.

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

11. Titling of Juveniles and Entering Information in the ITS

- a. (b) (7)(E) [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

920.00 Foreign Nationals

When foreign nationals are arrested or detained, they must be advised of their right to have their consular officials notified. In some cases, the nearest consular officials must be notified of the arrest or detention of a foreign national, **regardless of the national's wishes**.

Consular officials are entitled to have access to their nationals in detention, and are entitled to provide consular assistance.

When a government official becomes aware of the death of a foreign national, consular officials must be notified.

When a guardianship or trusteeship is being considered with respect to a foreign national who is a minor or incompetent, consular officials must be notified.

(b) (7) (E)
[Redacted]

[Redacted]

930.00 Non-Federal Crimes

(b) (7) (E)
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E)

[Redacted text block]

[Redacted text block]

[Redacted text block]

Chapter 10

Weapons, Protective Equipment, Security, and Critical Incident Response

1000.00 Background

(b) (7)(E)

(b) (7)(E)

This section also explains OI policies in the event of a critical incident.

1000.10 Violations

Violation of OPM OIG firearms policies and procedures or applicable Federal, State, or local law is a serious offense. Personnel violating these regulations may be subject to disciplinary action.

1000.11 Definitions

1. "DEADLY FORCE": Is force that is reasonably likely to cause death or serious physical injury.
2. "REASONABLE BELIEF": Is synonymous with "Probable Cause." It is determined by a totality of the facts and circumstances known to agents at the time, and the logical inferences that may be drawn from them.
3. "NECESSARY": The necessity to use deadly force based on the existence of a reasonable belief that the person against whom such force is used poses an imminent danger of death or serious physical injury to the agent or other persons.
4. "IMMINENT DANGER": "Imminent" does not mean "immediate" or "instantaneous", but that an action is pending. Thus, a subject may pose an imminent danger even if he is not at that very moment pointing a weapon at the agent. For example, imminent danger may exist if special agents have probable cause to believe any of the following:
 - a. The subject possesses a weapon, or is attempting to gain access to a weapon, under circumstances indicating an intention to use it against the SA or others; or,
 - b. The subject is armed and running to gain the tactical advantage of cover; or,

- c. A subject without a deadly weapon, but with the capability of inflicting death or serious physical injury, is demonstrating an intent to do so; or,
 - d. The subject is attempting to escape from the vicinity of a violent confrontation in which the suspect inflicted or attempted the infliction of death or serious physical injury.
5. "CRITICAL INCIDENT": Any situation faced by law enforcement/emergency service personnel which has a stressful impact sufficient enough to overwhelm the usually effective coping skills of either an individual or a group. The event may have the potential to interfere with the ability to function either at the scene or later. If the incident is extreme in nature, it may serve as the starting point for Post-Traumatic Stress Disorder.

1000.12 Use of Force Policy

(b) (7)(E)



(b) (7)(E)

1000.13 Application of the Use of Force

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

1. SA's will immediately report to their Supervisor or other designated OIG personnel, any incident involving the use of force.
2. (b) (7)(E)
3. All Special Agents (SAs) are required to have periodic training on the Use of Force / Use of Deadly Force Policy, Methodology, and Legal requirements.
4. Any use of force, deadly force or less than deadly force, must be justified under OI policy in conjunction with the Federal Law Enforcement Training Center (FLETC), Use of Force Model, as adopted by the OI.
5. (b) (7)(E)

SA's supervisor must be notified immediately by the SA and by any other employee witnessing the event, and;

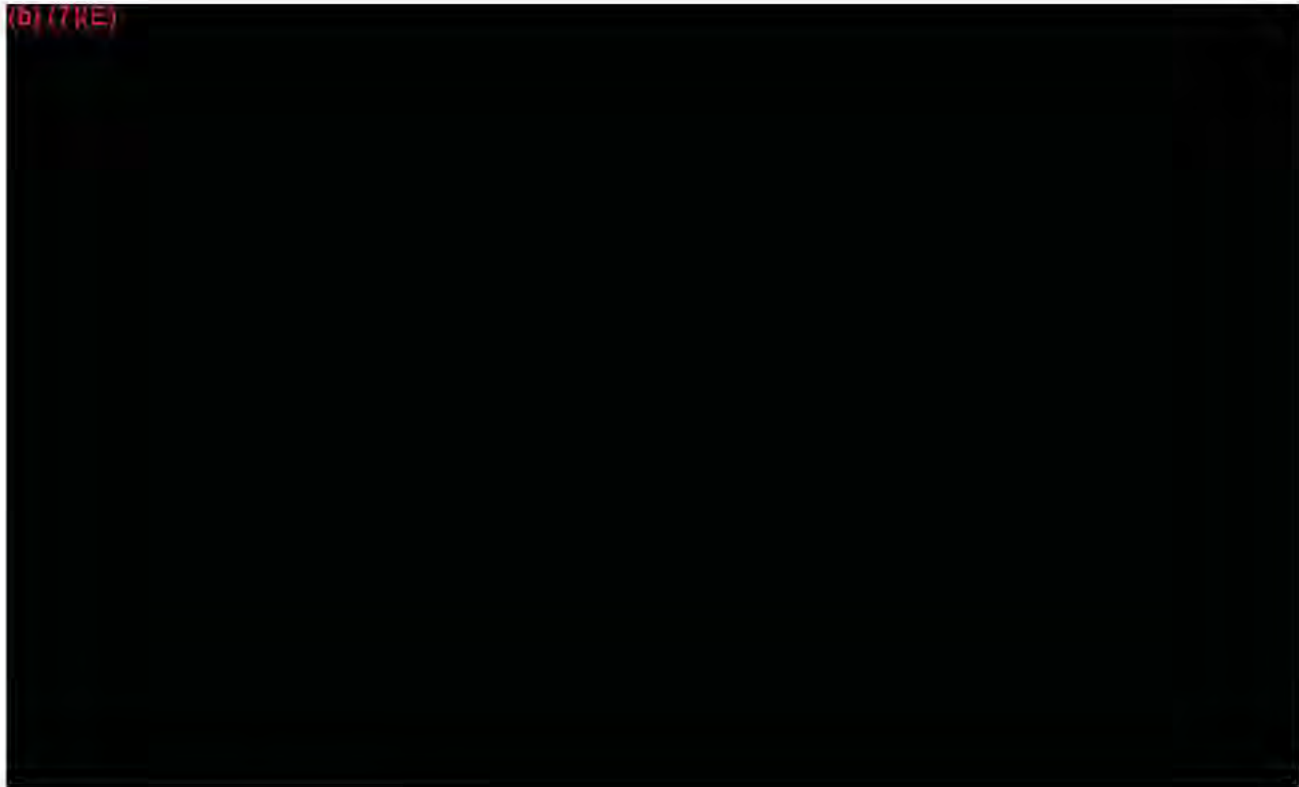
- a. The AIGI or other designated personnel will evaluate each incident separately to determine whether the actions were appropriate.
 - b. If the actions were considered questionable, the AIGI or other designated personnel will provide the SA with corrective guidance.
6. If a violation of guidance set forth in this Chapter or other OI policy has occurred, an inquiry will be initiated by the SAC at the direction of the AIGI, which may result in disciplinary action against the SA, if it is found that the SA violated OI regulations or applicable laws.

1000.14 General Policies

(b) (7)(E)



(b) (7)(E)



1000.15 Firearms Training

SAs are responsible for meeting all proficiency, training, and safety standards for assigned firearms.

1. **New special agents:** Prior to being issued a firearm and before being authorized to carry a firearm in the performance of their duties, all new agents must meet the following criteria:
 - a. Complete the (b) (7)(E) or equivalent.
 - b. Receive instruction in the OI Use of Force Policy and all requirements of this chapter.
 - c. (b) (7)(E)
2. **Special agents**
 - a. Quarterly Qualification

(
b
)
)
)
(
E
)
[Redacted text block]

3. Firearms Coordinator

The responsibilities of the Firearms Coordinator will be to:

- a. Receive and maintain quarterly and monthly reports regarding SA qualifications.

- b. Issue all authorized OI weapons including firearms, magazines, ammunition, and other related firearms equipment to each SA.
- c. Ensure that records are maintained for OI issued firearms, ammunition, and related equipment.
- d. The Firearms Coordinator shall be a certified firearms instructor whose duty station is OI Headquarters and shall be designated by the AIGI.

4. Firearms and Tactical Needs Committee

Established is a Firearms and Tactical Needs Committee comprised of each certified and qualified OI Firearms Instructor, Control Tactics Instructor, Active Shooter and Use of Force Instructor.

The purpose of the committee is to:

- a. Review, assess, update and suggest changes to firearms and control tactics related policy.
- b. Review, assess, update and suggest changes to firearms, tactical and officer safety related equipment.
- c. Collaborate on training goals and establish firearms and control tactics related training to meet established goals and the OI Mission.

5. Record Keeping

- a. Information on each qualification will be maintained by the Firearms Coordinator and each regional ASAC.
- b. The ASACs will prepare a quarterly memorandum by the tenth day first month of the new quarter advising the Firearms Coordinator of those SAs who have and have not qualified during the prior quarter. The memorandum will also contain information as to the number of SAs who have qualified during that new quarter. The ASACs or regional firearms instructors will also prepare monthly memorandums to the Firearms Coordinator with the same information as the quarterly memo.

6. Failure to Qualify

SAs who fail to achieve a qualifying score during the quarter will not be authorized to carry a firearm until such time as they qualify. The SA will be required to surrender their firearm to an OI firearms instructor immediately, or as soon as possible if an OI firearms instructor

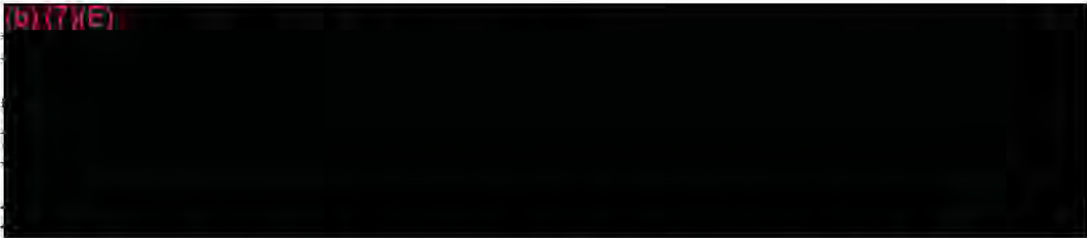
is not present at the qualification session.

- a. Remedial training will be provided as needed to assist the SA to obtain a qualifying score.

7. Excused Absence from Quarterly Qualification

- a. In the event that an SA is unable to attend firearms qualification during a quarter due to operational necessity, temporary medical condition, or other extraordinary circumstance, an excused absence may be permitted.
- b. The excused absence must be in writing and approved by the AIGI. The approved excused absence will be filed with the office shooting records.
- c. An SA will not be excused from qualifying for more than one consecutive quarter; if the SA does not qualify in the next quarter, the SA must surrender their weapon. The SA will then qualify as soon as practical, at which time the weapon will be returned.

8. Medical Conditions and/or Physical Limitations

- a. (b) (7)(E)

- b. The medical and/or physical limitations must be documented in writing by a medical professional, approved by the AIGI, and retained in the shooting/firearms records.
- c. Recovery from the medical/physical limitations will also be documented in writing, and the SA will then qualify as soon as practical. The weapon will be returned upon qualification.
- d. As it pertains to any SA whose medical condition requires limited or no exposure to lead or lead products, the agency will make reasonable accommodations for the SA to qualify at a lead-free firearm range using lead-free ammunition, or at an approved simulation training facility, such as a Range 3000.

(b) (7)(E) [Redacted]

1000.16 Weapons Issuance and Security

In this section, (b) (7)(E) [Redacted]
(b) (7)(E) [Redacted]

1. The OI Firearms Coordinator issues all firearms, magazines and ammunition. The headquarters defensive tactics instructor will issue (b) (7)(E) [Redacted]
(b) (7)(E) [Redacted]
2. The OI Firearms Coordinator will ensure that (b) (7)(E) [Redacted]
(b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

1000.17 Carrying and Concealing Weapons

(b) (7)(E) [Redacted]

(b) (7)(E)

A large black rectangular redaction box covers the top portion of the page.

(b) (7)(E)

A very large black rectangular redaction box covers the majority of the page's content.

(b) (7)(E)



1000.19 (b) (7)(E) - Prohibited Actions

- (b) (7)(E) [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

(b) (7)(E)

(b) (7)(E)

1000.22 Use of Force Resulting in Physical Injury

1. General Guidelines

- a. SAs who cause physical injury by any use of force will immediately seek emergency medical treatment for those persons injured and will render first aid, as appropriate.
- b. When Use of Force incidents result in death, serious physical injury, or property damage, SAs will notify local law enforcement authorities of the incident and

location as soon as it is reasonably possible to do so. If the SA involved is physically unable to report the incident, notification shall be made by any OIG personnel aware of the incident.

- c. SAs or, if physically unable, any OIG personnel aware of the incident, will immediately report the incident to his/her supervisor regardless of time of day. This will be followed by a written report of the incident by the SA using the Critical Incident Report (See **Appendix L**). The Critical Incident Report shall be completed as soon as possible, with the understanding that it is considered a “Statement” for purposes of Sections 1000.23D and E.3 of this manual.
- d. OIG personnel who are injured as a result of a use of force encounter must report this injury on an OWCP Form CA-1 to their supervisor or other designated OIG personnel.
- e. An SA involved in a Use of Force incident resulting in death or serious physical injury will immediately be placed on administrative leave or special duty status, as appropriate, pending the results of appropriate inquiries into the incident.

2. Reporting

The supervising SAC or other designated OIG personnel will immediately notify the AIGI of the incident, and will furnish the AIGI with all available basic information relevant to the incident. Such information may include:

- a. The name of the SA(s) involved, case assignment, and a general description of the activity in which the SA(s) was involved at the time of the incident (e.g., interview, protection, search, arrest, etc.).
- b. Date, time, and place of the incident.
- c. Description of the weapon used, including serial number, type and number of rounds fired in the case of a firearm, where applicable.
- d. Injuries caused or received.
- e. Any Property damage and description.
- f. Names of any persons arrested, current custodian of arrestee(s), and list of offenses charged.
- g. Description of the weapon used by the offender.

- h. Identification of any persons witnessing the incident.
- i. Involvement of other law enforcement agencies, either directly in the incident itself, or in the investigation of the incident.
 - i) It is understood that some of the basic information listed above may not be available until after the supervising SAC or other designated personnel has arrived at the scene, coordinated with other law enforcement agencies responsible for investigating the incident and/or reviewed the Critical Incident Reports prepared by the involved SAs. It is the responsibility of the supervising SAC or other designated personnel to keep the AIGI informed on a continuing basis as more facts become available. The supervising SAC or other designated personnel shall prepare a memorandum for the AIGI summarizing the basic information listed above once all the information has been obtained. This memorandum is separate and distinct from the post-incident administrative inquiry addressed in Manual Section 1000.24.

1000.23 Critical Incident Response Procedures

The following guidance assumes that an OPM/OIG SAC or other designated supervisory personnel will arrive at the scene shortly after a critical incident. (b)(7)(E)

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

ii) (b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

2. Cooperation with investigating agencies

a. (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

f. (b) (7)(E) [Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

3. Support for Families

a. SAs involved in any critical incident should notify their families about the incident as soon as practical. (b) [Redacted]

(7)(E) [Redacted]

b. If an SA has been injured, (b) (7)(E) [Redacted]

[Redacted]

4. Injured Agent Procedures

(b) [Redacted]
(7) [Redacted]
(E) [Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

■ (b) (7)(E) [Redacted]

5. **Line of Duty Death:** (b) (7)(E) [Redacted]

6. Post-Incident Counseling

- a. Post-trauma stress counseling and/or intervention, including but not limited to that provided by the Employee Assistance Program (EAP) (1000.25), shall be made available to SAs involved in any critical incident, incident resulting in serious physical injury and/or any other use of force incident.
- b. Participation in a post-traumatic stress counseling program shall be mandatory when the incident resulted in a fatality or serious physical injury. Participation may be discretionary if the incident did not result in a fatality or serious physical injury.
- c. If counseling is mandatory, the SA should initiate the appropriate contact within a reasonable amount of time after the incident occurred.

7. Dissemination of Information/Media Contact

- a. OI personnel should be informed of the ongoing situation. (b) (7)(E) [Redacted]
- b. OI personnel are prohibited from communicating with the media. No information concerning any incident or injury shall be released to anyone outside the OI, except the appropriate law enforcement authorities, without the expressed approval of the IG. All media inquiries must be directed to the IG or the agency's designated Media Relations personnel.
- c. OIG policy is not to disclose to the media or otherwise make public the identity of SAs involved in critical incidents. The IG will consider the interest of the SA(s) involved prior to issuing any media releases.

1000.24 Post-Incident Administrative Inquiry

The AIGI at his/her discretion may dispatch a fact-finding team to conduct a thorough investigation and prepare a report concerning any critical incident, regardless of the circumstances.

The AIGI in consultation with the appropriate SAC or other designated supervisory personnel will determine the composition of the administrative inquiry team. (b) (7)(E)

[REDACTED]

(b) (7)(E)

The administrative inquiry shall be completed as expeditiously as possible, and the SA(s) involved in the incident will be advised of the outcome.

(b) (7)(E)

1000.25 Employee Assistance Program (EAP)

The EAP in OPM is a professional confidential counseling program designed to assist all OPM employees (and, in some situations, family members) with various personal problems. OIG employees do not require supervisory approval prior to contacting EAP for assistance with personal problems.

An SA involved in a critical incident or use of force incident is encouraged, and in some cases may be required (See 1000.23.I), to request counseling through the EAP. The affected SA will contact EAP for a referral to a counselor near his/her location. The SA and the counselor will then arrange to meet to conduct a critical incident stress debriefing and/or post-trauma stress counseling, as appropriate. With respect to critical incidents, EAP counseling will be made available at no cost to the employee involved.



UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

OFFICE OF
THE INSPECTOR GENERAL

(b) (7)(E)



(b) (7)(E)

We are confident that you will continue to conduct yourselves, both on and off-duty, in the professional and careful manner that you have in the past.



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

(b) (7)(E)



(b) (7)(E)



Attachment

(b) (7)(E)

[Back to Table of Contents](#)

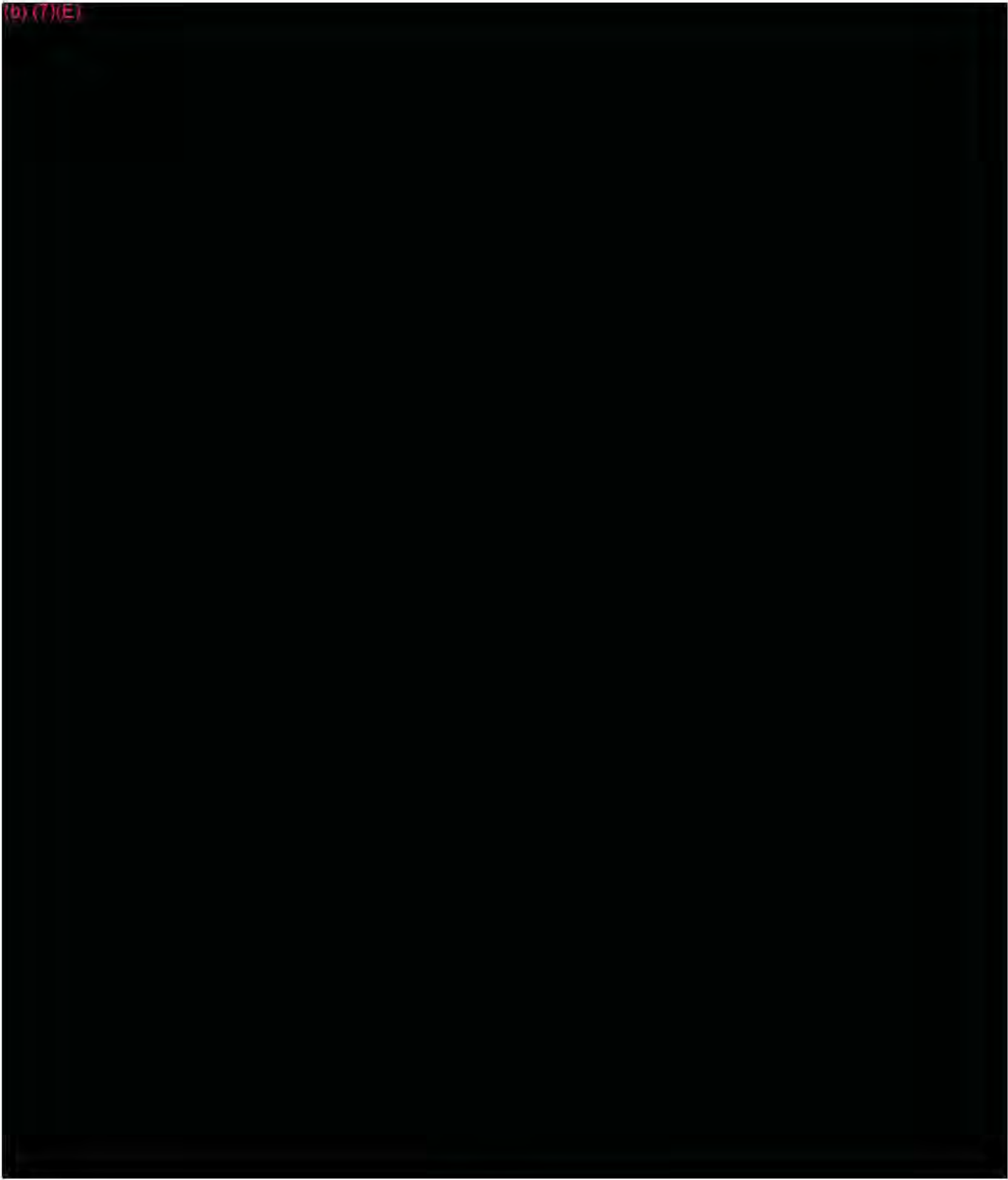
(b) (7)(E)



(b) (7)(E)



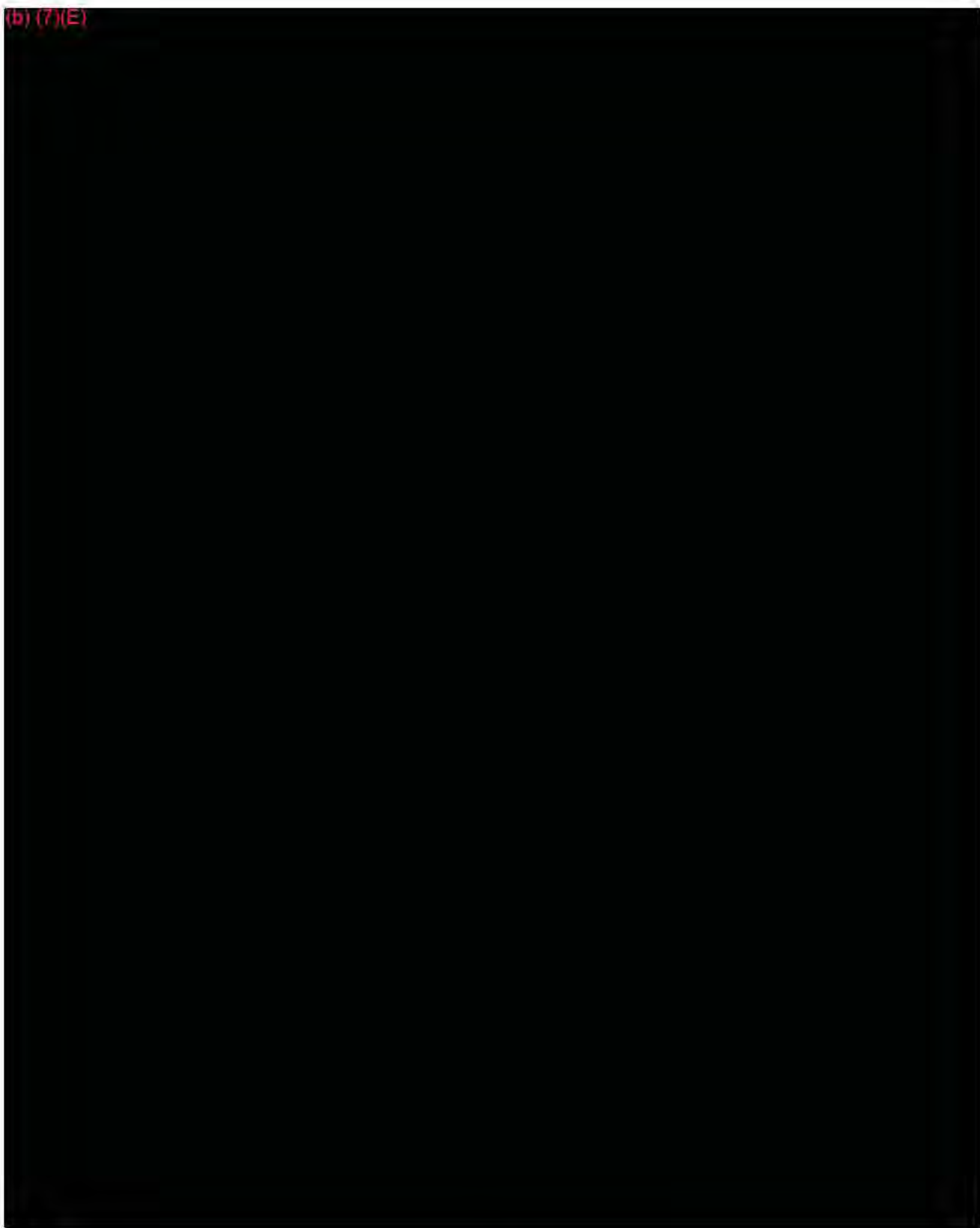
(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



-5-



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

CRITICAL INCIDENT REPORT

Date: _____ Time: _____ Name: _____

Region: _____ SAC: _____

Is the incident described herein the result of Use of Force? YES () NO ()

If NO, Please go to Section II

SECTION I

Use of Force Factors:

Facts:

1. Severity of the Crime:

2. Suspect Immediate Threat to
Safety of Agent(s)/Officer(s):

3. Suspect Immediate Threat to
Safety of Others:

4. Suspect Actively Resisting Arrest:



OFFICE OF
THE INSPECTOR GENERAL

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, DC 20415-1100

CRITICAL INCIDENT REPORT

Date: _____ Time: _____ Name: _____

Region: _____ SAC: _____

Is the incident described herein the result of Use of Force? YES () NO ()

If NO, Please go to Section II

SECTION I

Use of Force Factors:

Facts:

1. Severity of the Crime:

2. Suspect Immediate Threat to
Safety of Agent(s)/Officer(s):

3. Suspect Immediate Threat to
Safety of Others:

4. Suspect Actively Resisting Arrest:

**5. Suspect Attempting to Evade
Arrest by Flight:**

6. Number of Suspects Involved:

7. Number of Agents/Officers Involved:

**8. Size, Age & Physical Condition of
Agent(s)/Officer(s):**

**9. Size, Age & Physical Condition of
Suspect(s):**

10. Warning Feasible:

Tools Used (b) (7)(E) _____

TOTALITY OF CIRCUMSTANCES:

a. Duration of Action: _____

b. Did Force Applied Result in Injury: _____

c. Previous Violent History of Suspect (known to Agent/Officer at Time of Incident): __

d. Suspect Using or Under Influence of Alcohol or Drugs:

e. Suspect Mental or Psychiatric History (known to Agent/Officer at Time of Incident):

f. Innocent Bystanders Present Who Could Have Been Harmed If Force Not Used: ____

(b) (7)(E) _____

h. Any Other Relevant Facts: _____

Other Factors: Check All That Apply

- Inability to Disengage _____ Previous Assaults by Subject _____
- Confinement _____ Subject(s) Criminal HX _____ Close Proximity to
- Weapons _____ Sudden Attack _____ Known Fighting Ability _____
- Injury to Agent/Officer _____ Body Size Disparity _____
- Exhaustion of Agent/Officer _____ Presence of Bystanders _____
- Evading Arrest by: _____ Flight _____ Stealth _____ Hiding
- Agent/Officer on Ground _____ Engaged in Protest Activity _____
- Riot/Mob _____ Bloodborne Pathogens _____ Daylight _____
- Nighttime _____ Remote Location _____
- Winter _ Snow _ Ice _____ Rain _____ Summer _____
- Extreme Heat _____ Lack of Physical Compliance _____ Multiple Subjects _____
- Subject Inability to Comply _____ Residential Area _____ Commercial Area _____
- Involvement of Heights _____ Involvement of Speed/Vehicle _____ Urban Area _____
- High Crime Area _____ Water Environment _____ Fog/Haze/Smoke _____
- Fire _____ Secured Environment _____ Unstable Ground Cover _____
- Rural/Remote Area _____ Steep or Treacherous Terrain _____
- Guard Attack Animal(s) _____ Large Group Event _____ Armed Subject(s) _____
- Verbalization of Harm _____ Mentally Unstable _____

Remarks (Articulate Any Facts Checked Above): _____

WITNESSES:

- | | |
|----------|-----------|
| 1. _____ | 2. _____ |
| 3. _____ | 4. _____ |
| 5. _____ | 6. _____ |
| 7. _____ | 8. _____ |
| 9. _____ | 10. _____ |

NARRATIVE SUMMARY BY EMPLOYEE:

I certify that the above listed information is true and correct:

Name of Agent / Officer (Print)

Signature of Agent/Officer

Date

I certify that the above listed information is true and correct:

Name of Agent / Officer (Print)

Signature of Agent/Officer

Date of Signature

Chapter 11

Reports of Investigation

1100.00 Reports of Investigation - General

The results of each investigation are documented either in a Report of Investigation (ROI), Attorney Report (AR), Transmittal Memorandum (TM), or Management Advisory Report (MAR). The Report of Investigation and the Attorney Report are the standard method for documenting and communicating investigative findings. The only difference is that the ROI is used internally to report investigative findings upon the close of the case. The Attorney Report is identical in format to the ROI with the exception that there is no case disposition section. The AR is submitted to the United States Attorney's Office for review and consideration of criminal prosecution or civil violations.

A Transmittal Memorandum is used to communicate investigative findings to OPM officials for information or administrative action. A Transmittal Memorandum is used in lieu of a Report of Investigation when the investigation relates to employee misconduct that does not constitute a criminal violation, prosecution has been declined, or review of the allegation does not establish sufficient factual basis for further OIG criminal, civil or administrative investigation, but indicates that a referral to an official of OPM or another Government agency is appropriate.

The MAR is used when an OIG investigation identifies problems that require the immediate attention of the program office. When investigations involve OPM components, programs, or employees, OPM OIG must address whether a lack of management controls, inadequate compliance with those controls, or a deficiency within the system allowed waste, fraud, or abuse to occur or to go undetected. The issues documented in the MAR may or may not be directly related to the allegations under investigation. Depending on the urgency of the issue(s) identified, the MAR may be issued prior to completion of the investigation. This report is used in addition to or as a supplement to the Report of Investigation.

1110.0 Report Standards

Each OIG investigative report, whether a ROI, AR, TM, or MAR must be clearly and concisely written to:

- Present factual data fully, accurately, and objectively. Any findings shall include any exculpatory material.
- Present factual investigative findings, supported by sufficient evidence to demonstrate their accuracy and reasonableness.

- Present factual investigative findings that are comprehensive to support a conclusion on the allegation/violation.
- Investigative reports can be distributed only to the appropriate officials for action, and must have the following statement listed on the bottom of the last page:

WARNING: This document is the property of the United States Office of Personnel Managements, Office of the Inspector General, and is on loan to your office. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving office without specific prior authorization of the Assistant Inspector General for Investigations.

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Investigative reports are to be reviewed and approved by the special agent's immediate supervisor or SAC prior to issuance to the United States Attorney's Office for prosecution consideration or for final case closure approval.
- Investigative reports should be prepared in a timely manner. (See IM 430.13.)

1110.10 Planning and Care in Report Writing

In preparing an investigative report, the special agent should be aware that the report could be released for a variety of purposes. All or portions of a Report may be disclosed before or during a trial, under discovery proceedings.

An investigative report may also be released in whole or in part in response to a congressional request, a Freedom of Information Act request, or an adverse action or other administrative proceeding.

Because of the potential for close scrutiny, the report should only include the essential facts of the case. The report should not refer to third parties, or include opinions or rumors, unless they are relevant to the investigation and are so identified. The special agent should use proper English language format and check for spelling errors.

1120.00 Report of Investigation Format

The following format should be used to report findings on OIG investigations. (Reports of Investigation are not required for complaints or proactive projects. See IM 420.20 and 420.40.) Information in a report should be organized in a logical and easy to understand fashion. When appropriate, the report should be presented in the chronological sequence of the investigation, or the events.

Longer reports, and those on complex or extensive cases, may be organized other than chronologically if clarity would be improved. For example, the report in a case involving several allegations could be organized by the individual allegations. A case involving allegations against a number of individuals or contractors could be organized according to the individual or contractor.

The report should be no longer than necessary to ensure a complete, accurate presentation of the facts of the case and the results of the investigation. The report should exclude unnecessary or extraneous information. For example, information on the number of times a special agent visited a location before a witness or subject could be interviewed should be omitted from the investigative report unless such information is pertinent to the findings of the investigation.

Appropriate laws, regulations and publications should be summarized in the body of the report and attached to the report as exhibits. All information from an Official Personnel Folder (OPF) must directly pertain to the matter under investigation to be included in a report.

When identifying an individual for the first time in a report, his or her full name should be used. In subsequent references the individual can be referred to by last name and title, i.e., Dr. Jones, Mr. Smith, etc. When identifying government employees, business or professional people for the first time, include their titles.

When identifying the subject(s) or target(s) of your investigation for the first time in a report, his or her first and last name should be used and all letters capitalized, i.e. JOHN SMITH. In subsequent references, the subject(s) or target(s) of investigation can be referred to by last name with all letters capitalized, i.e. MR. SMITH, DR. SMITH. This capitalization of all letters in the subject(s) or target(s) name acknowledges a separation between subject/target and witness.

If any technical, medical, or scientific terms are used, they should be followed with an immediate parenthetical layman's explanation. Likewise any slang, jargon, or colloquialisms used by a witness or subject should be explained. Acronyms and sets of initials should be preceded by the complete phrase the first time they appear.

1130.00 Report of Investigation Content

The Report of Investigation contains the following sections:

- Case Agent Name
- Date
- Introduction / Title (Report of Investigation)
- Program Overview
- Basis of Investigation
- Statutes Violated (or Relevant Statutes)
- Case Summary

- Conclusion/Disposition
- Approvals
- Subjects of Investigation
- Attachments, if necessary

The following paragraphs describe the contents of each section in a Report of Investigations. **A sample Report of Investigation follows the section on writing style.**

1130.10 Introduction

The introduction is one short paragraph that identifies the target(s), summarizes the allegation(s), and identifies the OPM program involved in the investigation. An example of the introduction statement follows:

The following report of investigation relates to information that JOHN DOE fraudulently obtained government retirement annuity payments from the United States Office of Personnel Management (OPM), Civil Service Retirement System (CSRS), after the annuitant, Jane Doe, died on November 15, 1996.

The above paragraph simply tells the reader who the target is, what the case is about, and what program is involved.

1130.20 Program Overview

This section briefly describes the OPM program involved. Depending on the type of case, this section will change. OIG investigations frequently involve one of the following OPM programs; the Federal Employees Health Benefits Program (FEHBP), the Civil Service Retirement System (CSRS) / Federal Employees Retirement System (FERS), the Combined Federal Campaign (CFC), and the Federal Investigative Services (FIS).

Below are sample Program Overviews for these programs.

1. FEHBP – Health Care Fraud Cases

The U.S. Office of Personnel Management (OPM), Office of Inspector General (OIG) is responsible for preventing, detecting, and investigating fraud affecting programs operated and administered by OPM, including the Federal Employees Health Benefits Program (FEHBP). The FEHBP was established by the Federal Employees' Health Benefits Act (Public Law 86-382) on September 28, 1959. The provisions of the Act are implemented by OPM through regulations codified in Chapter 1, Part 890 of Title 5, Code of Federal Regulations. The FEHBP is a federally funded medical insurance program created to provide health insurance for federal employees, annuitants, and their spouses and dependent unmarried children under the age of twenty-six. Health insurance coverage is

made available through contracts with various health insurance carriers, and federal employees and annuitants can choose from a wide variety of insurance plans. The federal Government pays about 70% of the average health insurance premium. The insurance premiums paid by the Government and by employees/annuitants are deposited into the Federal Employees Health Benefits Fund, a trust fund account maintained at the US Treasury and administered by OPM. In this case, the affected FEHBP insurance carriers were the Government Employees Hospital Association (GEHA), the Mail Handlers Benefit Plan (MHBP), and the Blue Cross and Blue Shield Federal Employees Program (BCBS).

2. CSRS / FERS – Retirement Fraud Cases

The OPM Office of Inspector General (OIG) is responsible for preventing, detecting, and investigating fraud affecting programs operated and administered by OPM, including the Civil Service Retirement System (CSRS).

CSRS benefits are afforded to Federal employees, known as the “annuitant”, upon retirement from civil service. The annuitant receives CSRS benefits throughout his/her lifetime. Prior to retirement, the annuitant has the option to choose a spousal benefit. If the spousal benefit is selected, upon the annuitant’s death, CSRS benefits are payable to the surviving spouse. There is no benefit for the surviving children (unless incapable of self-support due to a mental or physical disability that existed prior to age 26).

3. CFC – Combined Federal Campaign Fraud Cases

The U.S. Office of Personnel Management (OPM), Office of Inspector General (OIG) is responsible for preventing, detecting, and investigating fraud affecting programs operated and administered by OPM, including the Combined Federal Campaign (CFC).

The CFC receives very little government funding, yet the program provides millions of dollars annually to local, national, and international non-profit organizations and charities worldwide. The funds are contributed by Federal employees. OPM OIG maintains an audit and oversight function of the collected CFC funds to safeguard the program from embezzlement, fraud, and misappropriation.

4. FIS – Federal Investigative Services

The U.S. Office of Personnel Management (OPM), Office of the Inspector General (OIG) is responsible for preventing, detecting, and investigating fraud within programs operated and administered by OPM, including the Federal Investigative Services (FIS). The OPM mission is to ensure that the Federal Government has an effective civilian workforce. FIS is responsible for conducting background investigations for most federal agencies and their contractors, for the purposes of security clearance and suitability determination. FIS

supports OPM's mission by protecting merit system hiring principles; ensuring the suitability of federal applicants, employees, and appointees; and conducting investigations of individuals who work in positions that have access to classified information.

The authority to conduct background investigations is contained within various Executive Orders, Title 5 United States Code (5 U.S.C.), and Title 5 of the Code of Federal Regulations (5 CFR). Specifically, but not exclusively, Executive Order 10450, as amended, requires agency heads to classify positions for sensitivity in relation to National Security. Executive Order 10450, as amended, further requires an investigation appropriate to the sensitivity level on each person in order to determine that the employment is consistent with the interests of National Security, and grants OPM Government-wide oversight responsibility of its implementation. OPM, under 5 CFR Part 5, is authorized to investigate the suitability of individuals entering the competitive Federal service, with suitability determinations normally made by the hiring agency.

1130.30 Basis of Investigation

The basis of investigation is a short one to three-paragraph section in which the case agent identifies the specific allegation or details of the complaint. If appropriate, he/she may identify who or what entity made the complaint, and who assigned the case. The following is an example:

(b)(7)(E)



1130.40 Statutes Violated

This section is where the special agent identifies the specific statutes relevant to the investigation by title, code, and name. The following is an example:

As to JOHN DOE:

Title 18 U.S.C. §1341	Mail Fraud
Title 18 U.S.C. §1347	Health Care Fraud

Note: "Statutes Violated" is the appropriate name for this section if evidence exists to substantiate the allegations. However, if the allegations are not substantiated, then this section may be named "Relevant Statutes."

1130.50 Case Summary

The case summary is where the agent reports, in a logical and orderly fashion, the chronological account of the facts developed through interviews, examination of records, and other investigative techniques, including the results of NCIC and other records searches. The basis of investigation may be repeated in this section as the initiation of the case. When reporting that an interview was performed, analysis of records, NCIC results, etc., the pertinent facts related to these actions should be summarized in one or two short paragraphs.

In some instances the OPM/OIG may have limited involvement in joint investigations, such as providing health care claims data to another agency or the United States Attorney's Office in support of civil or criminal violations uncovered by another agency. In cases where only limited involvement was necessary, the case summary can be a short overview of the case allegations, what agency performed the majority of the investigation, any utilized investigative techniques, and the findings. When any pertinent judicial or administrative action takes place that may affect an OPM program, i.e. debarment of a provider, restitution, the agent should obtain a copy of the signed criminal and/or civil complaints filed with the court and attach these documents to the report of investigation.

When the investigation involves a number of allegations or subjects, this section may be arranged according to issues, allegations, or subjects, rather than chronologically. However, regardless of the order, the facts pertinent to the case must be presented in a succinct, logical and orderly manner. The "who, what, when, where, how, and why" questions should always be addressed.

1130.60 Conclusion/Disposition

The conclusion/disposition briefly summarizes what statutes were violated and reports the final status of the case. This section should also be used to report any prosecutorial, judicial, or administrative actions, such as suspension/debarment, adverse personnel actions, indictments, arrests, plea agreements, settlement agreements, trials, convictions, court orders, and sentences.

If there is a declination by the U.S. Attorney's Office, a copy of the declination letter should be included as an attachment to the report and reported in this section.

1130.80 Approvals

The approvals consist of signature blocks for the special agent and the Special Agent in Charge (SAC) to indicate their approval of the report. Although this section would not be included with an attorney report, the special agent must submit the attorney report to his/her immediate supervisor (SAC) for review and approval prior to distribution.

1130.90 Subjects of Investigation

The subject of investigation section is to report all pertinent information related to the subject(s) or target(s). This section will include full names, any aliases or "also known as" (AKA) names, dates of birth, social security numbers, driver's license numbers, current and former addresses, fingerprint identification, FBI numbers, and a summary of any past criminal history or other pertinent information.

1130.91 Attachments

Attachments are the exhibits, affidavits, statements, interview reports, declination letters, copies of subpoenas, etc., which have been referred to in the body of the report. For Final Reports of Investigation submitted internally to the agent's immediate supervisor for approval to close the case, it is not necessary to attach any documents already in the Investigative Tracking System (ITS) (example, Memoranda of Interview) or in the hardcopy case file. However, Attorney Reports or Reports of Investigation which will be distributed outside the OI may require more attachments, as the agent may need to provide the Assistant United States Attorney or other recipients of the report with copies of Memoranda of Interview and other documents retained in the ITS or in the hardcopy case file.

Upon approval of the Final Report of Investigation, the report and hardcopy case file(s) should be placed in a storage area designated for closed cases.

1140.00 Investigative Activity Reports

When a significant event occurs during an investigation, such as an arrest, search warrant, indictment or information, plea agreement, settlement agreement, financial recovery, conviction, or sentencing, the special agent will prepare a short Investigative Activity Report (IAR) and submit in the ITS. The IAR will briefly summarize the allegation, and describe both the significant event and the current status of the case. A SAC may also request an IAR whenever a status report is desired on a particular investigation.

An IAR is also used to close a complaint.

1150.00 Transmittal Memorandum

A transmittal memorandum is used to transmit investigative findings to OPM officials for information or administrative action. A transmittal memorandum may be used when an investigation relates to employee misconduct that does not constitute a criminal violation, or employee misconduct for which prosecution has been declined. In such cases, a Transmittal Memorandum may be prepared in lieu of an ROI.

The memorandum should be directed from the Assistant Inspector General for Investigations (AIGI) or the Deputy Assistant Inspector General for Investigations (DAIGI) to the appropriate manager or program official. In cases when the appropriate addressee is the OPM Director, the memorandum should be directed from the Inspector General.

The memorandum should include a summation of the investigation and findings, and should indicate if the U.S. Attorney has declined prosecution in favor of appropriate administrative action. The memorandum should, in most cases, ask for the addressee to report to the OIG any action taken with regard to the investigation.

As with all reports, the special agent must submit the transmittal memorandum to his/her immediate supervisor (ASAC) for approval prior to forwarding to the DAIGI or AIGI.

1160.00 Management Advisory Report

The Management Advisory Report (MAR) is used when an OIG investigation identifies problems that require the attention of the program office. When investigations involve OPM components, programs, or employees, OPM OIG must address whether a lack of management controls, inadequate compliance with those controls, or a deficiency within the system allowed waste, fraud, or abuse to occur or to go undetected. The issues documented in the MAR may or may not be directly related to the allegations under investigation. Depending on the urgency of the issue(s) identified, the MAR may be issued prior to completion of the investigation. This report is used in

addition to or as a supplement to the Report of Investigation or Transmittal Memorandum.

The MAR should contain an explanation of the problem and the reason for urgency, if applicable; identification of possible benefits for taking immediate corrective action; and background information regarding how the problem was identified.

There are specific components related to an investigation that an OI staff member must consider prior to writing an MAR.

1. A willful criminal violation of law is not considered a management advisory and immediate investigative steps should be taken.
2. A lack of internal management controls or awareness that, without immediate attention, allows a violation involving fraud, waste and abuse to go undetected should be reported in an MAR.

When a problem requiring an MAR has been identified, the OI staff member will draft a memorandum directed from the Assistant Inspector General for Investigations (AIGI) or the Deputy Assistant Inspector General for Investigations (DAIGI) to the appropriate OPM manager or program official. After review by the staff member's supervisor(s), the draft MAR should be forwarded to the DAIGI and/or the AIGI.

The MAR is written in memorandum format and includes details of the agent's findings.

1170.00 Memoranda of Interview - General

Memoranda of Interview simply describe what was said during an interview. Interview reports should be written utilizing a simple three-step format as follows:

1. Opening Statement
2. Vital Information
3. Factual Body

The method adopted by the OIG utilizes the above three-step format and is written in the past tense, along with the simple formation of short, concise sentences that usually begin with the name of the person interviewed. The name should be capitalized throughout the report at the beginning of each new paragraph followed by the word "stated that". There are a number of other words that can be utilized in place of "stated", such as explained, described, advised, added, indicated, said, claimed, opined, recalled, etc.

Here is an example:

(b) (7)(E)



1170.10 Opening Statement

Every memorandum of interview starts with an opening statement, which identifies who was interviewed, when, where, and the names of all other individuals present. The opening statement should also reference any warnings or rights advisements given, if applicable.

On March 14, 2008, Special Agent Joseph Montana interviewed JERRY RICE at his current residence, 22 Del Monte Avenue, San Francisco, CA. MR. RICE was advised of the interviewing agent's identity, as well as the nature of the interview. In response to the questions asked, MR. RICE provided the following information.

1170.20 Vital Information

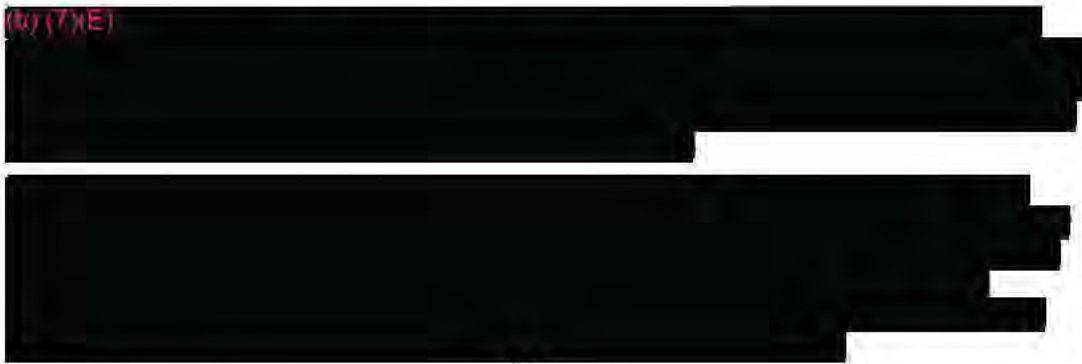
The next paragraph of an MOI should provide the vital information of the person interviewed. It should include the name of the person interviewed, social security number, date of birth, current address, work and home phone numbers, name of employer, etc. Here is an example:

JERRY RICE's social security number is 111-22-3333 and his date of birth is October 1, 1963. He currently resides at 2255 Juniper Street, Atherton, CA 94011. He advised that he could be reached via cell phone at (415) 355-5417 and/or his work number at (800) 428-5588, extension 253. He added that he now works for the Oakland Raiders located at 215 Highway 880, Oakland, CA.

1170.30 Factual Body

This is where the information furnished by the interviewee regarding the matter under investigation will be documented. Here is an example:

(b) (7)(E)



(b) (7)(E)

[REDACTED]

The name of the person being interviewed should be capitalized. When identifying the person for the first time, again the special agent should capitalize the entire first and last name, i.e. JOHN SMITH. In subsequent references the person interviewed can be referred to by last name using capital letters, i.e. SMITH.

If the person interviewed uses any technical, medical, or scientific term, it should be followed with an immediate parenthetical layman's explanation. Likewise any slang, jargon, or colloquialisms used by a witness or subject should be explained. Acronyms and sets of initials should be preceded by the complete title the first time they appear.

See IM 1191.00 for a sample MOI.

1180.00 Reports and Correspondence Retention

All investigative reports, correspondence, investigative notes, emails, and other documents related to an investigative case must be retained throughout the investigation. Regardless of record retention and destruction schedules, no records may be destroyed until after all possible judicial and administrative actions have been completed.

Furthermore, cases where a judgment (civil or criminal) is entered by a court should not be closed until 60 days after the judicial action, to allow time for the filing of appeals. Prior to closing cases involving court action, the assigned staff member must verify that no intent to appeal was filed. The ROI should be completed and the case placed in "pending" status while waiting for the time period for filing appeals to elapse.

When a case is closed, either as a complaint or as an investigation, and no (or no further) judicial and/or administrative action is anticipated, IM 1300.28 provides guidance regarding the destruction or return of documentary and physical evidence. However, IM 1300.28 pertains only to evidence collected and preserved by the OIG pursuant to procedures for maintaining a chain of custody.

The OIG routinely collects sensitive personal information, such as medical records, insurance claims, and bank records, which do not fall under the destruction policy at IM 1300.28 because copies and/or electronic files were obtained rather than originals, and therefore the documents

were not logged as evidence. Such documents containing sensitive personal information should be destroyed when the OIG no longer has need of them. When the following criteria are met, documents containing sensitive personal information shall be returned to the owner or destroyed, with the disposition of the documents fully documented. The criteria are:

- The documents contain information of a personal nature (e.g., personally identifiable information, medical records or claims forms, and/or financial records);
- The documents would have been logged as evidence if they had been obtained as originals rather than copies or electronic files; and,
- The documents are no longer of evidentiary value, because the complaint or investigation is being closed, and there is no pending or anticipated administrative action, prosecution, or judicial action of any form.

The destruction or return of documents meeting the preceding criteria must be documented by a memorandum to the case file uploaded to the investigative tracking system. A single memorandum may be used to record the destruction or return of multiple documents. This memorandum should:

- Itemize and specifically identify the documents destroyed or returned, with a description that is sufficiently thorough that the OIG could request the same documents again from the custodian of records, if necessary;
- Note the date the copies (or electronic files) were originally received by the OIG;
- Provide name and contact information for the person who furnished the copies to the OIG (plus the custodian of the original records, if the copies were obtained from a third party);
- Note the disposition of the records (returned or destroyed);
- Provide the date the records were disposed of;
- If destroyed, the destruction method used (e.g., shredded for paper records, deleted for electronic files, etc.).

1190.00 Writing Style

There are several methods, forms, styles, and formats of writing. For the purpose of all OI employees, investigative writing is a method of documentation written in an objective manner that describes what the OI employee noted, analyzed, reviewed, or otherwise observed.

(b) (7)(E)



(b) (7)(E)



[Back to Table of Contents](#)

1191.00 Sample Reports

Sample Report of Investigation

(b) (7)(E)



(b) (7)(E)



[Back to Table of Contents](#)

(b) (7)(E)



(b) (7)(E)



(b) (7)(E)



Signed: _____
Special Agent Tom Jones

Signed: _____
Bob Browser, SAC

WARNING: This document is the property of the United States Office of Personnel Managements, Office of the Inspector General, and is on loan to your office. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving office without specific prior authorization of the Assistant Inspector General for Investigations.

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Sample Memorandum of Interview



OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

MEMORANDUM OF INTERVIEW

(b) (7)(E)



(b) (7)(E)



WARNING: This document is the property of the United States Office of Personnel Management, Office of the Inspector General, and is on loan to your office. Contents may not be disclosed to any party under investigation nor may this document be distributed outside receiving office without specific prior authorization of the Assistant Inspector General for Investigations.

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Chapter 12

Administrative Sanctions

1200.00 Introduction

There are currently two separate administrative sanctions programs at OPM. Administrative sanctions related to the Federal Employees Health Benefits Program (FEHBP) are administered by the Office of the Inspector General (OIG) (See IM 1201.00 through IM 1201.18). Administrative sanctions related to all other OPM programs are administered by OPM's Contracting Group (See IM 1202.00 through IM 1202).

1201.00 FEHBP Administrative Sanctions

The OIG exercises a wide range of mandatory and permissive authorities to prohibit payment of FEHBP funds to a health care provider. The authorities serve to prevent abusive and fraudulent activities against the program and its beneficiaries. The Office of Investigations (OI) is responsible for identifying and generating debarment and suspension cases for referral to the OIG's Office of Administrative Sanctions (OAS) that are accurate, complete, and supported by the necessary documentation to implement the administrative sanction. This section provides general information about the administrative sanctions process and specific information about the roles and responsibilities of the OI in carrying out statutory obligations relative to that process.

1201.10 Authority

The authority for imposing administrative sanctions against FEHBP providers who have committed certain violations, as delegated to the OIG, is set forth in Title 5, United States Code, Section 8902a. The sanctions include debarment, suspension, civil monetary penalties, and financial assessments.

1201.11 General

This chapter contains policies and procedures regarding the coordination of the administrative remedies of suspension and debarment of health care providers stemming from investigations by the OI of provider fraud and abuse related to the FEHBP.

Effective and timely communication of information developed during OI investigations to OAS facilitates the resolution of suspension and debarment issues as expeditiously as possible.

Suspension and debarment actions are not punitive actions and they should be properly imposed to

protect the Government's business interests and the health/safety of FEHBP enrollees who may obtain services from an untrustworthy provider.

Furthermore, administrative sanctions support high standards of professional conduct and ethical business practices by holding those who commit violations accountable for their actions.

1201.12 Definitions

1. "Sanction" or "administrative sanction" means any administrative action authorized by 5 U.S.C. 8902a, including debarment, suspension, civil monetary penalties, and financial assessments.
2. "Debarment" means a decision by OPM's debarring official to prohibit payment of FEHBP funds to a health care provider, based on 5 U.S.C. 8902a(b),(c), or (d).
3. "Suspension" connotes a short-term action with the force of a debarment that is (1) effective immediately upon issuance of notice by OPM, (2) necessitated by the existence of a sufficiently serious risk to enrollee health and safety to warrant removing a provider from participating in the FEHBP in the most expeditious manner possible; and (3) based on substantiated evidence that a provider has violated one of the grounds for debarment set forth in 5 U.S.C. 8502(a).
4. "Debarring official" means an OPM employee authorized to issue debarments and financial sanctions under 5 U.S.C. 8902a.
5. "Suspending official" means an OPM employee authorized to issue suspension under 5 U.S.C. 8902a and 5 CFR 890.

1201.13 Effect of Debarment

A debarment is effective for a specified period of time commensurate with the seriousness of the act(s) which forms its basis. If a suspension precedes the debarment, the debarring official will normally consider the provider's contiguous period of suspension when determining the length of debarment. Individuals and entities are debarred from participation in the FEHBP, as defined in 5 U.S.C. 8902a (b), (c), or (d).

1. **FEHBP payment prohibited.** A debarred provider is not eligible to receive payment, directly or indirectly, from FEHBP funds for items or services furnished to a covered individual on or after the effective date of the debarment. Also, a provider cannot accept an assignment of a claim for items or services furnished to a covered individual during the period of debarment. These restrictions remain in effect until the provider is reinstated by

OPM.

2. **Government-wide effect.** Debarment precludes a provider from participating in all other Federal agencies' procurement and non-procurement programs and activities, as required by section 2455 of the Federal Acquisition Streamlining Act of 1994 (Public Law 103-355). Other agencies may grant a waiver or exception under their own regulations, to permit a provider to participate in their programs, notwithstanding the OPM debarment.

1201.14 Exceptions to the Effect of Debarments and Suspensions

A debarred/suspended health care provider may receive FEHBP funds paid for items or services furnished on an emergency basis if the FEHBP carrier serving the covered individual determines:

1. The provider's treatment was essential to the health and safety of the covered individual; and
2. No other source of equivalent treatment was reasonably available; or
3. The enrollee is bona fide unaware that the provider is debarred or suspended.

1201.15 Types of Debarment

1. Mandatory Debarments

The following types of violations constitute mandatory grounds for debarment of providers of health care services or supplies from participating in the program under 5 U.S.C. 8902(a) (b):

- a. Conviction, under Federal or State law, of a criminal offense relating to fraud, corruption, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a health care service or supply.
- b. Conviction, under Federal or State law, of a criminal offense relating to neglect or abuse of patients in connection with the delivery of a health care service or supply.
- c. Conviction, under Federal or State law, in connection with the interference with or obstruction of an investigation or prosecution of a criminal offense described in the paragraphs above.
- d. Conviction, under Federal or State law, of a criminal offense relating to the unlawful manufacture, distribution, prescription, or dispensing of a controlled substance.

years. The factors that OPM considers to be mitigating are:

- i. Whether the conviction(s) on which the debarment is based consist entirely or primarily of misdemeanor offenses;
 - ii. Whether court records, including associated sentencing reports, contain an official determination that the provider had a physical, mental, or emotional condition before or during the commission of the offenses underlying the conviction that reduced his level of culpability; or
 - iii. Whether the provider's cooperation with Federal and/or State investigative officials resulted in criminal convictions, civil recoveries, or administrative actions against other individuals, or served as the basis for identifying program weaknesses. Restitution made by the provider for funds wrongfully, improperly, or illegally received from Federal or State programs may also be considered as a mitigating circumstance.
- c. ***Maximum period of debarment.*** There is no limit on the maximum period of a mandatory debarment based on a conviction.

4. **Permissive Debarments**

A permissive debarment is one that is not mandated by law but is implemented at the discretion of OPM under 5 U.S.C. 8902a(c) or (d). OPM may impose permissive debarments against health care providers on the following bases:

- a. ***Licensure actions.*** OPM may debar any provider whose license to provide health care services or supplies has been revoked, suspended, restricted, or not renewed, by a State licensing authority for reasons relating to the provider's professional competence, professional performance or financial integrity. OPM may take this action even if the provider retains current and valid professional licensure in another State(s).
- b. ***Decision to mitigate or increase period of debarment is discretionary.*** Any decision to increase a period of debarment because of the presence of aggravating factors or to decrease it because of mitigating factors is discretionary with the debarring official.
- c. ***Ownership or control interests.*** 1) OPM may debar a health care provider that is an entity directly or indirectly owned, or with a control interest of 5 percent or more held, by an individual who has been convicted of any offense which would be a basis for debarment under 5 U.S.C. 8902a(b), against whom a civil monetary penalty has been assessed under 5 U.S.C. 8902a(d), or who has been debarred from

participation in the FEHBP by OPM. (2) OPM may debar any individual who directly or indirectly owns or has a control interest in a sanctioned entity and who knows or should know of the action constituting the basis for the entity's conviction of any offense described in 5 U.S.C. 8902a(b), assessment with a civil monetary penalty under 5 U.S.C. 8902a(d), or debarment from participation in the FEHBP by OPM.

- d. ***False, deceptive, or wrongful claims practices.*** OPM may debar any provider that the office determines, in connection with claims presented to an FEHBP carrier, has charged for health care services or supplies in an amount substantially in excess of such provider's customary charges for such services or supplies (unless the OPM finds there is good cause for such charge), or charged for health care services or supplies which are substantially in excess of the needs of the covered individual or which are of a quality that fails to meet professionally recognized standards for such services or supplies.
- e. ***False statements and misrepresentations.*** OPM may debar a provider that has knowingly made or caused to be made, any false statement or misrepresentations of a material fact reflected in a claim presented to an FEHBP carrier.
- f. ***Failure to furnish required information.*** OPM may debar a provider who knowingly fails to provide information requested by an FEHBP carrier or OPM, as needed to determine the amount or payability of a claim as set forth in 5 U.S.C. 8902a(d)(3).

5. Minimum and maximum length of permissive debarments.

- a. ***No mandatory minimum or upper limit on length of permissive debarment.*** There is neither a mandatory minimum debarment period nor a limitation on the maximum length of a debarment under any permissive debarment authority.
- b. ***Aggravating/Mitigating factors.*** The benchmark period for most permissive debarments is 3 years. However, the presence of aggravating/mitigating circumstances may support an OPM determination to increase or decrease the length of a debarment beyond the nominal periods set forth in Title 5, United States Code of Federal Regulations, Sections 890.1017 through 890.1021. This determination is discretionary with the debarring official.
- c. ***Length of permissive debarment based on revocation or suspension of a provider's professional licensure.*** Permissive debarments based on the revocation or suspension of a provider's professional license shall be for an indefinite period coinciding with the period during which the provider's license is revoked, suspended, restricted, surrendered, or otherwise not in effect in the State whose

action formed the basis for OPM's debarment. If aggravating circumstances are present, the provider may be debarred for an additional period beyond the duration of the licensure revocation or suspension.

1201.16 Suspension

A suspension is a type of administrative sanction which is taken for a temporary period of time pending the completion of an investigation and any ensuing criminal, civil, or administrative proceedings against a provider. If legal proceedings are not initiated within 12 months after the date of the suspension notice, the suspension must be terminated unless an extension is requested by the Department of Justice, the cognizant United States Attorney's Office, or other responsible Federal, State, or local prosecuting official. In such cases, the suspension may be extended for an additional 6 months. In no event, may a suspension extend beyond 18 months, unless legal proceedings have been initiated within that period. Generally, the legal proceedings are initiated by an indictment or criminal information.

- A suspension is effective immediately upon the suspending official's decision, without prior notice to the provider.
- The effect of a suspension is the same as the effect of a debarment. A suspended provider may not receive payment from FEHBP funds for items or services furnished to FEHBP-covered persons while suspended.

1201.17 Grounds for Suspension

OPM may suspend a provider if it obtains adequate evidence to support the reasonable belief that a particular act or omission has occurred (probable cause), and determines that immediate action to suspend the provider is necessary to protect the health and safety of persons covered by FEHBP. Evidence constituting grounds for suspension may include, but is not limited to:

- Indictment or conviction of a provider for a criminal offense that is a basis for mandatory debarment;
- Indictment or conviction of a provider for a criminal offense that reflects a risk to the health, safety, or well-being of FEHBP-covered individuals;
- Other credible evidence indicating, in the judgment of the suspending official, that a provider has committed a violation that would warrant debarment. This may include, but is not limited to:
 - Civil judgments;

- Notice that a Federal, State, or local government agency has debarred, suspended, or excluded a provider from participating in a program or revoked or declined to renew a professional license; or
- Other official findings by Federal, State, or local adjudicative bodies that determine factual or legal matters.

1201.18 Policies and Procedures in an OI Matter to Determine if an Administrative Sanction Action is Warranted

When OI opens and investigates an allegation, OI management is responsible for ensuring that an evaluation is made at the appropriate time, as to whether documentation and information is sufficient to support the suspension or debarment of a provider and accordingly, warrants referral to OAS for administrative action. In the case of a suspension, the standard of evidence is “adequate evidence” to support a reasonable belief that a particular act or omission has occurred. This is a lower standard than “preponderance of evidence” which is applied in debarment cases. “Preponderance of evidence” means proof of information that, when compared with that opposing it, leads to the conclusion that the fact at issue is more probably true than not. In addition, for suspension cases only, there must also be a basis for a determination by OPM that immediate action to suspend the provider is necessary to protect the health and safety of persons covered by FEHBP. This is normally considered to be satisfied if the provider is a member of the PPO of a FEHBP carrier, or if he/she has submitted claims to any FEHBP carrier.

Once an investigation is completed, or OI has identified evidence that may support a suspension or debarment action:

1. Upon becoming aware of circumstances which may serve as the basis for suspension or debarment, OI shall refer the matter to OAS for consideration via email at Debar.Internet@opm.gov. OI will work closely with OAS to ensure the coordination of suspension and debarment actions.
2. It is important that all conviction and settlement information on potential suspension/debarment actions is obtained in a timely manner. Information necessary and pertinent to OI cases that is not readily available, and may be used to assess and process suspension/debarment cases should be obtained and referred to OAS as soon as possible once it becomes available. Referrals for consideration of suspension/debarment action should include:
 - a. Recommendation and rationale for the referral;
 - b. OI point of contact;

- c. Statement of facts;
- d. List of last known home and business addresses, telephone numbers, and social security/taxpayer identification numbers for the provider, as well as affiliates/entities owned or controlled by the provider, and/or witnesses;
- e. List of any known active or potential criminal investigations/convictions, or criminal or civil proceedings;
- f. Information on any known prior convictions;
- g. Copies of all case initiations, case summaries, affidavits, confidential statements, search and arrest warrants, press releases, media coverage, and reports of investigation. If a case summary or other sensitive information cannot be disseminated for a particular reason, the SAC should coordinate the status of the investigation with OAS;
- h. Copies of signed court documents such as indictments, settlement agreements, plea agreements, and sentencing documents, such as the Judgment and Commitment Order.
- i. Cases referred to OAS may be returned to the originator for further information or development.

Special Agents should exercise caution in discussing potential suspension and debarment actions with a subject provider or defense counsel during an investigation. No statements should be made by a supervisor or an agent that imply that they can affect suspension or debarment proceedings other than by bringing any cooperation by the provider to the attention of the appropriate suspending or debaring official. An agency's decision concerning suspension and debarment may be reviewable in a Federal court. The provider is normally entitled to review any documents provided to the suspending and debaring official. In a proposed fact-based suspension or debarment prior to a criminal information being filed or indictment returned, an agent should:

1. Ascertain from OAS whether any investigative documents will be released to the subject(s) of the investigation.

The SAC and/or agent should take adequate precautions to ensure that the provision of information to OAS for subsequent release to the subject(s) of the investigation will not jeopardize the investigation; and

2. In instances where suspension or debarment action is proposed based on information obtained during the course of a criminal investigation and before the case is complete, close

coordination is needed with the Department of Justice to prevent the release of information, particularly grand jury material, which may compromise the investigation.

3. Affiliation and imputation provisions of suspension and debarment regulations cover not only the primary wrongdoer but also associated individuals or business entities.
4. Suspension and debarment actions must be entered in a timely manner into OI Investigative Tracking System.

1202.00 OPM Administrative Sanctions

OPM Contracting Policy 9.4 describes the methods and procedures followed by OPM for all debarment or suspension actions unrelated to the FEHBP. This includes, but is not limited to, debarment or suspension of background investigators employed or contracted by Federal Investigative Services (FIS) who have engaged in falsification of their work product (see **IM Chapter 8**). Unlike the FEHBP Administrative Sanctions program described earlier in this Chapter, the administration of the OPM Administrative Sanctions program has not been delegated to the OIG.

1202.01 Authority

OPM's authority to impose debarment and suspension actions derives from Section 9.402 of the Federal Acquisition Regulation (FAR). Causes for debarment are listed at 48 CFR 9.406-2. Causes for debarment include, but are not limited to:

- Conviction of or civil judgment for fraud in connection with a contract;
- Embezzlement, theft, forgery, bribery, falsification or destruction of records, and making false statements;
- Commission of any offense indicating a lack of business integrity or business honesty that seriously and directly affects present responsibility;
- A contractor's willful failure to perform in accordance with the terms of one or more contracts;

1202.02 General

Administrative sanctions imposed by OPM are not intended to punish, but rather to protect the Government's interests by ensuring that the Government only contracts with responsible parties.

Any contractor, subcontractor, or individual debarred by OPM is documented in the government-wide Excluded Parties Listing System (EPLS).

Pursuant to OPM Contracting Policy 9.4, recommendations for OPM debarment or suspension of a contractor, subcontractor, or individual shall be referred in writing to the Director of Contracting. Subsequent to review, OPM Contracting Policy submits an Action Referral Memorandum to OPM's Suspension and Debarment Committee (SDC). The SDC issues recommendations regarding proposed administrative sanctions to the OPM Suspension and Debarring Official.

1202.03 Policies and Procedures for OI Recommendations for OPM Administrative Sanctions

OI Supervisors and Managers are responsible for ensuring that an evaluation is made at the appropriate time, as to whether adequate evidence exists to support recommending OPM suspension or debarment of a contractor, subcontractor, or individual. Once an investigation is completed, or OI has identified evidence that may support a suspension or debarment action, the Senior Advisor to the AIGI serves as primary liaison between the OIG's Office of Investigations (OI) and the Director of Contracting for purposes of OI recommendations for OPM debarment/suspension.

Special Agents should exercise caution in discussing potential suspension and debarment actions with a contractor, subcontractor, individual, or defense counsel during an investigation. No statements should be made by a supervisor or an agent that imply that they can affect suspension or debarment proceedings other than by bringing any cooperation to the attention of the appropriate suspending or debarring official.

OI employees must also keep in mind that the suspended or debarred party is normally entitled to review any documents provided to the suspending and debarring official, and an agency's decision concerning suspension and debarment may be reviewable in a Federal court. Potential jeopardy to ongoing investigations must be considered when deciding whether it is appropriate to recommend a fact-based suspension or debarment prior to the final disposition of criminal prosecutions or affirmative civil enforcement.

1203.00 Program Civil Remedies (Reserved)

Chapter 13

Law and Evidence

1300.00 Law and Evidence - General

This chapter provides a discussion of basic principles of law and the law of evidence which will apply to investigations of civil, criminal, or administrative matters within the jurisdiction of the Office of Investigations. All special agents should be familiar with the **Federal Rules of Evidence** and the **Federal Rules of Criminal Procedure**. Both documents are available on the internet at www.uscourts.gov.

1300.10 Definitions of Law

Laws are rules of conduct which are prescribed or formally recognized as binding, and are enforced by the governing power.

1300.11 Common Law

Common law is comprised of the body of principles and rules of action relating to government and security of persons and property which derive their authority solely from usages and customs or from judgments and decrees of courts recognizing, affirming, and enforcing such usages and customs.

1300.12 Statutory Law

Statutory law refers to laws enacted and established by a legislative body. All Federal crimes are statutory but common law is frequently used to define words used in the statutes.

1300.13 Definitions of Crimes

A **crime** is an act against the United States only if committed or omitted in violation of a statute forbidding or commanding it, or in violation of a regulation having legislative authority.

1300.14 Evidence

The section of law which most frequently affects the conduct of an investigation is the **Federal Rules of Evidence (F.R.E.)** [(Title 28, U.S. Code). Of concern to the special agent is the

admissibility of evidence that the court, jury, board or hearing offices may properly consider in arriving at their conclusion, and what evidence they may not consider.

Although the agent is not responsible for determining the admissibility of evidence, a basic understanding and knowledge of some of the legal principles involved will assist the agent in preparing his or her case to withstand legal scrutiny. As defined in this chapter, "evidence" includes all prospective exhibits and testimony.

Collecting evidence is the basic means with which an agent accomplishes the objectives of an investigation. Sufficient evidence must be developed to establish the facts necessary to support or refute the allegations or complaints, whether the investigation is conducted for administrative, civil, or criminal action.

1300.15 The Law of Evidence

The law of evidence, which relates to the use of evidence in court, consists of: 1) rules of exclusion designed to keep from the jury information that is irrelevant, immaterial, incompetent, unreliable, confusing, wasteful of time, misleading or improperly prejudicial; and 2) rules that prescribe the manner of presenting evidence in court. "Relevant evidence" means "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without evidence" (F.R.E. 401). In addition, "all relevant evidence is admissible except as otherwise provided by the Constitution of the United States, by Act of Congress, by the rules, or prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible" (F.R.E. 402).

Evidence is only admissible if it is: 1) relevant (logically related to an issue in the case); 2) material (importantly related to an issue in the case); and 3) competent (generally reliable).

When an investigation is conducted and the results might conceivably be used in a court of law, close coordination with the SAC and prosecuting attorneys will assist the special agent in matters of evidence and interpretation of the laws. At the beginning of all cases, evidence should be collected and handled as if the case were ultimately to be used in a court of law.

1300.16 Evidence in Administrative Actions

The results of investigations may be used for administrative purposes or in adverse actions. The strict rules of evidence found in criminal or other court proceedings are not followed in administrative hearings and evidence should not be disregarded merely because it may not be admissible in a court of law.

1300.17 Evidence in Civil Actions

The **Federal Rules of Civil Procedure (28 U.S.C.)** govern the procedure in the United States District Courts in all suits of a civil nature. All evidence shall be admitted which is admissible under the statutes of the United States or under the rules of evidence applied in the courts of general jurisdiction of the state in which the United States Court is held.

1300.18 Evidence in MSPB Appeals

The Merit Systems Protection Board (MSPB) hears employee appeals of certain adverse actions such as those that lead to removal, or reduction in grade or compensation.

The strict Federal exclusionary rules of evidence are not followed in MSPB hearings. The presiding official determines the admissibility of evidence, assures that the evidence is relevant, material, and not unduly repetitious. Limits may be placed on the number of witnesses called to testify on any issue.

The weight accorded evidence depends upon the credibility of the source, the opportunity to test it through cross-examination, and whether it is believable in the context of the entire record.

1300.19 Classification of Evidence

Direct Evidence is evidence which tends to establish one or more of the principal facts in issue without the need for reference to evidence of any other fact.

Circumstantial Evidence is evidence of a collateral fact, or of another fact from which, either alone or with other accompanying information, the fact in issue may reasonably be inferred.

There is no difference between the admissibility of direct and circumstantial evidence. For the most part, the same rules of exclusion apply to both. Circumstantial evidence may be extremely useful in explaining, corroborating, and evaluating direct evidence.

1300.20 Forms of Evidence

The **Federal Rules of Evidence** prescribes three forms of evidence.

1. **Oral or Testimonial Evidence** is sworn testimony given by a witness in a trial or hearing. It is the most common form of evidence. Generally the witness will be allowed to testify only about things which he or she actually observed, heard, felt, or experienced. With few exceptions, a witness must personally appear and testify when he or she may be subject to

cross-examination.

2. **Documentary Evidence** includes anything in writing which is offered into evidence. Written evidence includes electronic data such as emails and metadata. The identity and authenticity of a document must be reasonably established as prerequisite to its admission into evidence. To be admissible as evidence in a court of law, documents must be authenticated.

Government records are authenticated by an official publication of the document or a copy of the record witnessed by its legal custodian, accompanied by a certificate from an official having a seal of office to establish that the witness is a legal custodian.

3. **Real Evidence** is the physical items or objects which are presented for examination in court for a hearing to prove or disprove a fact at issue.

1300.21 Collection of Evidence

The special agent should obtain evidence in a manner which would be admissible in a court of law so that full equity and justice are accorded the subject of an investigation. There are generally two ways of collecting evidence:

1. By testimony of a witness, which is usually admissible when the witness is competent, in other words, sane, sober, and reliable. The witness's observances and statements can be tested by cross-examination.
2. By the collection of real, physical or documentary evidence produced by, or associated with, an event or the accused.

1300.22 Collection and Preservation of Evidence

Collection and preservation of physical evidence is one of the most important responsibilities of the special agent. The special agent must maintain a proper "**chain of custody**" from the time he or she first receives evidence until it has been disposed of in court, returned to the original owner, or destroyed. Chain of custody means the preservation, in original condition, of the instrument of a crime or any relevant writing or other evidence, by the successive custodians of the evidence.

1300.23 Marking and Initialing of Evidence

In order to ensure that there is no doubt about the identity of particular evidence, the party furnishing the evidence should (b) (7)(E) The following standards apply to the

identification of seized documents:

1. The (b) (7)(E) [redacted] each document.
2. If such markings might (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

1300.24 Receiving, Identifying, and Tagging Physical Evidence

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

1300.25 Preserving Documentary and Physical Evidence

The Office of Investigations preserves and controls documentary and physical evidence through [redacted]

- Evidence Custodians: (b) (7)(E) [redacted]

contained in the bulk evidence storage rooms.

- **Evidence Storage Facilities:** (b) (7)(E) [Redacted]
- **Evidence Log:** (b) (7)(E) [Redacted]

1300.26 Evidence Log Procedures

Procedures relative to evidence logs are as follows:

1. (b) (7)(E) [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]
 - [Redacted]

1300.27 Documenting the Chain of Custody

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

1300.28 Disposition of Evidence

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

1301.00 Protection of Grand Jury Material

During the course of a grand jury investigation agents will normally gather evidentiary material such as books, records, and other documents while assisting the grand jury in its investigation of possible violations of criminal law. When material related to matters occurring before a grand jury ("grand jury or 6(e) material") is in their possession, special agents must prevent its unauthorized disclosure.

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (5)

□

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

3. (b) (5) [Redacted]

[Redacted]

[Redacted]

(b) (5) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

1301.10 Safeguarding Grand Jury Material

(b) (7)(E) [Redacted text block]

(b) (7)(E) [Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Figure 1300-01 – Evidence Tag



Figure 1300-02 – Evidence / Chain-of-Custody Form

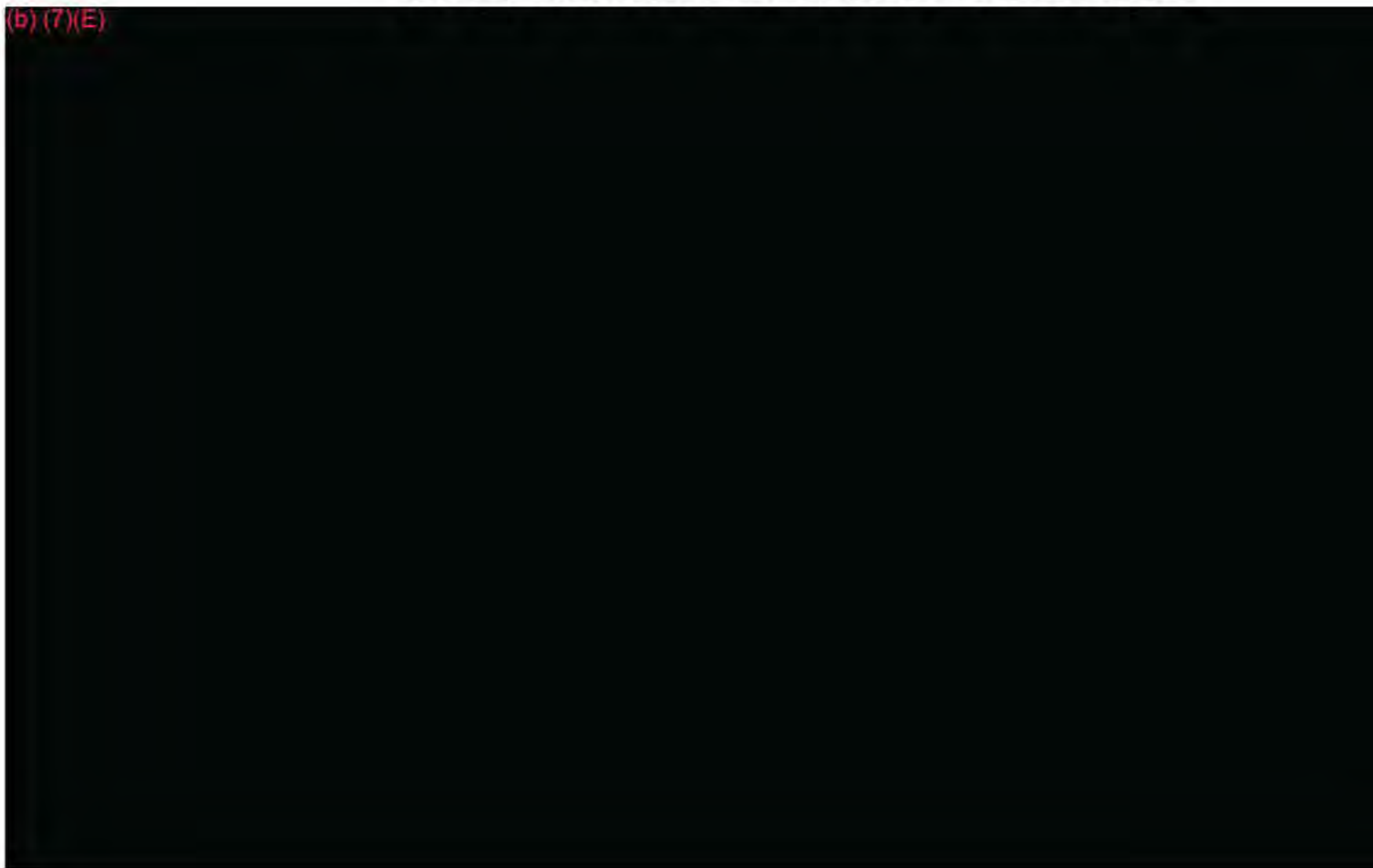


OFFICE OF THE INSPECTOR GENERAL

OFFICE OF INVESTIGATIONS

RECEIPT FOR PROPERTY RECEIVED / RETURNED RELEASED / SEIZED

(b) (7)(E)



(b) (7)(E)



Chapter 14

Witness/Victim Assistance Program

1400.00 Introduction

This chapter explains the Office of Investigations (OI) policies and procedures concerning witness and victim protection.

1400.10 Statutory and Regulatory Provisions

This section establishes Office of the Inspector General (OIG) policy guidelines for implementing the provisions of the Victim and Witness Protection Act of 1982, the Victims of Crime Act of 1984, the Victims' Rights and Restitution Act of 1990, the Violent Crime Control and Law Enforcement Act of 1994, the Antiterrorism and Effective Death Penalty Act of 1996, the Victim Rights Clarification Act of 1997, the Justice for All Act of 2004, and of Crime Victims' Rights Act Of 2004 (18 U.S.C. §3771)(collectively the "Victim/Witness Protection Statutes"). This section specifically incorporates the procedures outlined in the 2005 Attorney General Guidelines for Victim and Witness Assistance ("AG Victim Guidelines") (**Appendix M**). All personnel assigned to the Office of Investigations are required to understand and comply with the procedures in the AG Victim Guidelines.

1400.11 Background

The Crime Victims' Rights Act of 2004, 18 U.S.C. § 3771 provides that officers and employees of the Federal government shall make their best efforts to see that crime victims are notified of, and accorded, the following rights:

- The right to be reasonably protected from the accused.
- The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused.
- The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.
- The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding.

- The reasonable right to confer with the attorney for the Government in the case.
- The right to full and timely restitution as provided by law.
- The right to proceedings free from unreasonable delay.
- The right to be treated with fairness and with respect for the victim's dignity and privacy.

1400.12 Definitions

1. The term "crime victim" is defined differently by different Federal statutes. Unless otherwise noted, the AG Guidelines and this chapter use the following definitions:
 - a. **Victim, Enforcement of Rights:** For purposes of enforcing the rights enumerated the AG Guidelines, a victim is "a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia" (18 U.S.C. § 3771(e)) if the offense is charged in Federal district court. If a victim is under 18 years of age, incompetent, incapacitated, or deceased, a family member or legal guardian of the victim, a representative of the victim's estate, or any other person so appointed by the court may exercise the victim's rights, but in no event shall the accused serve as a guardian or representative for this purpose. (18 U.S.C. § 3771(e)) A victim may be a corporation, company, association, firm, partnership, society, or joint stock company. (1 U.S.C. § 1)
 - b. **Victim, Provision of Services:** For purposes of providing the services described in the AG Guidelines, a victim is "a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime." (42 U.S.C. § 10607(e)(2)) If a victim is an institutional entity, services may be provided to an authorized representative of the entity. If a victim is under 18 years of age, incompetent, incapacitated, or deceased, services may be provided to one of the following (in order of preference) for the victim's benefit:
 - i. A spouse.
 - ii. A legal guardian.
 - iii. A parent.
 - iv. A child.
 - v. A sibling.
 - vi. Another family member.

vii. Another person designated by the court. (42 U.S.C. § 10607(e)(2))

2. **Witness:** A witness is someone who has information or evidence concerning a crime, and makes that information available to a law enforcement agency. When the witness is a minor, the term witness includes an appropriate family member or legal guardian. The term witness does not include defense witnesses or those individuals involved in conducting OIG investigations.
3. **Serious Crime:** A serious crime is a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

1400.13 Policy

The provisions of the Victim/Witness Protection Statutes and the guidelines and procedures set forth below will be followed when dealing with matters relating to victims and witnesses involved in OIG investigations.

1400.14 Legal Status of Guidelines

These guidelines provide only internal guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any person in any matter, civil or criminal. Nor are eliminations placed on otherwise lawful prerogatives of the Office of Personnel Management. Rather, these guidelines are intended to ensure that responsible officials, in the exercise of their discretion, treat both victims and witnesses appropriately.

1400.15 Procedures and Individual Responsibilities

1. **Assistant Inspector General for Investigations**
 - a. Develop policies and procedures to assure that victims/witnesses are provided assistance in accordance with the provisions of the Victim/Witness Protection Statutes.
2. **Deputy Assistant Inspector General for Investigations**
 - a. Act as Primary Contact Person (PCP) for the OIG. The DAIGI may delegate the discharge of PCP responsibilities to subordinates. The PCP reviews all procedures to ensure the proper oversight of services to be rendered to victims/witnesses.

3. Primary Contact Person (PCP)

- a. Primary contact with the Department of Justice, Office of the Victims' Rights Ombudsman. On an individual case basis, makes contacts with Victim/Witness Coordinators (VWC) in the jurisdictions involved to determine their policy in relation to the particular victim or witness situation or problem.
- b. To the extent possible, avoid disclosure of victim or witness names except to authorized persons.
- c. Ensure that any property of a victim that is being held for evidentiary purposes is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes. (42 U.S.C. §10607(c)(6)) There may be circumstances, however, in which a victim's property will inevitably deteriorate or will be damaged through legitimate use in the law enforcement process. Contraband shall not be returned to victims.
- d. Ensure that each victim/witness is informed of the name, title, business address and telephone number of the person whom they should contact to obtain emergency medical and/or social services, restitution or other relief and the availability of public and private programs that provide counseling, treatment, and other support services.
- e. Explain the role of the victim/witness in a criminal investigation and prosecution, including what they may expect from the system, and what the system expects from them.
- f. Ensure that the victim/witness is notified of the status of the investigation, including the arrest of a suspected offender. This notice will be made to the extent possible as long as such information does not interfere with the investigation itself.
- g. In the event of the actual intimidation and/or harassment of a victim or witness, the PCP, directly or through subordinate, take immediate action to:
 - i) Notify the U.S. Attorney involved in the prosecution of the case;
 - ii) Render whatever interim assistance is necessary to the victim or witness; and
 - iii) Notify the responsible federal agency.
- h. Upon request of a victim/witness, coordinate with the appropriate VWC regarding employer or creditor notification of the cause of the victim/witness' absence from work or nonpayment of debt.

4. Special Agents in Charge\Assistant Special Agents in Charge\Team Leaders

- a. Act as PCP alternate
- b. Provide instructions to Special agents concerning their responsibilities in carrying out certain provisions of the Victim/Witness Protection Statutes.
- c. Assure that the PCP is notified of any situation in which the provisions of the Victim/Witness Protection Statutes might be invoked.
- d. Ensure that any information in the case file that is pertinent to the defendant's sentence is brought to the attention of the U.S. Attorney or the U.S. Probation Office. This information will assist in the preparation of the victim impact statement in the U.S. Probation Office's pre-sentence report to the presiding judge.

5. Special Agent

- a. Through your supervisor, notify the PCP of any situation in which the provisions of the Act could be invoked.
- b. Immediately notify your SAC or ASAC of any actual instances of intimidation or harassment of any victim or witness.
- c. Assist the PCP, VWC, and the U.S. Attorney, as necessary, in carrying out the provisions of the Victim/Witness Protection Statutes.
- d. Ensure that victims/witnesses routinely receive information on the prohibition against victim/witness intimidation or harassment and the appropriate remedies and that they are advised to report such incidents to the PCP or their subordinate.
- e. When interviewing a victim or witness at his or her place of employment, explain to the employer and others the status of the individual as a victim/witness and the necessity for conducting the interview at that time.

Chapter 15

Medical and Physical Standards

1500.00 Background

Title 5 CFR 339, “Medical Qualification Determinations,” contains OPM’s basic guidance on the establishment of medical standards and physical requirements for Federal civilian positions. Medical standards and physical requirements have been established for criminal investigator positions (GS-1811) in OPM designated as primary under 5 U.S.C. 8336 (c).

1501.00 Definitions

1. **Primary positions:** These positions generally consist of OPM/OIG criminal investigators performing the operational details of criminal investigations such as interviewing witnesses; interrogating suspects; reviewing, collecting, and analyzing records, facts, and evidence; performing undercover assignments; obtaining and serving warrants; using firearms; and carrying out arrests, searches, and seizures.
2. **Secondary positions:** These positions generally consist of OPM/OIG managerial, supervisory, technical, or administrative positions (some with operational, policy-making, and oversight responsibilities) which clearly require the first-hand knowledge, skills, abilities, and experience gained in the performance of primary law enforcement positions.

1502.00 Medical Requirements

Per Section IV-B of OPM’s Operating Manual for Qualification Standards for General Schedule Positions, the duties of positions in the GS-1811 series “require moderate to arduous physical exertion involving walking and standing, use of firearms, and exposure to inclement weather. Manual dexterity with comparatively free motion of finger, wrist, elbow, shoulder, hip and knee joints is required. Arms, hands, legs, and feet must be sufficiently intact and functioning in order that applicants may perform the duties satisfactorily. Sufficiently good vision in each eye, with or without correction, is required to perform the duties satisfactorily. Near vision, corrective lenses permitted, must be sufficient to read printed material the size of typewritten characters. Hearing loss, as measured by an audiometer, must not exceed 35 decibels at 1000, 2000, and 3000 Hz levels. Since the duties of these positions are exacting and responsible, and involve activities under trying conditions, applicants must possess emotional and mental stability. Any physical condition that would cause the applicant to be a hazard to himself/herself, or others is disqualifying.”

1503.00 Hiring Standards

Hiring standards for OPM-OIG Criminal Investigator Primary Positions, to include age requirements, physical requirements, and medical standards were formally approved by OPM on April 5, 1991 (Attachment A). The purpose of the standards is to ensure that appointees are able to execute the rigorous and hazardous duties associated with Criminal Investigator positions, such as carrying firearms, executing arrests, seizing evidence, transporting evidence, conducting surveillance, and working under generally arduous environmental conditions. All of these duties require physical strength, stamina, agility, and the ability to act or react quickly.

1503.10 Minimum/Maximum Age Requirements

Minimum age for persons hired for OPM-OIG criminal investigator primary positions is 21 years at time of appointment. Maximum entry age for persons hired for primary positions is 37 years at time of appointment, unless that person qualifies for a veteran's preference.

1503.20 Medical Examinations

1. Applicants

All applicants for OPM/OIG criminal investigator primary positions covered under the law enforcement provisions of either CSRS or FERS will be required to undergo a pre-employment medical examination by agency designated physicians to determine if they are physically and medically qualified to perform the full duties of the position. Any physical condition which would hinder an individual's full, efficient, and safe performance of his/her duties as a criminal investigator or failure to meet any of the required physical or medical qualifications will usually be considered **disqualifying** for employment, except when convincing evidence is presented that the individual can perform the essential functions of the job efficiently and without hazard to themselves or others.

- a. Employability determinations are made by the AIGI.
- b. Applicants who refuse to submit to the required pre-employment medical examination will not be considered for employment as a criminal investigator.
- c. Applicants with a military service-connected disability must bring a copy of their Veteran's Administration (VA) Rating Decision with them to the pre-employment medical examination for the examining physician's review
- d. At the discretion of the AIGI, pre-employment medical examinations may be waived for applicants who are currently employed as criminal investigators by other Federal agencies.

2. Employees

The OPM-OIG may require medical examinations of individuals employed as criminal investigators, either on a periodic basis or whenever there is a question about the employee's continued ability to meet the physical or medical requirements of the position.

Per 5 CFR 339.102 (c), an employee's refusal to be examined in accordance with a proper agency order is grounds for appropriate disciplinary or adverse action.

3. Costs of Medical Examinations

When OPM/OIG requires a medical examination of an applicant or employee, the costs of the original medical examination will be paid by OPM/OIG, as required by 5 CFR 339.304. Any follow-up personal medical expenses incurred by the applicant/employee are the individual's responsibility.

1503.30 Application of Physical and Medical Standards

The physical requirements and medical standards detailed in OPM-OIG's hiring standards are designed to aid OPM/OIG management officials and examining physicians in determining what medical problems may hinder an individual's ability to satisfactorily perform the duties of the criminal investigator position without causing undue risk to themselves or others, and to ensure consistency in the application of these standards for applicants and employees. The medical conditions listed in the standards are not intended to be all-encompassing nor are they meant to establish absolute requirements for OPM/OIG criminal investigator positions. In general, the existence of a medical condition or impairment, or a history of such a condition, is disqualifying only when there is a direct relationship between the condition and the essential duties of the position.

1503.40 Employability Determinations

Per 5 CFR 339.102 (c), failure to meet a properly established medical standard or physical requirement means the individual is not qualified for the position unless a waiver or reasonable accommodation is indicated. However, applicants and employees cannot be disqualified arbitrarily on the basis of medical standards, physical requirements, fitness tests, or other criteria that do not relate specifically to job performance.

OPM/OIG management will refer to 5 CFR 339, to OPM's Operating Manual for Qualification Standards for General Schedule Positions, and to OPM's Human Resources Handbook when making qualifications decisions about specific medical problems. Employment related decisions involving health status are fundamentally management, not medical decisions.

1503.50 Waiver of Physical Requirements/Medical Standards

All requests for waivers of criminal investigator physical requirements and/or medical standards will be submitted to the AIGI, who is the OPM/OIG deciding official.

Failure to meet the established medical standards or physical requirements means that the individual is not qualified for the position unless there is sufficient evidence that he/she can perform the duties of the position safely and efficiently despite a condition that would normally be disqualifying. OPM/OIG must waive any medical standard or physical requirement for a person who is able to demonstrate the capacity to perform safely and efficiently. Factors to be considered when making a determination include: health and safety considerations; recent successful performance in the same/similar position; successful performance of other life activities with similar physical and environmental demands; certification from a counselor from either the Veterans Administration or a State vocational rehabilitation agency; use of a prosthesis or other mechanical aid (including eye glasses and hearing aid) enabling the candidate to perform the work; successful performance of a real or simulated work sample; and a determination that the condition may be reasonably accommodated (without undue hardship on the agency) pursuant to the Rehabilitation Act of 1973, as amended.

1504.00 Physical Fitness Program

As referenced above, per the physical and medical standards for criminal investigators, criminal investigators must be in good health and maintain a level of manual dexterity and strength sufficiently adequate to perform the duties of the position. The goal of the physical fitness program is to afford criminal investigators an opportunity to develop and maintain fitness through physical activities.

The OPM supports physical fitness as an essential element of Occupation Health Programs that are authorized within the Federal Government under Title 5 U.S.C. 7901. Federal agencies may establish and operate physical fitness programs to promote and maintain employee health.

The U.S. Department of Labor has issued guidelines on financial liability and furnished information on a procedure to review claims for injury or occupational disease related to participation in physical fitness programs. According to the Federal Employees Compensation Act (FECA) Bulletin, Number 87-9, issued on January 12, 1987, employees who are enrolled in an approved Physical Fitness Program are considered to be "in the performance of duty for FECA purposes while doing authorized exercises." This bulletin goes on to say that injuries or diseases arising from participation in an employing agency's fitness program are covered under FECA.

1504.10 Administration of Physical Fitness Program

The OIG's Physical Fitness Coordinator(s) are responsible for administering the Physical Fitness Program. All criminal investigators are expected to participate, unless they have received a medical waiver.

1504.20 Physical Fitness Training

Criminal Investigators are granted up to three (3) duty hours per week for physical fitness training. Since the purpose of the physical fitness program is to promote regular exercise, these hours may be used in increments no greater than 1 1/2 hours per day and no less than 3/4 hour per day (examples: 1 hour per day/3 days per week; 1 1/2 hour per day/2 days per week; and, 3/4 hours per day/4 days per week).

Physical fitness training includes activities that will maintain or improve the individual's level of fitness conditioning (cardiovascular endurance, flexibility, agility and strength). The OIG's Physical Fitness Coordinator(s) determine whether particular activities are approved for physical fitness training. Examples of approved activities include: walking, running, swimming, bicycling, aerobics, weight training, calisthenics, circuit training, martial arts, and stretching. Any activity not on this list must be referred to the Physical Fitness Coordinator(s) for approval, if it is to be performed during duty hours. When deciding whether to approve an activity, the Physical Fitness Coordinator(s) will consider several factors, including: 1) whether the activity will help maintain/improve fitness; and 2) the level of risk involved in the activity. Activities that are inherently dangerous (e.g., rock climbing, parachuting, etc.) or relatively sedentary in nature (e.g., golfing, horseshoes, etc.) will not be approved for physical fitness training. Team sports may/may not be approved, depending on the level of physical activity and the level of risk involved in the sport.

The OIG will not pay for membership in a health or athletic facility.

1504.30 Physical Fitness Training and LEAP

The three (3) duty hours per week for fitness training may be used toward the annual average of two extra hours per regular work day required to earn law enforcement availability pay. However, in order for the time spent on fitness training to be considered "duty hours", it must be performed during the work day. This would include fitness training conducted at the beginning or the end of the work day. However, fitness training performed on holidays, weekends, or when the investigator takes a full day of leave may not be counted as "duty hours" for FECA or LEAP purposes.

1504.40 Physical Fitness Training and the Use of the Government Vehicle

As stated in 1504.00 above, criminal investigators are “in the performance of duty” while engaged in approved physical fitness training during duty hours. Therefore criminal investigators are permitted to use their assigned government vehicles in order to travel to the location of approved physical fitness activities (gyms, pools, athletic facilities, etc.) during duty hours.

1504.50 The Physical Efficiency Battery

In order to monitor the effectiveness of the Physical Fitness Program and the conditioning of those participating, on an annual basis all criminal investigators will be required to take the Physical Efficiency Battery (PEB) that was developed and implemented by the Federal Law Enforcement Training Center (FLETC). FLETC’s PEB has five components, designed to test cardiovascular endurance, flexibility, agility, strength, and body composition. The components include: a 1 ½ mile run/walk; a “sit-and-reach” flexibility test; an agility course; a maximum-resistance bench press; and a body composition measurement with skinfold calipers. The PEB test will be administered under the direction of a FLETC-trained Physical Fitness Coordinator. The PEB may be modified at the discretion of the Physical Fitness Coordinator(s) to ensure the safety of all participants and to suit the equipment/facilities available. (For example, push-ups may be substituted for the bench press if a fixed bench press station is not available.)

A record of each criminal investigators’ participation in the PEB will be maintained by Physical Fitness Coordinator(s).

The requirement to participate in the PEB test may be waived for a criminal investigator who develops an injury or other medical condition that would temporarily preclude their ability to participate.

Appendices

Appendix Listing

Appendix A	<u>IG Act of 1978</u>
Appendix B	<u>CIGIE Quality Standards for Investigations adopted for Federal Offices of of Inspectors General</u>
Appendix C	<u>Whistleblower Protection Act of 1989</u>
Appendix D	<u>OPM Guidelines for Handling Personally Identifiable Information (PII)</u>
Appendix E	<u>(b) (7)(E)</u>
Appendix F	<u>Provisions of the Attorney General’s Guidelines for Offices of Inspector Inspector General with Statutory Law Enforcement Authority</u>
Appendix G	<u>Attorney General’s Guidelines for Domestic FBI Operations</u>
Appendix H	<u>Attorney General’s Guidelines Regarding the Use of Confidential Informants</u>
Appendix I	<u>CIGIE Guidelines on Undercover Operations</u>
Appendix J	<u>Attorney General’s Guidelines for Undercover Operations</u>
Appendix K	<u>CIGIE Quality Standards for Digital Forensics</u>
Appendix L	<u>Department of Justice “Less Than Lethal” Policy</u>
Appendix M	<u>Attorney General’s Victim Guidelines</u>