



governmentattic.org

"Rummaging in the government's attic"

Description of document: Title of Thesis: Unlawful Disclosure In The New Information Sharing Era, 2004. Released by the Office of The Director of National Intelligence (ODNI)

Requested date: 18-September-2017

Release date: 04-December-2024

Posted date: 23-December-2024

Source of document: FOIA Request
Director, Information Management Office
ATTN: FOIA/PA
Office of the Director of National Intelligence
Washington, D.C. 20511
Email: ODNI_FOIA@odni.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 DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

3 December 2024

Reference: ODNI Case No. DF-2022-00321

This letter provides an interim response to your Freedom of Information Act (FOIA) request to the Defense Intelligence Agency (DIA), dated 18 September 2017, requesting 18 specific theses written by students at the National Intelligence University. As previously noted by DIA, DIA transferred these cases to the Office of the Director of National Intelligence (ODNI) in 2022.

ODNI processed this request under the FOIA, 5 U.S.C. § 552, as amended and located 17 of the theses requested. Note, despite a thorough search, “Rationing the IC: The Impact of Private American Citizens on the Intelligence Community” was not located.

This interim response provides a response on ten of the theses. During the review process, we considered the foreseeable harm standard and determined that certain information must be withheld pursuant to the following FOIA exemptions:

- (b)(3), which applies to information exempt from disclosure by statute. Specifically, the National Security Act of 1947, as amended:
 - Section 102A(i)(1), 50 U.S.C. § 3024(i)(1), which protects information pertaining to intelligence sources and methods; and
 - Section 102A(m), as amended, 50 U.S.C. § 3024(m), which protects the names and identifying information of ODNI personnel.
- (b)(6), which applies to information that, if released, would constitute a clearly unwarranted invasion of personal privacy.

Be advised, we continue to process your request. If you are not satisfied with this response, a number of options are available. You may contact me, the FOIA Public Liaison, at ODNI_FOIA_Liaison@odni.gov, or the ODNI Requester Service Center, at ODNI_FOIA@odni.gov or (703)-275-1313. You may also submit an administrative appeal to the Chief FOIA Officer, c/o Chief, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511 or emailed to ODNI_FOIA@odni.gov. The appeal correspondence should be clearly marked “Freedom of Information Act Appeal of Adverse Determination” and must be postmarked or electronically transmitted within 90 days of the date of this letter.

Lastly, the Office of Government Information Services (OGIS) of the National Archives and Records Administration is available with mediation services and can be reached by mail at 8601

Adelphi Road, Room 2510, College Park, MD 20740-6001; telephone (202) 741-5770; toll-free (877) 684-6448; or email at ogis@nara.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Erin Morrison". The signature is fluid and cursive, with a long horizontal stroke at the end.

Erin Morrison
Chief, Information Review and Release Group
Information Management Office

UNLAWFUL DISCLOSURE IN THE NEW INFORMATION SHARING ERA

by

Major, U.S. Army
PGIP-M Class 2004

Unclassified thesis submitted to the Faculty
of the Joint Military Intelligence College
in partial fulfillment of the requirements for the degree of
Master of Science of Strategic Intelligence

July 2004

The views expressed in this paper are those of the author and
do not reflect the official policy or position of the
Department of Defense or the U.S. Government

ABSTRACT

TITLE OF THESIS: Unlawful Disclosure in the New Information Sharing Era

STUDENT:

CLASS NO: PGIP-M 0204

DATE: July 2004

THESIS COMMITTEE CHAIR:

SECOND COMMITTEE MEMBER:

Effective counterterrorism and homeland security efforts by the Intelligence Community (IC) and the Law Enforcement Community (LEC) depend on critical cooperation, information sharing, and intelligence sharing between the military, IC, and LEC. Prior to September 11th, 2001 the process of information and intelligence sharing was always the foundation of counterterrorism and national security. However, in the post-September 11th era information sharing has become essential for national security, homeland defense, and effective counterterrorism. Information sharing inherently involves the movement of classified information and intelligence from one person, agency, or location to another. The movement of information or intelligence has inherent risks, including unlawful disclosure. Minimizing this risk and unauthorized disclosures is a top priority for the IC and the LEC.

The risk of unlawful disclosure, including espionage, has ancient roots. There are many well-known and obscure cases of unlawful or improper disclosures of classified information and intelligence. One of the most devastating aspects of unlawful or wrongful disclosures (also known as “leaks”) is that they diminish the essential power of classified intelligence and classified information. The essence of classified intelligence

and classified information is that it consists of secrets derived from secret sources and methods. Unlawful or wrongful disclosure of classified intelligence or information compromises the sources and methods of the Intelligence Community and ultimately undermines national security. Unlawful disclosures also significantly diminish the value of the classified information for decision makers when it is disclosed to or is obtained by U.S. Government enemies or adversaries.

The post-September 11th era has ushered in a new era of increased intelligence and information sharing to combat global and domestic terrorism. The increased levels of intelligence and information sharing is clearly evident between federal agencies, but the most dramatic increases in intelligence and information sharing are between the IC and various state and local government agencies, including the LEC. Increased intelligence and information sharing between the federal and state levels of government pose significant risks of increased unlawful and wrongful disclosure. This serious issue requires immediate attention by the President, Congress, and the IC and LEC to minimize the imminent dangers of unlawful and wrongful disclosure of classified information and intelligence. The consequences of unlawful disclosure ultimately cost lives and are a serious threat to national security.

Effective safeguards and enforcement measures must be developed to balance the critical needs of national security with the corresponding need to share classified intelligence and information with state and local officials to enhance national security. In addition, community awareness about the dangers posed by unlawful disclosures must be increased to better protect classified information. My thesis is that the unlawful disclosure of classified information and intelligence will increase significantly during the

new information sharing era, unless effective safeguards are developed and vigorously enforced to protect the information and the sources and methods. Effective national security will require seamless information sharing and earnest cooperation between the federal government and state and local governments. Not sharing information is not an option according to Congressional and executive mandates. Meanwhile, significant barriers continue to hinder the information sharing process and U.S. national security hangs in the balance. Concerns about unauthorized disclosures are among the most significant barriers to an effective information sharing process and these concerns should be taken seriously.

Real or perceived concerns about the risk of unauthorized disclosures is a reason cited by intelligence and law enforcement personnel who are either reluctant to share relevant information with outside agencies or avoid sharing relevant and actionable information. Since the risk of unauthorized disclosure is a legitimate concern, then an effective balance must be struck between boundless information sharing and sharing relevant actionable information with appropriate officials. Information must be shared between agencies regardless of governmental level, while simultaneously protecting the classified information from unauthorized disclosure.

This thesis was written in an unclassified format to facilitate the widest possible dissemination of the research. A classified bibliography (not enclosed) was developed to assist members of the IC and the LEC with additional research on related topics.

DEDICATION

To my wife _____ who fully supported this research project from its inception, and continued to support the project without giving me unreasonable grief. Love is patient and so are you. I love you and thank you for “everything.” No exceptions.

To my brilliant children, _____, _____, _____, and _____; my thoughts of each of you inspire me daily. Each of you are a reflection of the best of our ancestors and your own uniqueness. Future generations will benefit from your plans and positive actions to make the world a better place.

SPECIAL THANKS

Special thanks to _____ and _____ for their earnest interest in academic excellence and leadership, and for mentoring me through the thesis research, writing, and submission process. My sincere appreciation to _____ Staff Judge Advocate, U.S. Army Space and Missile Defense Command, for supporting my attendance at the Joint Military Intelligence College. Special thanks to the PGIP-R/M Class of 2004, especially Seminar “V” (Victory) for two tough years of teamwork and friendship. Finally, my eternal loving thanks to _____ for being there during “thick and thin.”

CONTENTS

Dedication and Special Thanks.....	ii
List of Graphics.....	v
Chapter	Page
1. INTRODUCTION.....	1
Information and Intelligence Sharing and Disclosures of Classified Material, 1	
Definitions, 3	
Statement of the Problem, 6	
Research Question and Hypothesis, 8	
Assumptions, 9	
Methodology, 9	
Overview of Chapters, 10	
2. REVIEW OF INFORMATION SHARING STATUTES, EXECUTIVE ORDERS, REGULATIONS, AND POLICIES.....	12
Information Sharing Statutes, 12	
Executive Orders, 16	
Regulations, 21	
Policies, 22	
Unlawful Disclosure Statutes, 27	
3. METHODOLOGY.....	30
4. CASE STUDY: SENATE-WHITE HOUSE RICIN INCIDENT.....	33
Introduction and Overview, 33	
Case Study Analysis, 35	
Applicable Information Sharing Laws and Procedures, 36	
Conclusion, 37	

5. INFORMATION SHARING SURVEY.....	40
Military and Intelligence Community Officials, 40	
Local Law Enforcement and Emergency Response Officials, 47	
Conclusions, 53	
6. RECOMMENDATIONS TO COUNTER THE UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION.....	55
Uniform and Comprehensive Standards, 56	
Legislative Action, 57	
Executive Action, 62	
Intelligence Community Action, 64	
State and Local Law Enforcement, 66	
7. KEY FINDINGS, CONCLUSIONS, AND IMPLICATIONS.....	69
Key Findings, 69	
Conclusions, 69	
Implications, 72	
Recommendations for Further Research, 75	
 Appendixes	
A. Information Sharing Survey.....	78
B. The New Terrorist Threat Integration Center (TTIC).....	81
C. Classified Information Nondisclosure Agreement Briefing Booklet.....	82
D. Protection of Certain National Security Information.....	84
E. Classified National Security Information.....	86
F. Major Reviews of the U.S. Secrecy System.....	90
Bibliography	93

LIST OF GRAPHICS

Map	Page
1. Capitol Hill, U.S. Senate, Washington, DC.....	38

Figure	
1. A Target-Centric View of the Intelligence Process.....	43

Table	
1. Target-Centric Intelligence Process, Survey Question 5.....	44
2. Disclosures of Classified Information, Survey Question 6.....	45
3. Safeguarding Classified Information, Survey Question 7.....	46
4. Homeland Security Act Protections, Survey Question 11.....	50

CHAPTER 1

INTRODUCTION

By definition, intelligence deals with the unclear, the unknown, and the deliberately hidden. What the enemies of the United States hope to deny, we work to reveal.

-- George J. Tenet, Former Director of Central Intelligence¹

INFORMATION SHARING AND DISCLOSURES OF CLASSIFIED MATERIAL

Effective counterterrorism and homeland security efforts depends on critical cooperation, information sharing, and intelligence sharing between the defense, intelligence, and law enforcement communities. Prior to September 11th, 2001 the process of information and intelligence sharing was an important part of counterterrorism and national security. However, in the post-September 11th era information sharing has become a requirement for effective national security and is considered to be essential for effective counterterrorism and homeland defense. Information sharing inherently involves the movement of classified information and intelligence from one person, agency, or location to another. This movement of information or intelligence has inherent risks, including unlawful disclosure. Unlawful and unauthorized disclosure of classified or sensitive information, including espionage, has been a problem that has existed from the pre-American revolution era to the present.² From Benedict Arnold in

¹George J. Tenet, Director of Central Intelligence, "Iraq and Weapons of Mass Destruction," speech presented at Georgetown University, Washington, DC, 5 February 2004, URL: <www.georgetownuniversity/publicaffairs/tenet/05022004.html>, accessed 8 March 2004.

²Glen P. Hastedt, *Espionage: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO Press, 2003), 175-183. Excellent chronology of the history of espionage from 1765 to 2003.

the mid to late 1700's³ to the Rosenberg couple in the 1950s to spies like John Walker and Aldrich Ames in the 1990's.⁴ There are many well-known and obscure cases of unlawful or improper disclosures of classified information and intelligence, including cases of espionage. One of the most devastating aspects of unlawful or wrongful disclosures (also known as "leaks") is that they diminish the essential power of classified intelligence and classified information. The most damaging and horrific cases of unlawful disclosure are those that result in the death of U.S. personnel and the loss of billions of dollars in technical intelligence collection "superiority." This damage to the USG intelligence collection process leaves national security at risk from unknown attacks within and outside of the continental United States.

The essence of classified intelligence and classified information is that they are secrets derived from secret sources and methods (SAM). Unlawful or wrongful disclosure of classified intelligence or information compromises the SAM of the Intelligence Community and ultimately undermines national security by giving United States Government (USG) adversaries advantages that they otherwise would not possess and exploit.

The post-September 11th era has ushered in a new era of increased intelligence and information sharing to combat global and domestic terrorism. Although, the U.S. government's (USG) response to increase information sharing is reasonable and necessary, the question of whether adequate safeguards have been effectively implemented in response to increased dissemination is undetermined.

³Hastedt, 108.

⁴Hastedt, 140.

The author conducted an Information Sharing Survey⁵ as part of the research for this thesis. The result of the survey suggests that there has not been sufficient time for the IC to determine the impact of the HSA and the new information sharing initiatives on the security and protection of classified information. There is a full discussion of the information sharing survey in Chapter 5.

DEFINITIONS

There are a few terms related to information sharing and unlawful disclosure that require definitions. The term “foreign government” encompasses more than its literal meaning and also includes foreign entities that are not recognized by the USG. **Foreign government** “includes . . . any person . . . acting or purporting to act for or on behalf of any faction, . . . department, . . . bureau, or military force of or within a foreign country, or for or on behalf of any government or any person . . . purporting to act as a government within a foreign country, whether or not such government is recognized by the United States.”⁶ This very broad statutory definition indicates the sensitivity of the USG to potential foreign threats to national security, particularly when these threats involve classified information.

The essence of intelligence is “classified information” and data that is analyzed to produce intelligence. **Classified information** “means information which . . . is, for reasons of national security, specifically designated by a United States Government

⁵E-mail survey, “Information Sharing Survey,” conducted by the author, April-May 2004.

⁶18 U.S.C. § 794, Gathering and Dissemination of Classified Information. Cited hereafter as 18 U.S.C. § 794.

Agency for limited or restricted dissemination or distribution.”⁷ Federal agencies have the authority to determine what information that they control should be designated as classified information. Once this designation is made the information is protected from unauthorized disclosure as determined by applicable laws and regulations. Some forms of classified information are so designated to afford protection to the source of the information or the method by which it was derived, “sources and methods (SAM). Signals intelligence (SIGINT) and “communications intelligence” are examples of the types of information that require enhanced and special protections due to the increased potential for exposing the SAM of the information. **Communication intelligence** “means all procedures and methods used in the interception of communications and the obtaining of information such communications by other than the intended recipients.”⁸ This broad definition is intended to encompass all SAMs that could be used to derive communication intelligence. Because it is impossible to keep pace with technological advances related to interception of communications, “all” SAMs related to such interception are given the highest levels of classification and access to this information and intelligence is tightly controlled based on need.

The term “need for access” means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.”⁹ This determination is made by the particular federal agency and access is also provided across agency boundaries based on

⁷18 U.S.C. § 794.

⁸18 U.S.C. § 794.

⁹U.S. President, Executive Order 12968, “Access to Classified Information,” 2 August 1995. Cited hereafter as U.S. President, EO 12968.

memoranda of agreement and other interagency arrangements. The heart of the “need for access” concept is the goal of federal agencies to limit or eliminate unauthorized disclosures of classified information.

The term “unauthorized disclosure” means a communication or physical transfer of classified information to an unauthorized recipient¹⁰ or person. Basically, providing classified information to a person or entity that is not have the appropriate clearances and need to know constitutes an “unauthorized disclosure.” The type of persons or entities to which it is not permissible to convey classified information is understandably broad.

“Unauthorized person “means any person who, or agency which, is not authorized to receive [classified or other sensitive] information [as determined] by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.”¹¹ The communication or transfer of classified information to any unauthorized person constitutes a “violation” and is a federal crime. A “violation” means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.”¹² There are other specific legal definitions related to information sharing and unlawful disclosure, however this abbreviated list is sufficient for a basic understanding and discussion of the topic. Additional terms and concepts will be explained as needed in each chapter. In addition,

¹⁰U.S. President, Executive Order 13292, “Further Amendment to Executive Order 12958, as amended, Classified National Security Information,” 25 March 2003. Cited hereafter as U.S. President, EO 13292.

¹¹18 U.S.C. § 794.

¹²U.S. President, EO 13292.

the appendixes include several detailed explanations of terms related to classified information nondisclosure, national security information, and the Terrorist Threat Integration Center (TTIC).

STATEMENT OF THE PROBLEM

The increased levels of information sharing has been mandated and has become standard policy among federal agencies,¹³ however the most dramatic increases of intelligence and information sharing are being seen between the Intelligence Community and various state government agencies. Although state and local officials are not currently slated to receive raw information and intelligence traffic, current information sharing concepts do not specifically exclude the sharing of this information. This increased intelligence and information sharing between the federal and state levels of government pose significant risks of increased unlawful and wrongful disclosure. These serious issues require urgent attention by the President and Congress. In addition, the Intelligence Community (IC), the Federal Law Enforcement Community (LEC), and State and local law enforcement must coordinate and cooperate to minimize the imminent dangers of unlawful and wrongful disclosure of classified information and intelligence. The potential consequences of unlawful disclosure ultimately cost lives and are a serious threat to national security. “A recent classified study of media leaks has convincingly shown that leaks do cause a great deal of harm to intelligence effectiveness against

¹³Terrorist Threat Integration Center (TTIC), URL: <<http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html>>, accessed 28 April 2004.

priority national security issues, including terrorism.”¹⁴ During a White House press conference Ari Fleischer stated that unauthorized disclosures threaten national security:

as a result of an unauthorized disclosure of intelligence information, it was revealed publicly that the United States had Osama bin Laden's satellite phone. As soon as it was publicly revealed, we never heard from that source again. We never again heard from that satellite phone. That can damage America's ability to know important information that this government needs to protect the country. Public disclosure of that information can damage our ability to protect the country.¹⁵

In addition, the USG spends billions of dollars on the collection of information. The compromise of these collection assets, through unlawful disclosures, significantly decreases their effectiveness. Effective safeguards and enforcement measures must be developed to balance the critical needs of national security with the corresponding need to share classified intelligence and information to enhance national security. The research supports the hypothesis that unlawful disclosures of classified information and intelligence will increase significantly during the new information sharing era unless specific safeguards are developed and vigorously enforced to protect these vital resources and their underlying sources and methods. These safeguards involve

¹⁴James B. Bruce, *Laws and Leaks of Classified Intelligence, The Consequences of Permissive Neglect*, Central Intelligence Agency Homepage, URL: <<http://www.odci.gov/csi/studies/vol47no1/article04.html>>, accessed 13 June 2004. James B. Bruce is the Vice Chairman, Director of Central Intelligence Foreign Denial and Deception Committee.

¹⁵Ari Fleischer, White House Spokesperson, Office of the Press Secretary, “White House Press Briefing,” briefing presented at the White House, Washington, DC, 20 June 2002, URL: <www.whitehouse.gov/news/releases/2002/06/20020620-12.html>, accessed 15 April 2004.

RESEARCH QUESTION AND HYPOTHESES

Research Question

The research question for this thesis is: What impact will increased sharing of classified information between Federal agencies and state and local agencies have on unauthorized or unlawful disclosures of classified information? This issue has direct implications for national security at a time in when domestic and transnational terrorism has increased significantly.¹⁶

Complementary Hypothesis

The following complementary hypotheses are based on the preliminary review of Federal statutes relating to information sharing and other related executive orders, regulations, and policies:

-- Unauthorized and unlawful disclosures of classified information related to dissemination to state and local agencies will increase.

-- The Intelligence Community must play an essential role in the development and implementation of increased information sharing mandates and policies to reduce and limit unauthorized disclosures of classified information due to dissemination to state and local agencies.

Key Questions

¹⁶U.S. Department of State, Bureau of Public Affairs, *Patterns of Global Terrorism 2003: Corrected Year in Review, Appendix A, and Appendix G* (Washington, DC: DOS Publication 31932, 2003). URL: <www.state.gov/s/ct/rls/pgtrpt/2003/>, accessed 23 June 2004.

1. What role does current information sharing statutes, executive orders, regulations, and policies play to enable or impede information sharing between Federal agencies and state/local agencies?
2. Are current safeguards for classified information effective and adequate?
3. What role should the stakeholders play in the development of information sharing and information protection policy and what are the significant implications for the Intelligence Community?
4. What recommendations and lessons learned can the Intelligence Community contribute reduce unauthorized disclosures of classified information at both the Federal and state/local levels?

ASSUMPTIONS

There are three assumptions that form the basis of this thesis. First, that information sharing will continue to increase among Federal agencies, and between those agencies and state and local agencies. Second, future terrorist attacks within the United States homeland are inevitable (it is not a matter of whether additional terrorist attacks will occur, but rather when and where). Finally, effective solutions can be developed to decrease the frequency and severity of unauthorized disclosures

METHODOLOGY

The two primary research methods are used to determine the validity of the hypotheses. First, applicable information sharing statutes, executive orders, regulations,

and policies will be reviewed and analyzed. In addition, scholarly materials related to information sharing, including related graduate-level research, will be reviewed to provide a political and cultural context to the information sharing statutes, executive orders, regulations, and policies. In addition, relevant research information, for example, was found in a Senate report titled *Joint Inquiry Into Intelligence Community Activities Before And After the Terrorist Attacks of September 11, 2001*.¹⁷

The second primary research method used was surveys and interviews. The information sharing survey group gathered the opinions of military and intelligence community officials, state and local law enforcement, and other government personnel with experience related to information sharing.

OVERVIEW OF CHAPTERS

Chapter Two reviews selected information sharing statutes, executive orders, regulations, and policies concerning information sharing. Chapter Three discusses the methodology of this thesis, including a justification for data collection, analytical methods and research procedures. Chapter Four is a case study of the recent Senate-White House Ricin incident that illustrates information sharing in operation and allows an evaluation of the effectiveness of information sharing. Chapter Five is an evaluation and discussion of the information and intelligence sharing survey results. Chapter Six provides several recommendations that could counter significant increases in unlawful and unauthorized disclosures of classified information and intelligence. Chapter Seven is

¹⁷U.S. Congress, Senate, Select Committee on Intelligence and House, Permanent Select Committee on Intelligence, *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Cong., 2d sess., 2002, S. Rept. 107-351, H. Rept. 107-792, 354 – 367. Cited hereafter as U.S. Congress September 11th Joint Inquiry.

a summary of the thesis and includes the key findings and their implications.

Recommendations for further research are also presented in the final chapter.

This research and the resulting recommendations will facilitate the USG's ability to share information with all available sources and agencies (both federal and state/local) and also gather information from these same sources. However, protection of this vital information and the dissemination of timely and actionable information and intelligence to the state/local levels must be effectively protected from unauthorized disclosure.

CHAPTER 2

REVIEW OF INFORMATION SHARING STATUTES, EXECUTIVE ORDERS, REGULATIONS, AND POLICIES

However much we like to think of government as one of laws and institutions, the personalities and relationships of the people filling these important positions also affect agency working relations.

-- Mark M. Lowenthal, *Intelligence: From Secrets to Policy*¹⁸

INFORMATION SHARING STATUTES

Although there has been considerable media attention on the controversial issue of information sharing since September 11, 2001, information sharing is not a completely new phenomenon. Prior to the Pearl Harbor attack Army and Navy Intelligence, as well as the FBI communicated regularly at weekly staff meetings about world conditions and monthly reports were also written.¹⁹ There was “immediate liaison with the FBI, the District Intelligence officer of the Navy, the FCC, and all the Territorial and Federal Departments such as customs, immigration and Treasury.”²⁰ It is well known that this coordination and communication was not sufficient to prevent the devastating Japanese attack on Pearl Harbor, however the concept and importance of information sharing was well understood as being critical to overall national and military security. In 1947, the

¹⁸Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2d ed. (Washington, DC: CQ Press, 2003), 30.

¹⁹Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), 36-38.

²⁰Wohlstetter, 37.

National Security Act²¹ became the statutory foundation for the reorganization of the United States government's foreign policy and military apparatus. This act also created the Central Intelligence Agency. In 1981, President Ronald Reagan signed Executive Order 12333,²² created what is commonly known as the "Intelligence Community (IC),²³ and established the essential groundwork for intelligence coordination between various federal and state agencies.

The two most comprehensive post-September 11, 2001 statutes dealing with information sharing, particularly between federal, state, and local government, are the Homeland Security Act of 2002²⁴ and the USA Patriot Act.²⁵ Despite the comprehensive nature of the Homeland Security Act and other statutes that address information sharing in the wake of the September 11th terrorist attacks, there are numerous practical, "grass-roots" issues that must be solved before effective, continuous, and seamless information sharing can occur. When the personnel or agencies are legally prohibited from sharing information due to a lack of the proper security clearances then frustration is inevitable and intelligence failures with increased risk of terrorist or enemy attack results. It is essential that all personnel be properly cleared before they handle classified material. Nevertheless, local law enforcement personnel are frustrated by the slow and backlogged security clearance process. "For months, local officials involved in homeland operations

²¹*National Security Act of 1947.*

²²U.S. President, Executive Order 12333, "United States Intelligence Activities," 4 December 1981, 1-2. Cited hereafter as U.S. President, EO 12333.

²³The Intelligence Community (IC) consists of the following federal executive agencies: CIA, NSA, DIA, GIA, NRO, DOS, FBI, DOT, DOE, and the intelligence elements of the military branches.

²⁴*Homeland Security Act of 2002*, Public Law 107-296 (2002). Information sharing between the Department of Homeland Security and other federal, state, and local agencies is mandated.

²⁵*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, 50 U.S.C. § 1804 (a)(7)(B). Cited hereafter as USA Patriot Act.

have complained about the complexity of obtaining federal clearances for their police and emergency response officials.” Michael Stanek, Minnesota Homeland Security Director, stated that “a major frustration is that different agencies have different procedures and standards for granting clearances, “not one of them [federal and state agencies] recognizes the other,” he said in an interview.²⁶ Many state and local government officials express similar frustrations about the Federal security clearance process that involves full background investigations and adjudication or determinations about granting or denying security clearances. However, federal officials have repeatedly warned of the security risks involved in broad distribution of security clearances.”²⁷ It is this possible overly “broad distribution of security clearance” that may necessarily follow increasing mandates for increased information sharing.

The USA Patriot Act was almost unanimously passed by Congress on 24 October 2001. Only six weeks after the terrorist attacks of September 11th this law granted new powers to law enforcement agencies and personnel to combat terrorism.²⁸ The provisions of the USA Patriot Act that are the most relevant to this thesis are those that relate to information sharing between federal law enforcement and state and local government (law enforcement and non-law enforcement).

²⁶Jim McGee, “Bush Greenlights Ridge on Security Clearances Outside Beltway,” *CQ Homeland Security: Government Reorganization*, 30 July 2003, URL: <<http://homeland.cq.com/hs/display>>, accessed 2 February 2003.

²⁷McGee, “Bush Greenlights Ridge,” 30 July 2003.

²⁸Alfred Cumming, “FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress,” *CRS Report for Congress* RL32336, “CRS Military and National Security,” Washington, DC: Congressional Research Service, Library of Congress, 6 April 2004), URL: <www.fas.org/man/crs/RL32336>, accessed 28 May 2004.

Although the USA Patriot Act directly addressed the issue of unauthorized disclosure of classified information by directing that procedures specified jointly by the Attorney General and the DCI govern the process.²⁹ In addition, the act authorizes \$25 million per year from 2003 to 2007 for “assistance programs that emphasize coordination . . . for sharing resources [and] combining intelligence . . . functions, and the development of policy, procedures . . . and other best practices.”³⁰ This basically entails using the standard security clearance procedures of the federal government. Currently these procedures have not been modified are effective and practical for granting security authorizations to state and local officials is undetermined.

The slow security clearance process adversely impacts state and local officials who believe that they have a “need to know” classified information and require security clearances to effectively fight crime, including terrorism. Federal personnel also complain about the security investigation backlog.³¹ According to Carol Schuster, Associate Director, National Security Preparedness Issues, “over half of the 530 investigations we examined took over 204 days to complete. Less than 1 percent took less than 90 days, and 11 percent took more than a year.”³² The administrative process of obtaining required background investigations and clearances is slow and severely

²⁹USA Patriot Act § 403-5d(1).

³⁰USA Patriot Act § 221.

³¹U.S. Congress, House, Sub Committee on National Security, Veterans Affairs, and international Relations, Committee on Government Reform, *Inadequate Personnel Security Investigations Pose National Security Risks: Statement of Carol Schuster, Associate Director, National Security Preparedness Issues, National Security and International Affairs Division, Hearings, 106th Cong., 2nd sess., 16 February 2000, H. Rept. 106-152, URL: <www.loyola.edu/dept/politics/intel/hserial106-152>, accessed 5 June 2004. Cited hereafter as U.S. Congress, Sub Committee on National Security, *Personnel Security Investigations*.*

³²U.S. Congress, Sub Committee on National Security, *Personnel Security Investigations*, 3.

backlogged. Nevertheless, since USG law and policy has directed that federal agencies share information and intelligence with state and local officials and agencies, then the administrative process that supports these mandates must be updated and energized to keep pace with the increased demand for security clearances. In addition, there are significant changes in the security investigation and adjudication process that must be made in order to adequately protect classified information as the number of state and local personnel who are granted security clearances increases.

EXECUTIVE ORDERS

Various executive orders over the last twenty-three years address information sharing and the protection of information from unauthorized disclosure. For example, since December 1981, provisions of executive order 12333 mandate and encourage information sharing between agencies and departments.³³ Other relevant executive orders include executive orders 13231, 13228, and 12958, these executive orders address Critical Infrastructure Protection, Homeland Security, and Classified National Security Information, respectively. The following is a brief discussion of each of the current executive orders that address information sharing or unauthorized disclosure of information. Executive orders are one of the primary methods for the President to implement policies and exercise direction over executive agencies.

³³U.S. President, EO 12333.

Executive Order 12333, United States Intelligence Activities³⁴

The key provision of E.O. 12333 relating to information sharing states that “all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.”³⁵ However, E.O. 12333 also states that “maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community,”³⁶ It could be argued that Some might argue that analytical competition and superiority requires that agencies limit sharing or not share their best information with other agencies to maintain their own analytical edge. Clearly, the agency with the best information should emerge with the best intelligence product. The inherent problem with such a view is that the current threats against U.S. national security are so complex that most, if not all, agencies, including the Central Intelligence Agency or the Defense Intelligence Agency, must rely on other federal agencies and state and local governments for timely and relevant information to develop actionable intelligence. No agency can produce effective actionable intelligence in a vacuum. Key provisions of E.O. 12333 include the following:

The Director of Central Intelligence shall establish such boards, councils, or groups as required for the purpose of obtaining advice from within the Intelligence Community concerning: (1) Production, review and coordination of national foreign intelligence; (2) Priorities for the National Foreign Intelligence Program budget; (3) Interagency exchanges of foreign intelligence information; (4) Arrangements with foreign governments on intelligence matters; (5) Protection of intelligence sources and methods; (6) Activities of common concern; and (7) Such other matters as may be referred by the DCI.³⁷

³⁴U.S. President, EO 12333.

³⁵U.S. President, EO 12333, 1:1.d.

³⁶U.S. President, EO 12333, 1: 1.1a.

³⁷U.S. President, EO 12333.

Executive Order 13231, Critical Infrastructure Protection

“Information Sharing . . . with industry, State and local governments, and nongovernmental organizations to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers established on a voluntary basis by industry, and other related operation centers.”³⁸ This executive mandate requires coordination between all federal, State and local agencies that involve or are relevant to the protection of USG and private critical infrastructure. Furthermore, “. . . in this and other related functions, the Board shall work in coordination with the NCS, the Federal Computer Incident Response Center, the NIPC, and other departments and agencies, as appropriate.”³⁹

Although the focus of executive order 13231 is infrastructure protection, there was very little emphasis on protecting the critical infrastructure from within. However, the internal threat of unlawful disclosure and internal compromise is recognized as being the most vulnerable aspect of critical infrastructure protection.⁴⁰

Executive Order 13228, Homeland Security and Homeland Security Counsel

This provision is one of the cornerstones of the new mandate for federal agencies

³⁸U.S. President, EO 13231, “Critical Infrastructure Protection in the Information Age,” 16 October 2001, 5(b). Cited hereafter as U.S. President, EO 13231.

³⁹U.S. President, EO 13231.

⁴⁰Clay Wilson, “Network Centric Warfare: Background and Oversight Issues for Congress,” *CRS Report for Congress* RL32411, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, 2 June 2004), URL: <www.fas.org/man/crs/RL32411>, accessed 12 June 2004.

to share information and intelligence down to the state and local levels. The primary thrust of the executive order is its emphases on both “dissemination” and “exchange” of information. However, this executive mandate for sharing and disseminating information is apparently limited by applicable law and by the circumstances that would require information sharing for homeland security purposes. The purpose of executive order 13228 is to:

ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities. Executive departments and agencies shall, to the extent permitted by law, make available to the Office all information relating to terrorist threats and activities within the United States.⁴¹

The vague limiting references to “permitted by law” which appears in many executive orders is a catch-all phrase that is intended to alert the reader that other applicable laws or regulation may apply to the particular situation. Currently there is a comprehensive mandate from the President to evaluate all laws and regulations related to information sharing to determine whether these laws, regulations, or executive orders prevent, hinder, or encourage information sharing⁴² In addition, information sharing is encouraged only to the extent that it does not compromise national security or the protection of the information in the process. The Executive branch and Congress

⁴¹U.S. President, Further Amendment to Executive Order 13228, as amended, “Creation of Office of Homeland Security and Homeland Security Counsel,” 8 October 2001, URL: <[www.whitehouse.gov/news/releases/2001/10/20012.html](http://www.whitehouse.gov/news/releases/2001/10/20011020012.html)>, accessed 25 April 2004. Cited hereafter as U.S. President, EO 13228.

⁴²Richard A. Best, Jr., “Homeland Security: Intelligence Support,” *CRS Report for Congress* RS21283, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, updated 23 February 2004), URL: <www.fas.org/RS21283>, accessed 28 May 2004.

understand that an appropriate balance must be found between sharing information and protecting the information from unauthorized disclosures.⁴³

Executive Order 12958, Classified National Security Information⁴⁴

It is clear that executive order 12958 illustrates the difficult challenges involved with the maintenance of secrecy for national security purposes and the need for openness in a democratic society. Despite the challenges, executive order 12958 reaffirms the policy that “protecting information critical to national security remains a priority.”⁴⁵ The executive order requires that the USG have a

uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government Our Nation’s progress depends on the free flow of information. Nevertheless . . . national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our homeland security.⁴⁶

Although protecting national security information is a priority, so is sharing this information with appropriate government officials at all levels of government. Hoarding or blindly protecting information becomes illogical and directly contradicts that underlying basis for protecting the information. Ironically, protecting national security is

⁴³Harold C. Relyea, *Homeland Security: The Presidential Coordination Office*, *CRS Report for Congress* RL31148, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, updated 30 March 2004), URL: <www.fas.org/man/crs/RL31148>, accessed 28 May 2004.

⁴⁴U.S. President, Executive Order 12958, “Classified National Security Information,” 17 April 1995, 1-2. Cited hereafter as U.S. President, EO 12958.

⁴⁵U.S. President, Further Amendment to Executive Order 12958, as amended, “Classified National Security Information,” 25 March 2003, under “White House News Releases,” URL: <www.whitehouse.gov/news/releases/2003/03/20030325.html>, accessed 25 April 2004. Cited hereafter as U.S. President, EO 12958.

⁴⁶EO 12958.

simultaneously the reason for sharing and protecting classified information. When classified information is needed by a State or local government shareholder, or by a foreign partner nation, to counter or defeat a terrorist threat, then appropriate “tearlines”⁴⁷ must be developed and used. Ultimately, protection of classified information must yield to the mandate to share classified information, at some point, before disaster strikes. Nevertheless, the challenge remains to determine when this critical point is reached.

REGULATIONS

The following selected U.S. Army regulations illustrate how U.S. law and policy are implemented. Each branch of the military and many Federal agencies have specific regulations that relate to access to and release of official information, external collaboration, and coordination and dissemination of finished intelligence or raw information⁴⁸. Specific details about these issues related to classified information are unavailable due to their classification level. As indicated, these selected regulations focus on the capabilities, limitations, and responsibilities concerning collaboration and sharing of information between the Army and other agencies. It is interesting to note that specific agency regulations are generally more protective than the apparent mandates of executive order pronouncements or statutory requirements. This may indicate that that agency cultural attributes often override policy goals concerning information sharing.

⁴⁷“Tearline” is a term commonly used by Intelligence Community (IC) personnel and Law Enforcement (LE) to describe discrimination point between information that is classified and information that is not. Tearlines are used within the IC and LE communities to discriminate between various levels of classification prior to the dissemination of that information.

⁴⁸U.S. Army Regulation (AR) 381-10, U.S. Army Intelligence Activities (Washington, DC: Department of the Army, July 1984). Cited hereafter as U.S. AR 381-10; Department of Defense (DoD) Directive 5240.1, DoD Intelligence Activities (Washington, DC: Department of Defense, April 1988). Cited hereafter as DoD Directive 5240.1.

However, it may also indicate that specific agency regulations and actual practice on information sharing are actually consistent with the prevailing political will. The cultural nuances reflected in agency information sharing regulations and policies either support or frustrate national information sharing initiatives.

Other US Army regulations that address the release or dissemination of information or intelligence include:

- Access to and Release of Official Information⁴⁹
- External Collaborative Computing Security Policy⁵⁰
- Coordination and Dissemination of Finished Intelligence Publications⁵¹

The underlying policy concern for these regulations is the maintenance of the delicate balance between providing access to classified information to personnel who require the information for legitimate USG purposes and the protection of information from unauthorized disclosure.

POLICIES

In late February 2004, Secretary Tom Ridge made a clear policy statement and set a target date concerning Federal agency information sharing with State and local government governments. Secretary Ridge stated: “we will secure real-time nationwide connectivity between all 50 states and territories. This will mean

⁴⁹U.S. Army Regulation (AR) 10-22, Access to and Release of Official Information (Washington, DC: Department of the Army, March 2003). Cited hereafter as AR 10-22.

⁵⁰U.S. Army Regulation (AR) 11-2, External Collaborative Computing Security Policy (Washington, DC: Department of the Army, 29 August 2003). Cited hereafter as AR 11-2.

⁵¹U.S. Army Regulation (AR) 51-4, Coordination and Dissemination of Finished Intelligence Publications (Washington, DC: Department of the Army, 28 April 2000). Cited hereafter as AR 51-4.

multi-directional information sharing — the first phase of which, cyber-connectivity, will be completed within the next three months.”⁵² In addition to this recent statement by Secretary Ridge there are other indicators of the USG policy concerning information sharing with state and local government. Federal law enforcement agencies like the FBI have

formed a state and local law enforcement advisory committee that is designed to foster cooperation between the bureau and their local counterparts. And perhaps even more significantly, in his recent reorganization of the FBI, Director Mueller created the Office of Law Enforcement Coordination. This office is tasked specifically with ensuring that the actions of the FBI's various components are coordinated with, and communicated to, state and local law enforcement agencies throughout the nation.⁵³

Initiatives such as this on by the FBI and other mandated cooperative actions by other federal agencies have made information sharing a stated priority for all federal agencies involved in the war on terrorism and national security. The part that makes these information sharing initiatives unique is the new emphasis on sharing with state and local officials. The USG in general and agencies like the FBI only share information because of the legal requirement to do so, but there is an overall reluctance to share information, even with other federal agencies. This reluctance increases when the state and local agencies are involved. Federal agencies have no problems with receiving information from the state and local levels, but the problems and barriers arise when “sharing” involves the flow of information from the federal level to the state and local levels.

There is a long history involving challenges concerning access to USG or FBI

⁵²Alice Lipowicz, “Ridge Proposes Plan to Link First Responder Radios,” CQ Homeland Security: Local Response, 23 February 2004, URL: <<http://homeland.cq.com/hs/display>>, accessed 29 April 04.

⁵³U.S. Congress, Senate, 198th Cong., 1st sess., 1245, S. Doc. 98-16, 10. URL: <<http://elibrary.bigcalk.com>. Security and Intelligence Community: Chief Bill Berger, Congressional Testimony.

information. As noted earlier, there are organizational cultural hurdles that must be addressed, but it is possible that some cultural norms have merit. The reluctance of federal agencies to enthusiastically share information with state and local agencies could stem from a legitimate concern that increased information sharing is counterproductive under certain circumstances. The case study in Chapter 4 addresses this issue. As previously mentioned, this tension between agencies like the FBI and outsiders is not new.

Since the days of J. Edgar Hoover, state and local officials . . . complained that the [FBI] is highhanded with its local counterparts and . . . looks for any excuse not to share even the most innocuous intelligence information. It will still be impossible to share certain, highly classified national security information.⁵⁴

The lack of cooperation and other challenges appear to be continuing in the post-11 September, 2001 era based on the accounts of state and local officials.

Despite the stated USG policy on information sharing there are clear indications that the stated policy conflicts with the actual situation in the field. Local LE officials have expressed serious concerns about the lack of cooperation on information sharing. “Baltimore's police commissioner says he was dumbfounded to learn that the Federal Bureau of Investigation would give him the names of suspects who might be connected to the September hijackings but not their photographs.”⁵⁵ This is a real-world indication that information sharing between the federal and state levels, or in this case, between an IC member and local LE is not consistent with the stated policy that requires information sharing take place seamlessly. However, security concerns on the part of the FBI could

⁵⁴Philip Shenon, “Local Officials Accuse F.B.I. of Not Cooperating,” *The New York Times*, 12 Nov 2001, B6.

⁵⁵Shenon, “Local Officials Accuse F.B.I.,” B6.

have been a factor that dictated this situation. Other similar situations have occurred nationwide.

Another example of poor information sharing that may indicate a disconnect between policy and practice involves the mayor of Reno, Nevada who was "shocked to learn from a local television reporter -- not from the F.B.I. -- that the bureau had seized a suspicious letter from a local Microsoft office and that a preliminary test indicated it was laced with anthrax. Two months after state and local law enforcement officials found themselves forced onto the front lines of a global war on terrorism, many are complaining that the F.B.I. is refusing to provide them with the information they need to protect their communities."⁵⁶ This example is consistent with the experience of other federal officials.

Additional challenges exist between the FBI and local police officials who understand the local situations and can be instrumental with intelligence collections and investigations. According to Louis J. Freeh of the FBI:

I understand what the F.B.I. is about -- it's all about culture and elitism," said Chief Michael J. Chitwood in Portland, ME. "Sept. 11 should have changed all that. But it didn't. Sept. 11 showed that there are terrorists who lived among us. Who better to know these people than the local police?" He said the exchange of information with the F.B.I. remained "a one-way street," with the bureau accepting information but offering none in return. The city's police were quickly drawn into the Sept. 11 investigation after it was discovered that two of the hijackers had spent their final night in Portland.⁵⁷

Based on this statement, Mr. Feech appears to understand the tension between the FBI and local police and honestly admitted to the Senate Committees on Appropriations,

⁵⁶Shenon, "Local Officials Accuse F.B.I." B6.

⁵⁷Shenon, "Local Officials Accuse F.B.I." B6.

Armed Services, and the Select Committees on Intelligence that there is a problem and that local police are part of the ultimate solution for optimal national security.

It is interesting to note that prior to the September 11th, 2001 terrorist attacks changes in USG policy on information sharing were underway:

In an effort to keep pace with the changing terrorist threat to the United States, the FBI is implementing a new management and operational initiative to further strengthen its ability to combat terrorism. This initiative, referred to as MAXCAP05, has as its goal the achievement by Fiscal Year 2005 of five core competencies or capacities for its Counterterrorism Program: investigative, intelligence, communications, liaison, and program management.⁵⁸

Another policy indicator involves information sharing between the Immigration and Naturalization Service (INS) and other agencies, including state and local coordination and communications. Janice L. Jacobs, Deputy Assistant Secretary of State for Visa Services stated the following at a hearing concerning information sharing, before the Senate Committee on the Judiciary, Subcommittee on Immigration:

I appreciate the opportunity to address you on a subject that all of us in the executive and legislative branch agree is crucial: the swift and proper exchange of information among relevant agencies controlling the security of our borders. The Department of State's visa work abroad constitutes the "forward based defense" of the United States against terrorists and criminals who seek to enter the country to harm us. We have no higher responsibility and we are determined to do this work in the best and most comprehensive manner possible.⁵⁹

Ms. Jacobs' testimony indicates that effective information sharing policy in action does help protect national security and U.S. borders. These are merely a few of the example

⁵⁸U.S. Congress, Senate, Committees on Appropriations, Armed Services, and Select Committee on Intelligence, *Threat of Terrorism to the United States: Statement for the Record, Louis J. Freeh, Director, Federal Bureau of Investigation*, 99th Cong., 1st sess., 10 May 2001. Cited hereafter as U.S. Congress, Senate, *Threat of Terrorism*.

⁵⁹U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Immigration, *Hearing on Information Sharing: Testimony of Janice L. Jacobs, Deputy Assistant Secretary of State For Visa Services*, 107th Cong., 2d sess., 15 July 2003. S. Rept. 107-48. URL: <<http://travel.state.gov/testimony8.html>>, accessed 22 March 2004.

where seamless communication and information sharing can make a huge difference if it is done in a way that protects the information from unauthorized disclosure.

UNLAWFUL DISCLOSURE STATUTES

One of the many ways to determine the overall policy on a particular issue entails an evaluation of the penalties the USG attaches to violations of the laws concerning the particular policy issue. The penalties for the unauthorized disclosure of information range from administrative discipline to life imprisonment. The question as to whether an officer or employee of the U.S., or other person, violated any unlawful disclosure statute depends on the circumstances surrounding the alleged violation.

It is critical to note that the jurisdiction or power of these statutes extend and apply to any person, not merely U.S. government personnel. However, First Amendment protections insulate the media from prosecution because of the deference given to freedom of the press and freedom of speech when weighed against the “safety or interest of the United States.” The challenge here is due to the concern that unlawful disclosure may cause an undue suppression of protected free speech or free press that are contrary to the values and principles of the U.S. Constitution and strike at the core of American values.

The following statutes illustrate the depth and breadth of government efforts to protect national security information from unauthorized disclosure. The penalties for violating these statutes vary, but are an indication of USG policy through the legislative. Given the magnitude of the damage that unauthorized disclosure can cause to the national

security, the penalties for violation are relatively lenient as compared to other federal crimes.

The potential punishment for disclosure of classified information under 18 United States Code section 278 is serious, but not in relation to the more severe penalties for other federal crimes. This section states that

whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, . . . or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information . . . shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.⁶⁰

Although military and defense information is potentially among the most sensitive U.S. government information, it is surprising that Congress did not decide to make the penalties for unauthorized disclosure of defense information significantly more serious than for the disclosure of other types of government information. For example, gathering, transmitting or losing defense information “that the President has determined would be prejudicial to the national defense shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.”⁶¹

Concerning public money, property or records, “whoever embezzles, steals, purloins, or knowingly converts his use or the use of another, or without authority, sells,

⁶⁰18 U.S.C. § 798, Disclosure of Classified Information.

⁶¹18 U.S.C. § 793, Gathering, Transmitting or Losing Defense Information.

conveys or disposes of any record ...or thing of value of the United States or of any department or agency.⁶²

The most serious offenses related to unauthorized disclosures involve situations where a person or persons are gathering or delivering defense information to aid a foreign government.⁶³ According to this applicable statute, it is more egregious to provide any USG information or materials to a foreign government, even if the information or materials are not classified. Rather than to focus on the classification of the material, the threshold for violating this statute is whether the information or material is can potentially harm USG interests. The penalty provision of the statute reads:

Whoever, with intent or reason to believe that it is to be used to the injury of the United States . . . communicates, . . . or attempts to communicate . . .to any foreign government, . . .directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.⁶⁴

In addition, statutory protection for the identities of USG undercover intelligence officers is provided and violators face a maximum of ten years imprisonment.

⁶²18 U.S.C. § 641, Public Money, Property or Records.

⁶³Glen P. Hastedt, *Espionage: A Reference Handbook* (Santa Barbara, CA: ABC-CLIO Press, 2003), 181. According to Hastedt, "CIA counterintelligence officer Aldrich Ames and his wife, Rosario, pleaded guilty to charges of spying for the Soviet Union . . . considered the most damaging spy case in U.S. history. Ames spied between 1985 and 1994. His information was linked to the deaths of at least nine [U.S. Government] agents."

⁶⁴18 U.S.C. § 794, Gathering or Delivering Defense Information to Aid Foreign Government.

CHAPTER 3

METHODOLOGY

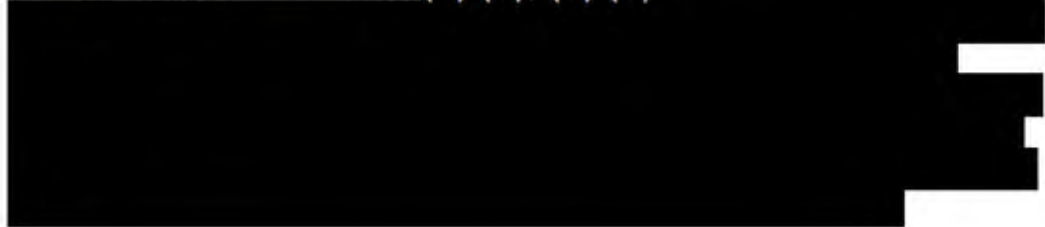
Research Procedures

The instruments used for this thesis consisted of a primary and secondary research sources, survey (electronic and hard-copy), and interviews (in-person and telephonic). Standard academic research techniques and procedures were used for this thesis. The survey population consisted of the following categories of persons: Military Officials, Intelligence Community Officials, Federal Elected Officials, State Elected Officials, State Law Enforcement or Emergency Response Officials, Local Elected Officials, Local Law Enforcement and Emergency Response Officials, and other persons within and outside the intelligence community with experience related to information sharing.

The focus of the research for this thesis was open source. Although numerous classified documents were reviewed, no information or data from these documents are included in any written portion of this thesis. A separate classified bibliography was prepared for future research.

Field research materials from several conferences, including one sponsored by the Terrorist Threat Integration Center (TTIC), were used for research. In the Spring 2004 in Chantilly, Virginia, presentations by the following persons (or their representatives):

John Brennan, Director TTIC; (b) (3), (b) (6)



(b) (3), (b) (6)

John Surina,
Deputy Assistant Secretary for Administration, Department of Agriculture;

(b) (3), (b) (6)

and Russell Travers,
Associate Director for Defense Issues, TTIC (see Appendix F).

In addition, research concerning information sharing was obtained from attendance at the Information Sharing Working Group (ISWG) meetings held at the State Department in the spring of 2004. The information obtained from the ISWG meetings is not specifically mentioned in this unclassified version of this research project. However, the insight and perspectives gained from the ISWG were valuable parts of the overall research and critical thinking phases of this thesis project. The ISWG discussed and developed solutions for complex inter-agency issues concerning information sharing.

One of the most important topic discussed involved the protection of compartmented information and the compatibility of information systems between agencies. Participation at these conferences and meetings provided exposure to discussions that developed proposed solutions and recommendations for improving information sharing and overcoming information sharing challenges, including security concerns and institutional cultural barriers.

The focus of the discussions at most of the related conferences and meetings focused on the how the tragic events of 11 September 2001 prompted the President, Congress, Federal and State agencies, and private companies to determine what information sharing challenges existed that could have prevented the terrorist attacks on the World Trade Center and the Pentagon. Investigations and reports reveal that there might not have been anything that could have been done to prevent these terrorist attacks.

Nevertheless, it is clear that unauthorized disclosure of classified information (purposefully or inadvertently) to any person or entity that intends to do harm to the national security of the USG is a challenge that must be urgently addressed, according to most experts.

CHAPTER 4

CASE STUDY: RICIN INCIDENT AT SENATE-WHITE HOUSE

Secret Service did not immediately inform the FBI, the U.S. Postal Inspection Service or other agencies about the White House letter [containing ricin] when it was discovered . . . delay lasted weeks.

-- Dan Eggen, *The Washington Post*⁶⁵

INTRODUCTION AND OVERVIEW

This case study focuses on an actual situation involving possible terrorist incidents that occurred at the U.S. Senate and the White House. The incidents are instructive because they illustrate how information sharing mandates, combined with various institutional cultural norms and behavior patterns, produced an environment where information sharing was not a priority and parochial interests prevailed over the national interest. The case contains many issues that implicate leadership, internal agency policies, and government policy, but the focus of this case study will be on information sharing of classified or sensitive information between USG agencies and organizations involved in the same or similar incident.

On 2 February 2004, “a white powdery substance [was] found near a pile of mail in [the office of] Senate Majority Leader Bill Frist . . . authorities announced that [the] substance was tentatively identified as ricin, and further tests [on 3 February] confirmed

⁶⁵Dan Eggen, “Letter With Ricin Vial Sent To White House: November Discovery Was Kept Quiet,” *Washington Post*, 4 February 2004, A7.

the presence of the poison.”⁶⁶ Senator Frist’s office is located in the Dirksen Senate Office Building on Capitol Hill in Washington, DC (see Map 1).

On 3 February 2004, it was revealed (leaked) that the U.S. Secret Service intercepted a letter containing powdered ricin in a metal vial. The letter was intercepted at an off-site mail sorting facility used by the White House.⁶⁷ The name of the addressee on the letter was not publicly disclosed by the Secret Service. However, the letter was signed ““Fallen Angel” and contain[ed] complaints about trucking regulations.”⁶⁸ Four months earlier, on 15 October 2003, a letter containing powdered ricin in a metal vial was found in a mail sorting facility in Greenville, South Carolina. This letter contained complaints about trucking regulations and was signed “Fallen Angel.”

In the South Carolina [ricin] case, “the Centers for Disease Control and Prevention [CDC] were called in to test the mail facility and its workers. The FBI also released detailed information about the case and . . . announced a \$100,000 reward for information leading to a conviction.”⁶⁹ There was immediate information sharing, analysis, and coordinated action to ensure the safety of the people potentially exposed to the ricin and concern for overall national security.

⁶⁶Eggen, “Letter With Ricin,” A7.

⁶⁷“Ricin, a poison derived from the castor bean, is easy for practically anybody to make, and it is so deadly—there is no cure—even a tiny amount may be sufficient to kill. In fact, ricin is so easily made that ricin-related incidents occur every few years in the United States.” Law Enforcement Agency Resource Network, <http://www.adl.org/Learn/news/ricin_threat.asp>, accessed 17 March 2004.

⁶⁸Eggen, “Letter With Ricin,” A7.

⁶⁹Eggen, “Letter With Ricin,” A7.

In the Senate ricin case over sixteen government employees were force to decontaminate and at least four government buildings, including the Dirksen Senate Office Building was shutdown. Immediate information sharing occurred at the initial evacuation stages of the incident, but both information sharing and coordination of efforts decreased with time.

In the White House ricin case information about the incident was not reported by the Secret Service to the CDC, Federal Bureau of Investigation (FBI), or any others federal, State, or local agencies that are responsible for investigation, containment, decontamination, or intelligence analysis. The White House ricin incident originally occurred in November 2003 and was finally revealed by a “law enforcement official in the administration, who declined to be identified by name or agency.”⁷⁰ According to Ann Roman, a Secret Service spokesperson, there is an “ongoing investigation” into the White House ricin incident. “Roman declined to comment on details of the case or why it was kept secret, citing the ongoing investigation. Roman also declined to say whether workers at the mail facility were tested or underwent decontamination procedures, and said the facility's location was kept secret for security reasons.”⁷¹

CASE STUDY ANALYSIS

All of the federal and State agencies involved with this real-world ricin scenario (case study) between November 2003 and June 2004 did not fully and effectively communicate, coordinate, or cooperate in a manner that was consistent with current

⁷⁰Eggen, “Letter With Ricin,” A7

⁷¹Eggen, “Letter With Ricin,” A7

mandated intelligence sharing initiatives. In addition, on 14 May 2004, Attorney General John Ashcroft announced the completion and initiation of the National Criminal Intelligence Sharing Plan. This Department of Justice (DOJ) initiative is designed to ensure “that all of its [federal] components are effectively sharing information with each other and the rest of the nation’s law enforcement community.”⁷²

APPLICABLE INFORMATION SHARING POLICY AND PROCEDURES

The National Criminal Intelligence Sharing Plan includes actions by DOJ and other federal, state, local, and tribal agencies. The basic concept of the plan “represents law enforcement’s commitment to take it upon itself to ensure that the dots are connected, be it in crime or terrorism.”⁷³ The provisions of the DOJ Intelligence Sharing Plan apply to the ricin incidents at the Senate, the White House, and in South Carolina. Information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant . . . federal officials contended a variety of issues impeded effective information exchange, ranging from the "inability of state and city officials to secure and protect classified information" to a lack of integrated databases.⁷⁴

⁷²Department of Justice, “National Criminal Intelligence Sharing Plan Fact Sheet,” *DOJ Press Release, 14 May 2004* (Washington, DC: DOJ, 2004), URL: <www.fbi.gov/dojpressrel/pressrel04/factsheet051404.htm>, accessed 21 May 2004. Cited hereafter as DOJ, *Press Release*.

⁷³DOJ, *Press Release*.

⁷⁴Martin E. Andersen, “Counterterror Data Unsatisfactory, Locals Tell GAO,” *CQ Homeland Security: Intelligence*, 27 August 2003, URL: <<http://homeland.cq.com/hs/display>>, accessed 29 May 2004.

The DOJ Intelligence Sharing plan and other information sharing statutory and policies about the urgent need for information sharing and cooperation are only effective if the personnel involved share that information with other agency personnel. It is especially important that the agencies that possess potentially relevant information actually share that information with other agencies that may need it. The best plans are only effective if there is an actual commitment to follow the plan's provisions and the spirit of those provisions. Did the relevant agencies involved in the ricin case study follow the letter and spirit of the current USG policy on information sharing? Clearly, they did not. However, a review of the actual challenges involved with the case and the agencies reveals that effective information sharing was frustrated by concerns about unlawful disclosure of classified or sensitive information. Agency concerns about the maintenance of secrecy and fear of unlawful disclosure may be the primary reasons behind the problems undercutting information sharing initiatives.

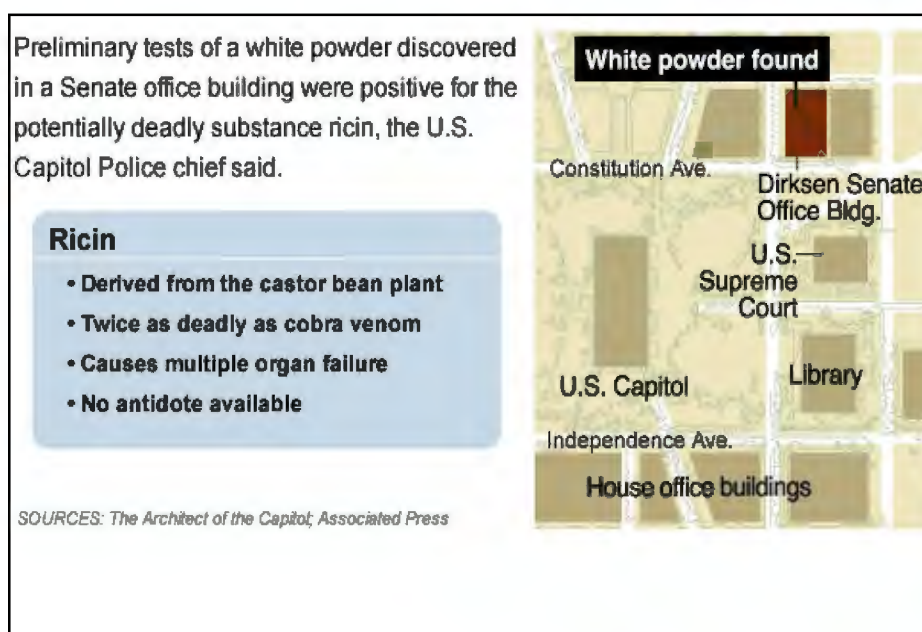
An interview with a government official who was closely involved with the Senate ricin incident confirmed that Dan Eggen's Washington Post article is accurate. Major progress in the information sharing realm has been made since September 11th, 2001, however there are still significant ongoing information sharing challenges (problems) between federal agencies, and between federal and state agencies.⁷⁵

CONCLUSION

According to a senior-level federal law enforcement official cooperation and information sharing among the government agencies "worked well at the lower levels,"

⁷⁵A source, senior-level law enforcement professional at a national law enforcement organization who wishes to remain anonymous, interview by the author, 15 June 2004.

however a “distinct level of distrust was [still] evident.”⁷⁶ This environment made agency personnel reduce the dissemination of information because of the concern that information would be leaked. This distrust led to a lack of equal access to investigative leads and reduced the probability of “connecting the dots” with other similar ricin related incidents. For example, the remarkable similarities between the South Carolina ricin incident and the White House ricin incident was not revealed for four months because the Secret Service decided not to share this information with other federal or state agencies.



MAP 1. Capitol Hill Area Where Senate Ricin Incident Occurred

Sources: *The Architect of the Capitol* and Associated Press

Poor information sharing procedures and practices were used during the Senate-White House ricin incidents. It appears that fear of unauthorized disclosure and actual unauthorized disclosures were factors that limited effective information sharing. This case study illustrates how information sharing mandates, such as the National Criminal

⁷⁶Anonymous source interview, 15 June 2004.

Intelligence Sharing Plan, conflicted with organizational cultural practices that resulted in an environment where information sharing was not seen as a priority. Distrust and fear of unlawful disclosure were cited as the reasons for not sharing information. Ultimately, parochial interests prevailed over the national interest.

CHAPTER 5

INFORMATION SHARING SURVEY

Real knowledge is to know the extent of one's ignorance.

-- Confucius

Imagination is more important than knowledge.

-- Albert Einstein

MILITARY AND INTELLIGENCE COMMUNITY OFFICIALS

The underlying basis for the increased need for information sharing in the post-September 11th era is increased necessity for collaboration to protect national security.

The unique and ambiguous challenges associated with counterterrorism require a greater understanding of the enemy. In addition, even greater understanding of the available information, and other resources, that all agencies (Federal, state, and local) have related to a particular threat is essential.

The collaborative “mind-set” requires a departure from the traditional intelligence cycle. The “target-centric approach” discussed by Dr. Robert M. Clark is the transparent foundation of the new information sharing era (see figure 1). The target-centric intelligence process seeks to “make all stakeholders (including customers) part of the intelligence process. Stakeholders in the intelligence community include collectors, processors, analysts, and the people who plan for and build systems to support them. Customers could include the president, the National Security Council staff, military

command headquarters, diplomats, the DHS, [and] local law enforcement.”⁷⁷ According to the information sharing survey seventy-five percent of the intelligence community agreed that a target-centric approach is sometimes the most effective process and the other twenty-five percent considered the target-centric process to be effective most often. These results mean that the great majority of personnel in the intelligence community still adhere to the notion that the traditional intelligence cycle is effective. This possibly indicates that cultural resistance to innovations in the collaborative process. This resistance could undermine information sharing initiatives, but a significant amount of the resistance to change is a result of mistrust, competition, and several statutes, regulations, and policies that impede information sharing. According to the findings in a recent General Accounting Office (GAO) report to the Secretary of Homeland Security, "information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant."⁷⁸ This finding by GAO raises additional, and far reaching, issues concerning information sharing. Information sharing and the concerns about minimizing unauthorized disclosure do not address the critical importance of shared information being timely, accurate, and relevant. Protection of shared information is vital, but actionable information is also vital.

The Robert Clark’s chart on the target-centric approach (Figure 1) does more that illustrate a more effective approach and alternative to the traditional intelligence cycle. Both the target-centric intelligence gathering approach and the traditional intelligence

⁷⁷ Robert M. Clark, *Intelligence Analysis: A Target Centric Approach* (Washington, DC: The CQ Press, 2004), 17.

⁷⁸ United States General Accounting Office Report for the Secretary of Homeland Security, August 2003. URL:// <<http://www.gao.gov/cgi-bin/getrpt>>, accessed 9 Feb 2004.

cycle reveal the areas of vulnerability for unauthorized disclosures of classified
information.

(b) (3)



(b) (3)



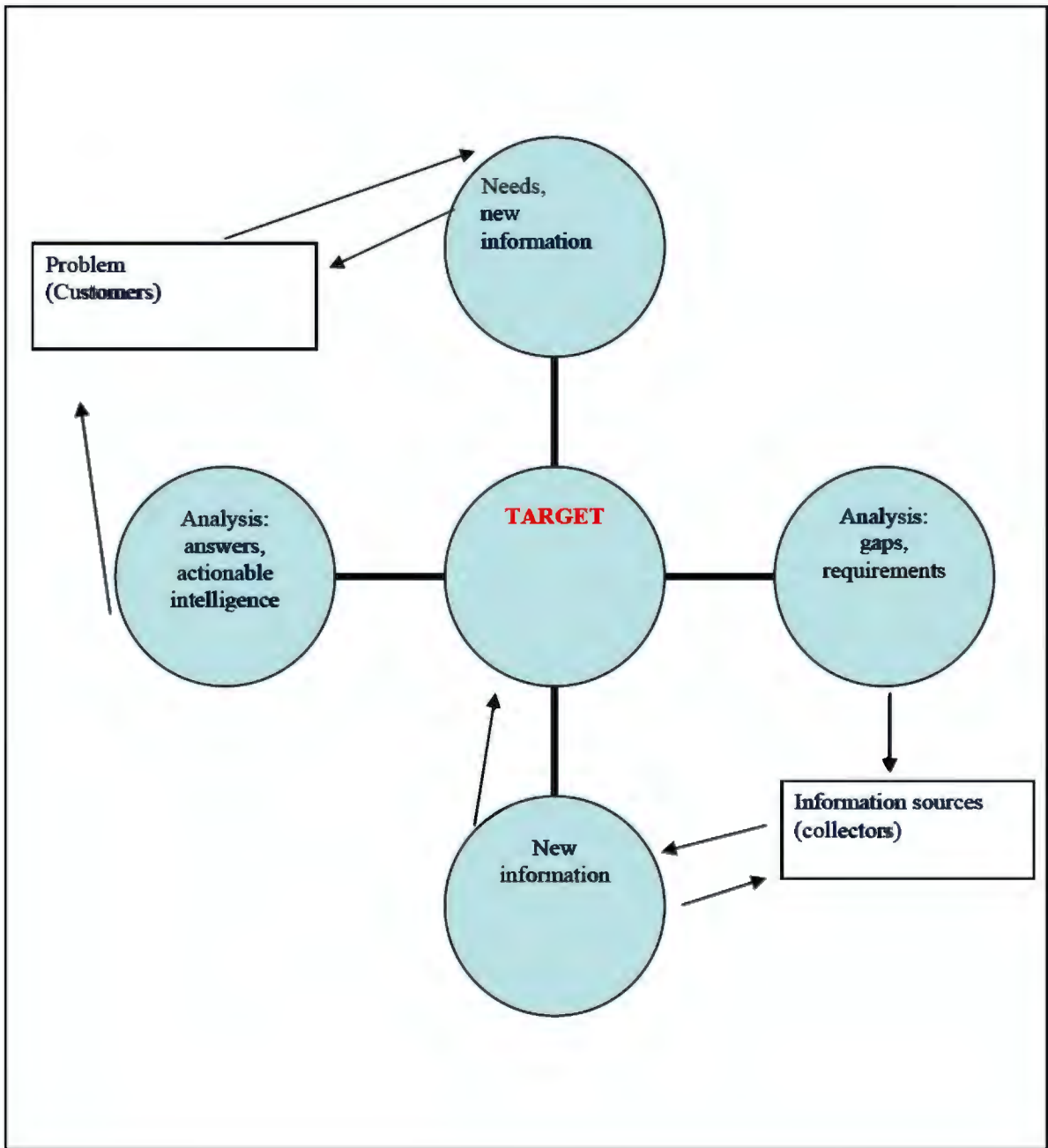


Figure 1. A Target-Centric View of the Intelligence Process⁸²

Source: Robert M. Clark, *Intelligence Analysis: A Target Centric Approach*

⁸²Robert M. Clark, *Intelligence Analysis: A Target Centric Approach* (Washington, DC: The CQ Press, 2004), 18.

According to question six (Table 3) of the information sharing survey an equal percentage of respondents thought that there would be an increased number of improper or unlawful disclosures of classified information due to increased information sharing



The “target-centric intelligence process” (i.e. All stakeholders construct a shared picture of the target from which all participants can extract the information they need to do their job and can contribute from their resources or knowledge to create a more accurate target picture) is most effective process.	Number of Responses	Response Ratio
Always	0	0%
Most Often 	20	25%
Sometime 	60	75%
Rarely	0	0%
Never	0	0%
Total	80	100%

Table 1. Target-Centric Intelligence Process, Survey Question 5

Source: Information Sharing Survey, conducted by author, April – May 2004.

initiatives at both the federal and state/local levels. Although these two segments of respondents are in sharp contrast, it is particularly noteworthy that forty percent of the respondents either agreed or strongly agreed that unauthorized disclosures would increase during the information sharing era. Furthermore, if you add the percentage of respondents that were unsure to those that agreed in some form, then the conclusion that at least fifty percent of the respondents recognize that unauthorized disclosure of classified information is a significant problem due to the increase of classified

information sharing between federal and state/local government agencies. Of course, this question merely documented that many other personnel involved with or familiar with information sharing initiatives appreciate the challenges and are seeking solutions.

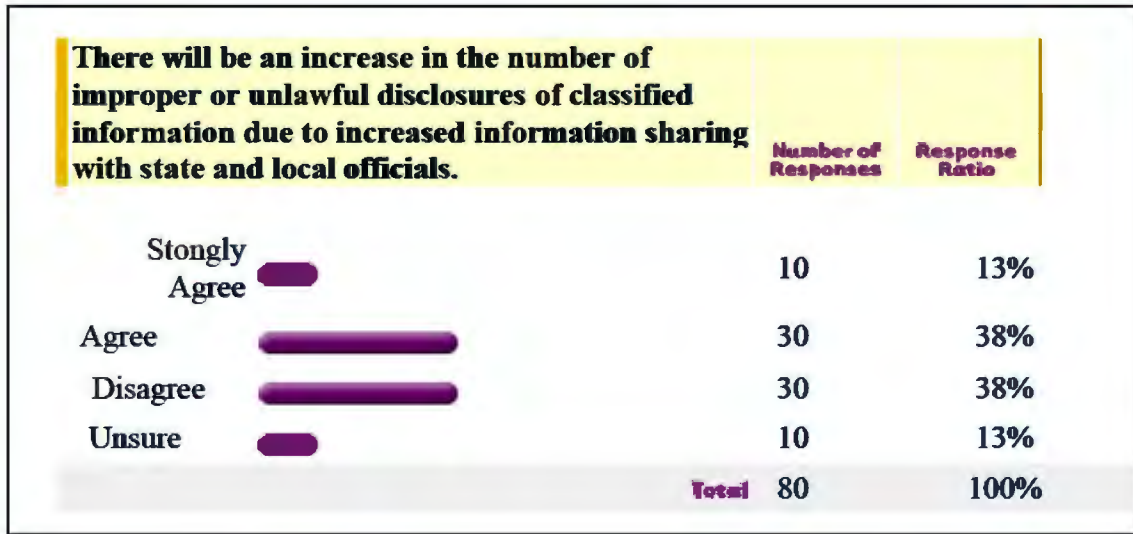


Table 2. Disclosures of Classified Information, Survey Question 6

Source: Information Sharing Survey, conducted by author, April – May 2004.

According to the results of question seven (Table 4) most respondents were optimistic about the development, implementation, and enforcement of safeguards for classified information. It is important to note that a significant twenty-five percent of the survey respondents disagreed that adequate safeguards could be developed, implemented, and enforced. This data does indicate that this segment of the intelligence community is pessimistic about the information sharing era. This survey data may also indicate that these personnel will be more likely to not full cooperate and share classified information with state and local officials. Although information sharing mandates exist, there are also

mandates to protect classified information from unlawful disclosure. Protecting classified information could be used as a justification by federal officials for not sharing classified information with state and local officials. The concept and need for finding the correct and effective balance between sharing and protecting classified information emerges as the key challenge.

Adequate safeguards can be developed, implemented, and enforced to prevent or minimize improper or unlawful disclosures of classified information during information sharing initiatives between federal, state, and local government.	Number of Responses	Response Ratio
Strongly Agree 	10	13%
Agree 	50	63%
Disagree 	20	25%
Unsure	0	0%
Total	80	100%

Table 3. Safeguarding Classified Information, Survey Question 7

Source: Information Sharing Survey, conducted by author, April – May 2004

One critical component to the dual challenge of safeguards and trust related to question seven is that many state and local officials do not have the required security clearances that are required for access to classified information. Regardless of the actual desire or intent of federal officials to share classified information with state and local officials, anyone who does not possess appropriate security clearances is prohibited from access to classified data and intelligence. Ironically, federal agencies control the granting

of security clearances and the process and procedures vary from a agency to agency. Therefore, many state and local law enforcement officials are frustrated by the situation. The concerns of these officials have been noted and acted upon by Congress and the President, however the implementation of policy and statutory directives remains a challenge. The dilemma involves sharing actionable information while protecting classified information, including sources and methods.

LOCAL LAW ENFORCEMENT OFFICIALS

Many state and local agencies do not have personnel cleared for even the lowest level of access to national security information," causing federal officials to be leery of sharing sensitive information outside Washington. . . . State and local law enforcement personnel are experiencing significant delays in getting clearances to obtain information from federal sources.

-- National Criminal Justice Association⁸³

The challenges faced by state and local law enforcement and emergency response officials are tremendous. However, legitimate concerns about granting authorization and use of classified information without harming national security is a delicate balance that must be struck despite the frustrations. The challenges are both administrative and substantive.

Administratively, adequate resources must be provided so that prompt and adequate security investigations can be conducted and rapidly adjudicated so that appropriate security clearances may be granted to state and local officials who have a

⁸³Jim McGee, "Bush Greenlights Ridge on Security Clearances Outside Beltway," *CQ Homeland Security: Government Reorganization*, 30 July 2003, URL: <<http://homeland.cq.com/hs/display>>, accessed 2 February 2003.

need to know classified information. However, substantively there is a prevailing concern among many survey respondents that many state and local officials, that have a need to know classified information, should not be granted access to classified information due to their background. This substantive issue is a major concern especially because federal officials are reluctant to lower the standards for security clearances to accommodate state and local officials. Furthermore, the administrative processing time for federal and military personnel who require security clearance is long and there actually is a tremendous backlog of cases that need investigation and adjudication. This is not merely a problem faced by state and local officials who need clearances. Federal agencies contend with the same administrative delays. However, although delays in the clearance adjudication process are prevalent, the process of investigation and adjudication cannot be taken lightly.

Granting a security clearance to a person that should not obtain one can have dire consequences for national security. The efficiency and speed of the process does need improvement, but not at the expense of security.

Multi-agency arrangements⁸⁴ and interagency cooperation⁸⁵ are two ways that agencies are bridging the information sharing gap. These arrangements also reduce reasonable concerns about unauthorized disclosures because various agency personnel are often located at shared facilities, sometimes at a neutral location.⁸⁶

⁸⁴U.S. Congress, Senate, Select Committee on Intelligence, Terrorist Threat Confronting the United States: Statement for the Record, Dale Watson, Executive Assistant Director for Counterintelligence Federal Bureau of Investigation (FBI) 2002, 99th Cong., 1st sess., 6 February 2002. Cited hereafter as U.S. Congress, Senate Terrorist Threat.

⁸⁵U.S. Congress, Senate Terrorist Threat.

⁸⁶U.S. Congress, Senate Terrorist Threat.

An example of multi-agency cooperation is the “National Infrastructure Protection Center (NIPC). The NIPC is interagency center . . . that serves as the focal point . . . to warn of and respond to cyber intrusions. NIPC programs have been established in each of the FBI’s 56 Field offices.”⁸⁷ Nevertheless, despite the many joint operations that combine federal, state, and local personnel many “characterize the relationship as one of more ‘co-habitation’ where the FBI clearly is in charge and non-federal representatives are viewed as second tier participants, despite often having greater knowledge of a particular case.”⁸⁸

Most personnel surveyed were unsure whether the Homeland Security Act of 2002 (HSA) provided adequate safeguards to protect classified information at the state and local levels have been instituted (See Table 1). Most of the persons surveyed are involved with information sharing under the HSA and had an opinion about the implications of increased information sharing and the risks of unauthorized disclosures. Some of these concerns are based on past agency practice or personal relationships, but other concerns are based on legitimate security concerns. Generally, the survey population was reluctant to discuss the issue of unauthorized disclosures of classified information in specific detail due to the sensitive nature of the topic. The survey questions were developed to maximize the response rate without alienating intelligence and law enforcement personnel.

⁸⁷U.S. Congress, Senate Terrorist Threat.

⁸⁸Cumming, “FBI Intelligence Reform,” *CRS Report*.

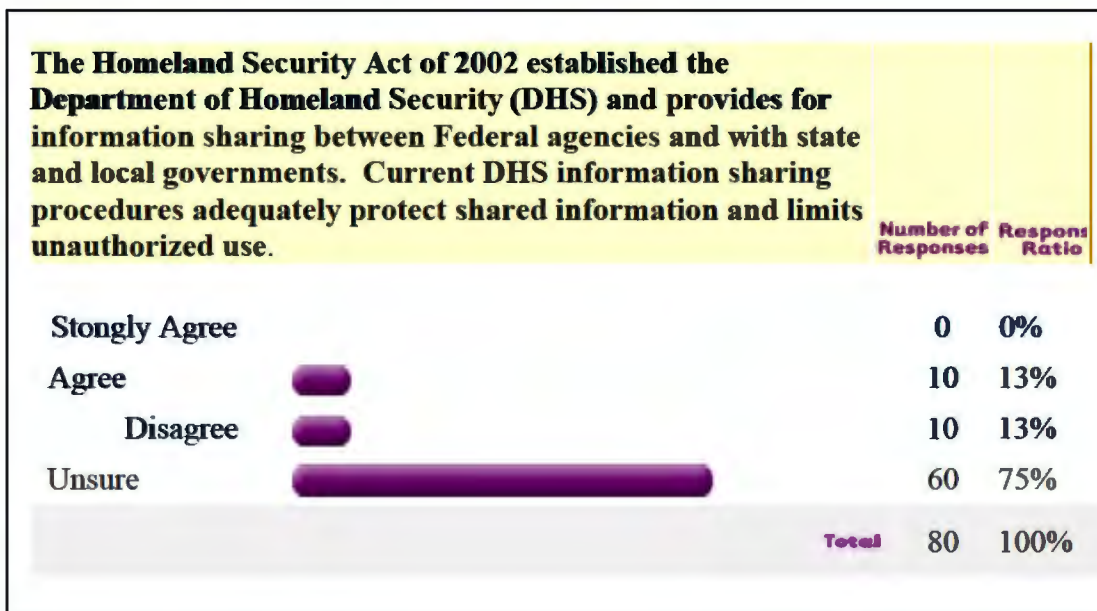


Table 4. Homeland Security Act Protections, Survey Question 11

Source: Information Sharing Survey, conducted by author, April – May 2004

The results of question number eleven from the information sharing survey clearly indicates that most of the people surveyed believe that the current information sharing procedures at the Department of Homeland Security (DHS) adequately protect shared information and limits unauthorized use. Although this survey was not designed to be a test, seventy-five percent of the respondents were correct about the existence of the information security procedures within the HSA. In fact, sections 221 through 225 of the HSA deal with various aspects of security for shared information. The mere existence of the provisions and the procedures does not necessarily mean that these safeguards are actually effective to prevent unauthorized information disclosures. However they provide a good foundation and starting point for information security.

The information security provisions and procedures in the HSA are:

- Procedures for Sharing Information⁸⁹
- Appointment of Privacy Officer⁹⁰
- Enhancement of Non-Federal Cyber-security⁹¹
- Net Guard⁹²

Each of these security provisions and procedures are vital parts of the overall information sharing system of the HSA.

Procedures for Sharing Information

One of the most important aspects about information sharing procedures is its emphasis on limiting unauthorized dissemination. These procedures protect both national security sources and methods, and also confidential information about individuals. Protection of confidential information is based on the Constitutional “right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”⁹³ In addition, Constitutional due process could protect persons from deprivation of any property rights they may have lost due to an unauthorized disclosure.⁹⁴

⁸⁹*Homeland Security Act of 2002*, § 221.

⁹⁰*Homeland Security Act of 2002*, § 222.

⁹¹*Homeland Security Act of 2002*, § 223.

⁹²*Homeland Security Act of 2002*, § 224.

⁹³*U.S. Constitution*, IV Amendment.

⁹⁴*U.S. Constitution*, V Amendment.

Appointment of Privacy Officer

The provision for appointment of a privacy officer mandates that a senior DHS official support the information security procedures. The Privacy Officer is required to assure that individuals are protected from the erosion of privacy protections. Under the HSA, Privacy Officer is required to use available technologies to prevent unauthorized disclosures.⁹⁵ This safeguard primarily focuses on individuals, however the USG also benefits from keeping privacy information about individuals out of the public domain. This makes people less susceptible to bribes, blackmail, or other forms of corruption.

Enhancement of Non-Federal Cyber-Security and Net Guard.

The cyber-security and Net Guard provisions of the HSA focus primarily on protection of information analysis (intelligence) and infrastructure protection. Unauthorized disclosure is one of several concerns within these provisions. However, two critical vulnerabilities of critical national information systems are threats of corruption and compromise. These threats are rarely inadvertent and the perpetrators are almost always unauthorized persons with a wrongful, criminal or malicious, purpose. The emphasis on national cyber-security increases in significance when the mere possibility, or high probability, of cyber-terrorism is considered. The threat of terrorism in any form increased the threat to national security and raises the stakes concerning the importance of preventing inadvertent and intentional unauthorized disclosures of classified information.

⁹⁵*Homeland Security Act of 2002*, § 224.

CONCLUSIONS

The agencies that make up the IC and the LE communities are extremely diverse in terms of mission, leadership, resources, and in their respective commitment to new post-September 11th, 2001 information sharing initiatives and mandates. This diversity is even more profound when the individual personalities of the personnel are considered. Despite this tremendous diversity, the overwhelming majority of personnel surveyed indicated that adequate safeguards for the increased information sharing between the federal government and the state and local government are either inadequate or they are unsure about the adequacy of the measures.

The responses to question (statement) number six (There will be an increase in the number of improper or unlawful disclosures of classified information due to increased information sharing with state and local officials) of the Information Sharing Survey indicated that thirty-eight percent of those surveyed both agreed and disagreed with the statement. However, another thirteen percent “strongly agreed” with the statement and the remaining thirteen percent were “unsure.” These survey results indicate that there is a potential problem with the security of information that will flow at increasing rates from the federal sector to the state and local levels. In the midst of this potential serious risk the survey indicated that there is optimism among the personnel that deal with information sharing.

The results of question number seven (Adequate safeguards can be developed, implemented, and enforced to prevent or minimize improper or unlawful disclosures of classified information during information sharing initiatives between federal, state, and

local government) clearly indicates that personnel are realistically optimistic about the challenges or risks involved with information sharing initiatives. Seventy-five percent of those surveyed either agreed or strongly agreed with the statement in question seven. The survey group appears to understand that since information sharing is an imperative to effectively combat terrorism, then the development of adequate safeguards is not only an imperative, but it *can* be accomplished.

The next chapter will explore some of the recommendation for countering unauthorized disclosure of classified information.

CHAPTER 6

RECOMMENDATIONS TO COUNTER UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

It is a criminal offence to name a covert CIA agent. The scandal is the biggest to hit the administration since Bush took office in January 2001. The US Justice Department opened a formal investigation on September 30 into "possible unauthorized disclosures" of the agent's identity by the Bush administration.⁹⁶

-- ABC News Online

The policy recommendations for countering unauthorized disclosure of classified and sensitive information fall into several categories. This chapter will outline several policy recommendations that address unauthorized disclosures. It is suggested that these policy recommendations be viewed as an integrated whole for potential implementation as a comprehensive national strategy to ensure enhanced information sharing without compromising national security with unauthorized disclosures. Many of the ideas are not new, but several of them have never been presented together and recommended as an overall national strategy.

The foundation of the comprehensive strategy should be based on the research and recommendations of a 1985 Secretary of Defense Security Review Commission Report,⁹⁷ the recommendations of the Mr. James B. Bruce and CIA's Foreign Denial and

⁹⁶ABC NewsOnline, Sunday, January 4, 2004, URL: <<http://www.abc.net.au/news/newsitems/s1019937.htm>>, accessed 17 February 2004.

⁹⁷Department of Defense, Office of the Secretary of Defense, *Keeping the Nation's Secrets: A Report to the Secretary of Defense, Commission to Review Department of Defense Security Policy and Practices* (Washington, DC: 1985), URL: <<http://www.fas.org/sgp/library/stilwell.html>>, accessed 13 June 2004. Cited hereafter as DoD Security Policy Review.

Deception Committee,⁹⁸ and the recommendations information sharing stakeholders who have experienced challenges with the implementation of information sharing policies.⁹⁹ The primary focus these policy and legislative recommendations is on protecting classified and sensitive information and intelligence, while allowing this information to be shared with appropriate governmental agencies without regard to their federal or State status.

UNIFORM AND COMPREHENSIVE STANDARDS

Uniform and comprehensive standards must be urgently developed and implemented for the eligibility, investigation, and access to security clearances. The process of obtaining and maintaining access to classified information varies from agency to agency. In addition, when States and local agencies are involved the process is often slower and backlogged. The development of national standards in the clearance process will alleviate two vital issues, the need for security and the need to limit unauthorized disclosures.

Under the current system various agencies do not share information with personnel from outside agencies unless they possess the applicable clearances and have the requisite need to know the specific information being shared. Although this process

⁹⁸James B. Bruce, *Laws and Leaks of Classified Intelligence, The Consequences of Permissive Neglect*, Central Intelligence Agency Homepage, URL: <<http://www.odci.gov/csi/studies/vol47no1/article04.html>>, accessed 13 June 2004. James B. Bruce is the Vice Chairman, DCI Foreign Denial and Deception Committee.

⁹⁹Josh Myer, "Fingers Point at An Intelligence Wall," *Los Angeles Times*, 14 April 2004. "The scapegoat emerging from the 9-11 commission isn't an elected official or agency but an obscure government policy that came to be known as 'the wall.'" However, according to Janet Reno, the wall was never overly restrictive, just interpreted incorrectly all these years. "There [were] simply no wall or restrictions on sharing the vast majority of counter-terrorism information."

can be difficult, slow, and frustrating it is important to balance the competing goals. Uniform standards will facilitate this process.

LEGISLATIVE ACTION

Legislative action is urgently needed to strike a balance between protecting national security, protecting the rights of citizens, and protecting classified information from unauthorized disclosure. One of the most important things that Congress could do immediately is to take emergency action with its ranks to address four major issues: Congressional secret sessions, strengthening of the Intelligence Identities Protection Act, clarifying the definitions and protections of Sensitive, but unclassified information, and launch a national “Anti-Leak” program.

Congressional Secret Sessions or closed sessions are used by Congress to “discuss issues of national security, confidential information, and sensitive communications received from the President.”¹⁰⁰ The primary reason for raising this issue as one that must be addressed by Congress is that it is widely reported and alleged that leaks of classified information flow from Congress to unauthorized persons on a routine basis. Some of this classified, confidential, or otherwise sensitive national security information should be safest when held by elected officials who are sworn to uphold the law and protect the best interests of the United States and its citizens.

According to the information sharing survey and other Congressional investigations there is a problem that Congress should address internally before the

¹⁰⁰Mildred Armer, “Secret Sessions of Congress: A Brief Historical Overview,” *CRS Report for Congress* RS20145, “CRS Military and National Security,” Washington, DC: Congressional Research Service, Library of Congress, updated 5 August 2003), URL: <www.fas.org/man/crs/RS20145>, accessed 28 May 2004.

Justice Department or the Executive branch takes urgent action (possibly criminal action). There are currently several investigations involving unauthorized disclosures of information from Congress and at least one current investigation involving a possible violation of the Intelligence Identities Protection Act.

Intelligence Identities Protection Act (IIPA)¹⁰¹ is an important issue that Congress should immediately address despite current investigations into criminal violations of this Act. This act makes it a criminal violation to disclose the identity of a covert USG agent without proper authorization.¹⁰² The investigative powers and the criminal and administrative penalties of the IIPA should be increased to demonstrate the seriousness of the USG policy against unauthorized disclosures, particularly when the improper disclosure involves the identity of a covert agent.

The protection of “sensitive, but unclassified (SBU) information, also called sensitive unclassified information” is a critical issue that is often over-shadowed by more publicized issues involving classified information.¹⁰³ The most important aspect about SBU information is that its unauthorized dissemination can cause serious damage to national security. Although, SBU information is not the primary focus of this thesis, it is necessary to briefly discuss it in regard to recommended actions for Congress.

¹⁰¹Elizabeth B. Bazan, “Intelligence Identities Protection Act,” *CRS Report for Congress* RS21636, “CRS Military and National Security,” Washington, DC: Congressional Research Service, Library of Congress, 3 October 2003), URL: <www.fas.org/man/crs/RS21636>, accessed 2 March 2004.

¹⁰²50 U.S.C. §§ 421-426, Intelligence Identities Protection Act (1984).

¹⁰³Genevieve J. Knezo, “Sensitive But Unclassified and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy,” *CRS Report for Congress* RL31845, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, updated 20 February 2004), URL: <www.fas.org/man/crs/RL31845>, accessed 15 April 2004.

One of the significant challenges with protecting SBU information from unauthorized disclosure is that there is a “lack of a clear definition . . . [that] complicates designing policies to safeguard such information and that, if information needs to be safeguarded, it should be classified.”¹⁰⁴ Although scientific and technical SBU items of information are not currently classified, but they may be eligible for classification. Many agencies that deal with scientific and technical information are reevaluating the factors that they use to determine whether various types of information may, in fact, qualify for classification. In addition, agencies may use various factors to develop nondisclosure policies to protect SBU information, in lieu of determining that the information is classified.

Federal agencies that often use SBU designations for information are the Department of Energy, the State Department, the U.S. Agency for International Development, the General Services Administration, the Federal Aviation Administration, and the National Aeronautics and Space Administration.¹⁰⁵ In 1997 the Department of Defense began using SBU as a ground for exemption under the Freedom of Information Act (FOIA).¹⁰⁶ The SBU FOIA exemption allows “each creator or handler of potential SBU information to make a ‘sensitive/non-sensitive’ determination on a case-by-case basis.”¹⁰⁷ Once this SBU designation is made personnel are required to be warned

¹⁰⁴Knezo, “Sensitive But Unclassified,” CRS Report, 10.

¹⁰⁵Knezo, “Sensitive But Unclassified,” CRS Report, ii.

¹⁰⁶5 U.S.C. § 552a, Freedom of Information Act of 1974; and 5 U.S.C. § 552, Freedom of Information Act of 1966.

¹⁰⁷Knezo, “Sensitive But Unclassified,” CRS Report, 18.

appropriately that “unauthorized disclosure of SBU information may result in criminal and/or civil penalties.”¹⁰⁸ The final disposition is determined on a case-by-case basis.

The Transportation Safety Administration (TSA) uses a similar designation that is similar to SBU called Sensitive Security Information (SSI).¹⁰⁹ The SSI designation is used by TSA to protect the details about the improvements in transportation security from public disclosure. This is another example of how critical classified, SBU, and SSI information are to national security. Congress must continue to coordinate and consolidate all these information designators into a comprehensive program that promotes and ensures national security, and minimizes unauthorized disclosures of information that compromises national security. This must be made a national priority and there are several actions that both Congress and the President can take.

The creation and adequate funding of a National “Anti-Leak”¹¹⁰ Program by Congress will benefit national security and fight terrorism and USG adversaries in several ways. First, the public needs to learn about the importance of protecting classified and sensitive national security information for national security. Second, a national program will decrease the market for classified information to fewer persons who are intentionally, versus inadvertently or negligently, disclosing classified or sensitive

¹⁰⁸Knezo, “Sensitive But Unclassified,” CRS Report, 18.

¹⁰⁹Mitchel A. Sollenberger, “Sensitive Security Information (SSI) and Transportation Security: Background and Controversies,” *CRS Report for Congress RS21727*, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, 5 February 2004), URL: <www.fas.org/man/crs/RS21727>, accessed 10 April 2004.

¹¹⁰The concept of a National Anti-Leak Program is indirectly implied, but not specifically outlined, within the concept of the DCI’s Foreign Denial and Deception Program. No information was discovered or obtained during the research phase of this thesis about any comprehensive national program to educate the public about the importance of reducing and eliminating the unauthorized disclosure of classified, SBU, and SSI. The specific concept and discussion of a National Anti-Leak Program in this thesis is believed by the author to be original. However, when you are sleep deprived many ordinary concepts seem to be unique.

information to the Nation's enemies and adversaries. Finally, creation of a national anti-leak program should decrease the amount and quality of classified information that is disclosed to the public. Some form of National shame would fall upon any person who is legally convicted of unauthorized disclosure. When more people understand the insidious connection between leaks and national security, then more people will subscribe to the notion that "good Americans" do not leak information. Currently this connection does not exist. A public information program, such as a National Anti-Leak Program, will be needed to address this serious problem.

The following are poster ideas for a National Anti-Leak Program:

1. America -- Love it, but *don't Leak it*.
2. Leaks are like friendly fire, American soldiers, sailors, and agents die because of "loose lips." Think safety first, *don't leak*.
3. Make America a *Leak Free Zone*. Don't make it easier for Terrorist.
4. Help fight terrorism daily, without going to a combat zone, *don't leak*.
5. Say no to terrorism and the leaks that make America weak. Say no to those who profit from leaks. Americans *do not* want news that harms national security. *Freedom is too valuable to leak it away*.

In addition to the Madison Avenue caliber advertisements and posters like the ones described above, the proposed National Anti-Leak Program will consist of pamphlets, videos, and an celebrity guest lecture series that would cover information (unclassified, open-source, non-confidential, and non-sensitive) about the importance of protecting the homeland and other vital national interests overseas. This national program would emphasize that the entire community plays a role in national security by not disclosing

classified information. Citizens also participate in protecting national security by encouraging others (especially the media) not disclose classified or national security sensitive information. Of course, there will always be conflicts concerning what should or should not be classified or determined to be SBU or SSI. Setting the standards will be a formidable task and the standards would need to be firm, yet flexible enough to accommodate circumstances related to specific information or documents.

EXECUTIVE ACTION

There are several actions that the President can take to protect national security. The President's focus should be on four areas related to Homeland Security. The Presidential Coordinating Office (Office of Homeland Security), Northern Command, Terrorist Identification, Screening, Critical Infrastructure Information Disclosure, and Tracking Under Homeland Security Presidential Directive 6.

The OHS and its Cabinet-level director, Tom Ridge, was established by on 8 October 2001 by Executive Order 13228.¹¹¹ Although the Director of DHS technically has jurisdiction over all agencies that relate to homeland security, it remains very difficult to accomplish policy objectives in such a nebulous environment. On essential aspect of the OSH is its need for classified information and accurate and timely unclassified information. In addition, the issue of unlawful disclosure is implicated because although several agencies now fall under one Director, it still remains to be determined if or when the new DHS will be able to actually function in a streamlined responsive fashion. It is

¹¹¹U.S. President, Executive Order 13228, "Office of Homeland Security," 8 October 2001. Cited hereafter as U.S. President, EO 13228.

hoped that DHS as a whole will eventually become clearly greater than the sum of its parts. The President should use his power and influence to ensure that information is flowing to his appointee, Tom Ridge, on his behalf and that the other federal agencies are fully supportive. Finally, the President has the power to send a clear message to all executive agencies, the military, and the governors of the several states that unlawful, unauthorized disclosures of classified information or sensitive but unclassified information will no be tolerated. President Bush must make it clear that leaks are against the nation's vital interests and that leaks undermine national security and the security and safety of troops (and supportive civilians) on the ground.

The establishment and implementation of Northern Command (NORTHCOM) by the President on 25 April 2002 allowed the USG and the Commander-in-Chief to fight terrorism in the homeland.¹¹² Since NORTHCOM relies on the flow of information from other federal agencies, including state and local agencies, it is imperative that classified information is protected during the process. The President, as military Commander and the appointing authority for the heads of the IC, has the power to ensure that information is both shared and protected. According to significant amounts of research on this topic conducted for this project, the information flow has improved, but still needs tremendous improvement to be optimally effective.¹¹³ “According to Lt. Gen. Edward G. Anderson III, Deputy Commander of U.S. Northern Command . . . on a scale of one to ten “with

¹¹²Christopher Bolkom and others, “Homeland Security: Establishment and Implementation of Northern Command,” *CRS Report for Congress* RS21322, “CRS Military and National Security” (Washington, DC: Congressional Research Service, Library of Congress, updated 14 May 2003), URL: <www.fas.org/man/crs/RS21322>, accessed 10 January 2004.

¹¹³Rich Tuttle, “General: Room For Improvement In Sharing Homeland Defense Info,” *Aerospace Daily*, 29 January 2004. “According to Lt. Gen. Edward G. Anderson III, Deputy Commander of U.S. Northern Command . . . on a scale of one to ten “with regard to how well we as a community, not just we NORTHCOM, are doing in information sharing, I would probably assess it as between seven and eight.”

regard to how well we as a community, not just we NORTHCOM, are doing in information sharing, I would probably assess it as between seven and eight.” Also, the risk of unauthorized disclosure of classified and sensitive information has the potential to rise dramatically because adequate safeguards and rigorous enforcement of existing unauthorized disclosure laws has not occurred. Better enforcement is an investigative challenge, but it is ultimately a political leadership challenge and responsibility. Sustained political will and adequate resources must be focused on the issue before real change will occur.

INTELLIGENCE COMMUNITY ACTION

The most significant positive impact that the IC can have on both information sharing initiatives by the President and Congress is to immediately begin to earnestly embrace the concept that information sharing and earnest collaboration is unquestionably in the best interest of the USG and national security.

Procedures to foster the flow of terrorist threat information out of the federal government — but that could require millions of state and local officials to sign oaths of secrecy — still are in the early drafting stages at the Department of Homeland Security, sources familiar with the process say.¹¹⁴

Outdated competitive notions that fostered the hoarding of information and intelligence in an attempt to either bolster credibility, prestige, or funding must be abandoned immediately. Such actions by individual members of the IC or by managers or agency

¹¹⁴Martin E. Anderson, *Fear of the Unknown: Interest Groups Wary of Pending Information Sharing Rules*, CQ Homeland Security: Local Response, 2 October 2003. URL: <www.homelands.cq.com/hs/display>, accessed 29 April 2004.

heads are diametrically opposed to the legitimate national security interests of the USG and its citizens.

In furtherance of the IC changing its culture to begin cooperating among IC members and with State and local (possibly tribal) agencies, Congress should develop accounting and agency funding mechanisms that reward cooperation and information sharing initiatives by IC members that demonstrate their respective commitment to the information sharing initiatives.

Robert Clark's target-centric approach to analysis is a possible engine for change toward increased and effective collaborative information sharing. This approach, as discussed in Chapter 5 (see Figure 1) is an optimal model for collaborative intelligence cycle.¹¹⁵ Unfortunately, disaster may have to strike and history may have to repeat itself before the IC truly understands the critical requirement (not option) for effective collaborative information sharing using target-centric analysis. To act otherwise in the face of executive, statutory, and agency regulatory mandates is negligent, at best, and possibly criminal.

According to the anonymous author of *Through Our Enemies Eyes*,¹¹⁶ America's enemies thrive on the disorganization and negative competition within the IC, and between the IC and State/local agencies. Terrorist reconnaissance cells are observing and gathering information about our vulnerabilities, including our routine lack of earnest cooperation. "Al Qaeda's attacks to date have shown increasing lethality and patient

¹¹⁵Clark, 101-126.

¹¹⁶*Through Our Enemies' Eyes* (Virginia: Brassey's, 2002), 230.

preparation. Its patience has been especially notable since 11 September 2001.”¹¹⁷ The IC actually has no choice except to fully embrace the information sharing era as the *only* way to be successful in the war on terror. The USG is already at a disadvantage due to the unconventional enemy that we must engage. The IC would be wise to refrain from creating additional advantages for the enemy by not sharing information fully while using appropriate and established security procedures to limit unauthorized disclosure of classified or sensitive information.

STATE AND LOCAL LAW ENFORCEMENT ACTION

The International Association of Chiefs of Police (IACP) developed a National Criminal Intelligence Sharing Plan that represented the interests and views of local, state, and tribal law enforcement and they developed an action plan that consists of twenty-eight recommendations concerning the enhancement of information sharing with the IC and federal LE. Several of the IACP recommendations also involve the prevention of unlawful disclosure of classified or LE sensitive information.

The IACP plan is called the Global Justice Information Sharing Initiative (Global Intelligence Working Group (GIWG)).¹¹⁸ It is important to include the IACP perspective in this study because the membership of this organization appears to appreciate the perspective of the rank and file sworn LE officers in the U.S. It is vital to note that “approximately 75 percent of the law enforcement agencies in the United States have less than 24 sworn officers, and [usually] do not have staff dedicated to intelligence

¹¹⁷*Through Our Enemies' Eyes*, 230-231.

¹¹⁸International Association of Chiefs of Police (IACP), “Criminal Intelligence Sharing Summit,” Spring 2002, *Conference Proceedings* (City, State: IACP, 2002), URL: <www.v-one.com/docs/nationalcriminal_Intelligence_Sharing_Plan.pdf>, accessed 15 January 2004, Cited hereafter as *IACP Conference Proceedings*.

functions.”¹¹⁹ It is valuable for policy makers to understand key considerations like this to better shape and implement effective strategies and resources to meet the tremendous challenges faced by sworn LE officers on the streets of America. These LE officers are the real eyes and ears of any effective national homeland security program.

The three most important aspects of the GWIG plan is its emphasis on building a “technology architecture to provide secure, seamless, sharing of information among systems,”¹²⁰ its promotion of the “need to identify an intelligence information sharing capability that can be widely accessed by local, state, tribal, and federal LE and safety agencies,”¹²¹ and that the key ingredient to any effective information sharing plan or collaborative effort that requires information sharing is trust. Trust between local, state, and tribal LE, but more critically, trust between the federal LE/IC and the state/local LE and first responders. The GWIG goal is to “foster trust among law enforcement agencies, policymakers, and the communities they serve.

There is nothing new in this IACP plan except the fact that their entire conference focused on the issue of the vital importance of information sharing. The real challenge will entail seeing if Congress and the President possess the political will and bi-partisan focus required to succeed. Whether the USG and its state/local/tribal partners must successfully balance information sharing initiatives with information security is the critical question that most stakeholders want answered affirmatively.

A comprehensive solution for countering the unauthorized disclosure of classified information in the new information sharing era must be developed, implemented, and

¹¹⁹IACP *Conference Proceedings*, 1.

¹²⁰IACP *Conference Proceedings*, 2.

¹²¹IACP *Conference Proceedings*, 3.

enforced by the all the stakeholders. The actions recommended in this chapter are shared and will only be effective if all the players take urgent action with adequate funding.

CHAPTER 7

KEY FINDINGS, CONCLUSION, AND IMPLICATIONS

We should begin by recognizing that spying is a fact of life . . . we can counter this hostile threat and still remain true to our values. We don't need to fight repression by becoming repressive ourselves. . . . But we need to put our cleverness and determination to work; we need to deal severely with those who betray our country. . . . There is no quick fix to this problem. Without hysteria or finger-pointing, let us move calmly and deliberately together to protect freedom.

-- President Ronald W. Reagan¹²²

KEY FINDINGS

The research data, evidence, and information produced by the literature and interviews support the complementary hypotheses that (1) unauthorized and unlawful disclosures of classified information related to dissemination to state and local agencies will increase, and (2) the Intelligence Community must play an essential role in the development and implementation of increased information sharing mandates and policies to reduce and limit unauthorized disclosures of classified information due to dissemination to state and local agencies.

CONCLUSIONS

Effective counterterrorism and homeland security efforts by the Intelligence Community (IC) and the Law Enforcement Community (LEC) depend on earnest cooperation, information sharing, and intelligence sharing between the military, IC, and LEC. Prior to September 11th, 2001 the process of information and intelligence sharing

¹²²Department of Defense, Office of the Secretary of Defense, *Keeping the Nation's Secrets: A Report to the Secretary of Defense*, Commission to Review Department of Defense Security Policy and Practices (Washington, DC: 1985), URL: <<http://www.fas.org/sgp/library/stilwell.html>>, accessed 13 June 2004.

was always the foundation of counterterrorism and national security. However, in the post-September 11th era information sharing has become essential for national security, homeland defense, and effective counterterrorism. Information sharing inherently involves the movement of classified information and intelligence from one person, agency, or location. The movement of information or intelligence has inherent risks, including unlawful disclosure. Minimizing this risk and actual unauthorized disclosures is a top priority for the IC and the LEC.

The risk of unlawful disclosure, including espionage, has ancient roots. There are many well-known and obscure cases of unlawful or improper disclosures of classified information and intelligence. One of the most devastating aspects of unlawful or wrongful disclosures (also known as “leaks”) is that they diminish the essential power of classified intelligence and classified information. The essence of classified intelligence and classified information is that they are secrets derived from secret sources and methods (SAM). Unlawful or wrongful disclosure of classified intelligence or information compromises the SAM of the Intelligence Community and ultimately undermines national security.

The post-September 11th era has ushered in a new era of increased intelligence and information sharing to combat global and domestic terrorism. The increased levels of intelligence and information sharing is clearly evident between federal agencies, but the most dramatic increases of intelligence and information sharing are being seen between the Intelligence Community (federal) and various state and local government agencies. Increased intelligence and information sharing between the federal and state levels of government pose significant risks of increased unlawful and wrongful

disclosure. These serious issues require immediate attention by the President, Congress, and both the Intelligence Community and the Law Enforcement Community (Federal, State, and local) to minimize the imminent dangers of unlawful and wrongful disclosure of classified information and intelligence. The potential consequences of unlawful disclosure ultimately cost lives and are a serious threat to national security.

Effective safeguards and enforcement measures must be developed to balance the critical needs of national security with the corresponding need to share classified intelligence and information to enhance national security. My thesis is that the unlawful disclosure of classified information and intelligence will increase significantly during the new information sharing era, unless effective safeguards are developed and vigorously enforced to protect the information and the sources and methods. The irony is that effective national security will require seamless information sharing and earnest cooperation between the federal government and state and local governments. Not sharing is not an option according to applicable Congressional and executive mandates. Nevertheless, significant barriers continue to haunt the information sharing process and U.S. national security hangs in the balance.

Real or perceived concerns about the risk unauthorized disclosures is a reason cited by intelligence and law enforcement personnel who are either reluctant to share relevant information with outside agencies or avoid sharing relevant and actionable information. Since the risk of unauthorized disclosure is a legitimate concern, then an effective balance must be struck between total information sharing and sharing relevant actionable information with appropriate officials regardless of governmental level, while simultaneously protecting the classified information from unauthorized disclosure.

This thesis was written in an unclassified format to facilitate access to federal, state, and local research data. The unclassified format also ensured the widest possible dissemination of the research. In addition, many of the survey participants were more cooperative with the research project in the unclassified environment and appreciated the opportunity to assist with non-attribution as a condition of participation. A classified bibliography (not enclosed with this thesis) may be developed and made available by the author subject to any limitations on the unauthorized disclosure of such information.

IMPLICATIONS

The policy and regulatory mandates for information sharing are clear, yet ambiguous. Federal agencies are required to share classified information with other federal, state, local and tribal governments. However, these same laws grant federal agencies tremendous authority to grant and deny required clearances for access to classified information. Furthermore, federal law enforcement and intelligence agencies have superior technology, national assets, and resources, as compared to state and local government. According to Presidential policy federal agencies are required to be the final adjudicator concerning protection of information that can jeopardize national security. Essentially, fighting domestic and global terrorism requires information sharing, but enhanced protections from unauthorized disclosure have not been developed. The current situation is an unacceptable risk.

The implications of the increased risk of unauthorized disclosure require immediate action. According to James Bruce, DCI Foreign Denial and Deception Committee:

Nearly all of the compelling evidence in support of the argument that leaks [emphasis added] are causing serious damage is available only in the classified domain. It thus seems daunting to make a persuasive public case for legal correctives to address unauthorized disclosures when so little of the evidence for it can be discussed publicly.¹²³

A comprehensive information sharing strategy that includes specific guidance, procedures, and enforcement provisions is urgently needed. The implications for delaying such action are unacceptable because they involve the disclosure of classified information to USG enemies and adversaries. The potential damage to USG national security for non-action is unlimited, and could potentially include the death of millions of Americans if a weapon of mass destruction or effects is used by a terrorist group. The enemies of the USG are “connecting the dots” that trusted agents give them purposely or inadvertently.

Our enemies, particularly terrorists, already have distinct advantages in the War on Terrorism. It has been said by numerous USG officials and terrorism experts that terrorists and criminals who seek to do harm to innocent people or destroy property only need to succeed once. But when national counterterrorism efforts fail once the outcome can be catastrophic.

In light of the tremendous challenges faced by the USG in the war against terrorism and the ongoing quest for national security, it never helps the USG when USG enemies and adversaries are provided unauthorized classified and sensitive information. Such disclosures of information and intelligence will increase terrorist capabilities,

¹²³James B. Bruce, *Laws and Leaks of Classified Intelligence, The Consequences of Permissive Neglect*, Central Intelligence Agency Homepage, URL: <<http://www.odci.gov/csi/studies/vol47no1/article04.html>>, accessed 13 June 2004. James B. Bruce is the Vice Chairman, DCI Foreign Denial and Deception Committee.

undermine USG capabilities, and directly decrease national security. The rapid increase of information sharing without adequate safeguards and zealous vigilance is a formula for disaster.

The findings and recommendations of the Joint September 11th Commission will probably address the effectiveness information sharing between all stakeholders involved with national security. During the hearings several government officials, including President George W. Bush and President William J. Clinton, testified before the Commission and provided insight about communication and information sharing.

During the final hearings on 17 June 2004, there was testimony from General Richard Myers, Chairman, Joint Chiefs of Staff; Admiral Charles J. Leidig, Commandant of Midshipmen, US Naval Academy; and General Ralph E. Eberhart, Commander, North American Aerospace Defense Command (NORAD) and U.S. Northern Command (NORTHCOM); several Special Agents of the FBI, and officials from the Federal Aviation Administration.¹²⁴ This testimony confirmed the importance of information sharing, but also the vital importance of maintaining a degree of secrecy was also emphasized. In an open society like the United States it is apparent that freedom of communication and the flow of ideas and information are cherished. However, the transparent mechanisms and systems that support these freedoms depend on secrecy and classified information. A balance must be struck and maintained between these key components of a democratic society to protect national security and democracy.

Finally, the inevitable implication of ineffective action in the realm of combating unlawful disclosures are creating a growing clear and present danger to national security.

¹²⁴U.S. Congress, Joint Commission, National Commission on Terrorist Attacks Upon the United States, 17 June 2004, URL: <<http://www.9-11commission.gov/about/index.htm>>, accessed 19 June 2004. Cited hereafter as 9-11 Commission.

RECOMMENDATIONS FOR FURTHER RESEARCH

The Joint Commission Hearings on the 11 September 2001 Terrorist Attacks ended on 17 June 2004. The findings and recommendations of this commission will undoubtedly spawn further research into whether the IC is organized and operates in the most effective manner against current and future enemies. According to Smith hypothesis, “the current increase in information sharing is driven by a heightened fear of terrorism. Once the fear subsides, the bureaucratic impediments to information sharing will resurface.”¹²⁵ The complimentary hypotheses of this thesis are first, unauthorized and unlawful disclosures of classified information will increase due to information sharing with State and local agencies. Second, the Intelligence Community and Congress must play an essential role in the development and implementation of increased information sharing mandates and policies to reduce unauthorized disclosures of classified information during the information sharing era. The hypotheses of this paper and the Smith thesis are partially contradictory. It is not fear, but rather rationality and logic that are the driving force behind increased information sharing. Despite organizational culture and history, the complexity of the terrorist threat and other complex intelligence analysis requirements demand collaboration and information sharing of the highest order. Possibly the desire for organizational success and effectiveness is the motivational force behind information sharing, but not fear.

¹²⁵(b) (6) ██████████ *Information Sharing: Between Law Enforcement and the Intelligence Community*, MSSI Thesis chaired by (b) (6) ██████████ (Washington, DC: Joint Military Intelligence College, July 2003), 12.

Nevertheless, the evidence is clear that information sharing initiative still remain ineffective, despite tremendous progress.

The research supports the finding that real and perceived concern for unauthorized disclosures of classified information are the primary stated reason for not sharing information and data between federal agencies. Furthermore, when the information is required to be shared with a state or local agency the reluctance to share increases and ultimately information sharing does not occur or is significantly reduced.

Further research related to information sharing and the protection of classified information is virtually guaranteed to be conducted in subsequent years. The target-centric approach to analysis proposed by Clark and already used extensively by the IC, requires stakeholder collaboration and the sharing of information. Effective tearline procedures must be incorporated into any successful information sharing system. In addition, most customers desire timely and actionable information and intelligence, not the entire raw database of information. Further research will be needed on the current intelligence organizations and future intelligence organizations as a result of the Joint Commission's recommendations and Congressional action. Ultimately, successful information sharing between the IC and state and local law enforcement, using target-centric intelligence analysis, is a necessity for effective national security. Achievement of this critical imperative will require an earnest commitment of resources, political will, and intra-agency cultural changes that support and encourage information sharing. Effective protection of classified information from unlawful disclosures during this process should flow seamlessly from the implementation of additional safeguards that are tailored to address the unique vulnerabilities of state and local stakeholders. There will

be serious consequences for national security if the USG fails to effectively share information or simultaneously fails to effectively protect classified information. Current threats to national security, especially terrorist threats, require the USG to find an effective balance between sharing and protecting classified information. Ultimately, effective protection of classified information from unauthorized disclosure will require the USG to rigorously enforce existing and new laws that protect classified information during the new information sharing era.

APPENDIX A

INFORMATION SHARING SURVEY

This national survey is being conducted by a graduate student at the Joint Military Intelligence College, Washington, DC. Please assist this thesis research on information sharing by completing this brief confidential survey. Your experienced-based opinions are invaluable and will contribute to an evaluation of the current state of information sharing between the various governmental levels. Your ideas for improving information sharing without compromising national security or Constitutional values are particularly important. **You may briefly explain your answers in the space provided after each question, if your schedule permits.** Thank you.

Questions 1 - 3. Survey Demographics.

1. Your position:

- A. Military Official
- B. Intelligence Community Officials
- C. Federal Elected Officials
- D. State Elected Officials
- E. State Law Enforcement or Emergency Response Officials
- F. Local Elected Officials
- G. Local Law Enforcement and Emergency Response Officials
- H. Other (Please specify: _____)

2. Number of years in current position or years of similar experience:

- A. 0-1
- B. 1-3
- C. 3-5
- D. 5-10
- E. 10-15
- F. 15-20
- G. 20-25
- H. 25+

3. Academic background or level:

- A. High School
- B. Associate Degree
- C. Bachelor's Degree
- D. Master's Degree
- E. Doctorate

- F. Professional Degree (e.g. RN, J.D.)
- G. Entrepreneur, self-study, or O.J.T.
- H. Other (Please specify: _____)

Questions 4 and 5. Select the response, A to D, that best matches your opinion ranging from Always to Never.

4. The “traditional intelligence cycle” (i.e. Requirements/Needs; Planning/Direction; Collection; Processing; Analysis; Dissemination; . . .) is the most effective.

Always Most Often Sometimes Rarely
Never
A-----B-----C-----D-----E

5. The “target-centric intelligence process” (i.e. All stakeholders construct a shared picture of the target from which all participants can extract the information they need to do their job and can contribute from their resources or knowledge to create a more accurate target picture) is most effective.

Always Most Often Sometimes Rarely
Never
A-----B-----C-----D-----E

Questions 6 - 9. Select the response (Strongly Agree, Agree, Disagree, or Unsure) that best matches your opinion.

6. There will be an increase in the number of improper or unlawful disclosures of classified information due to increased information sharing with state and local officials.

A. Strongly Agree B. Agree C. Disagree D. Unsure

7. Adequate safeguards can be developed, implemented, and enforced to prevent or minimize improper or unlawful disclosures of classified information during information sharing initiatives between federal, state, and local government.

A. Strongly Agree B. Agree C. Disagree D. Unsure

8. Current classified information protection systems adequately protect intelligence sources and methods while allowing government agencies to protect national security.

___A. Strongly Agree ___B. Agree ___C. Disagree ___D. Unsure

9. Open source intelligence is unclassified, but the techniques and methods used to exploit open source materials should be protected or classified.

___A. Strongly Agree ___B. Agree ___C. Disagree ___D. Unsure

10. The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and provides for information sharing between Federal agencies and with state and local governments. Current DHS information sharing procedures adequately protects shared information and limits unauthorized use.

___A. Strongly Agree ___B. Agree ___C. Disagree ___D. Unsure

Comments:

Information Sharing Survey launched on 28 Apr 04 from the Joint Military Intelligence College Computer Lab with the assistance of (b) (6) and (b) (6).

APPENDIX B

THE NEW TERRORIST THREAT INTEGRATION CENTER (TTIC)

- “Elements of the Department of Homeland Security (HS), the FBI’s Counterterrorism Division, the DCI’s Counterterrorist Center, and the Department of Defense will form a Terrorist Threat Integration Center to fuse and analyze all-source information related to terrorism.
- The Terrorist Threat Integration Center will continue to close the “seam” between analysis of foreign and domestic intelligence on terrorism. TTIC will:
 - Optimize use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies.
 - Create a structure that ensures information sharing across agency lines.
 - Integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. Be responsible and accountable for providing terrorist threat assessments for our national leadership.
 - The Terrorist Threat Integration Center will be headed by a senior U.S. Government official, who will report to the Director of Central Intelligence. This individual will be appointed by the Director of Central Intelligence, in consultation with the Director of the FBI and the Attorney General, the Secretary of Defense, and the Secretary of HS.
 - The Terrorist Threat Integration Center will play a lead role in overseeing a national counterterrorism tasking and requirements system and for maintaining shared databases.
 - The Terrorist Threat Integration Center will also maintain an up-to-date database of known and suspected terrorists that will be accessible to federal and non-federal officials and entities, as appropriate.
 - In order to carry out its responsibilities effectively, the Terrorist Threat Integration Center will have access to all intelligence information—from raw reports to finished analytic assessments—available to the U.S. Government.
 - A senior multi-agency team will finalize the details, design, and implementation strategy for the stand-up of the Terrorist Threat Integration Center.”

Source: White House Homepage, URL: <www.whitehouse.gov/news/releases/20030128>, accessed 28 April 2004.

APPENDIX C

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (STANDARD FORM 312) BRIEFING BOOKLET

This booklet provides you with information about the "Classified Information Nondisclosure Agreement," also known as the "SF 312." It includes a brief discussion of the background and purpose of the SF 312; the text of pertinent legislative and executive authorities; a series of questions and answers on its implementation; and a copy of the SF 312. Each organization may wish to supplement this booklet with additional guidance that addresses problems or circumstances unique to it.

This booklet should be available in the offices of those persons who brief individuals about the SF 312, e.g., security managers, security education specialists, or supervisors. Further, all persons who are asked to execute the SF 312, or have executed it or its predecessors, the SF 189 or SF 189-A, should have the opportunity to receive or borrow a copy upon request.

For additional guidance, please contact your security manager, supervisor or legal counsel within your organization. If questions concerning the SF 312 cannot be answered within your organization, please bring them to the attention of ISOO, 700 Pennsylvania Avenue, N.W., Washington, D.C. 20408, telephone number (202) 219-5250.

BACKGROUND AND PURPOSE

As an employee of the Federal Government or one of its contractors, licensees, or grantees who occupies a position which requires access to classified information, you have been the subject of a personnel security investigation. The purpose of this investigation was to determine your trustworthiness for access to classified information. When the investigation was completed, your employing or sponsoring department or agency granted you a security clearance based upon a favorable determination of the investigation results. By being granted a security clearance, you have met the first of three requirements necessary to have access to classified information.

The second requirement that you must fulfill is to sign a "Classified Information Nondisclosure Agreement," the SF 312. The President first established this requirement in a directive that states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." This

requirement is reiterated in the executive order on classified national security information. The SF 312 is a contractual agreement between the U.S. Government and you, a cleared employee, in which you agree never to disclose classified information to an unauthorized person. Its primary purpose is to inform you of (1) the trust that is placed in you by providing you access to classified information; (2) your responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from your failure to meet those responsibilities. Additionally, by establishing the nature of this trust, your responsibilities, and the potential consequences of noncompliance in the context of a contractual agreement, if you violate that trust, the United States will be better able to prevent an unauthorized disclosure or to discipline you for such a disclosure by initiating a civil or administrative action.

The third and final requirement for access to classified information is the "need-to-know;" that is, you must have a need to know the information in order to perform your official duties. The holder of classified information to which you seek access is responsible for confirming your identity, your clearance, and your "need-to-know." As a holder of classified information, you are responsible for making these same determinations with respect to any individual to whom you may disclose it.

As a cleared employee you should receive, according to paragraph No. 2 of the SF 312, a "security indoctrination briefing concerning the nature and protection of classified information, including procedures to be followed in ascertaining whether other persons to whom you contemplate disclosing this information have been approved for access to it...." After you receive such a briefing, you should have a basic understanding of the following:

- What is classified information?
- How do you protect it?
- Who may have access to it?
- How does the classification system function?

A variety of educational materials are available that provide answers to these questions. Several training methods may be used to convey this information, including briefings, interactive videos, and dissemination of instructional materials. Contact your security manager for more information.

APPENDIX D

TITLE VI-- PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION: PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES

Sec. 601.(a) Whoever, having or having had authorized access to, or learns of, classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than [\$25,000 to] 50,000 or imprisoned not more than [five to] ten years, or both.

DEFINITIONS

Sec. 606. For the purposes of this title:

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized", when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility in the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means--

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency--

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and--

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(6) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States," when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

APPENDIX E

CLASSIFIED NATIONAL SECURITY INFORMATION EXECUTIVE ORDER 12958 OF APRIL 17, 1995

Implementing Rule of the Classified Information Nondisclosure Agreement

Sec. 2003.20 Classified Information Nondisclosure Agreement: SF 312;
Classified Information Nondisclosure Agreement: SF 189; Classified Information
Nondisclosure Agreement (Industrial/Commercial/Non-Government): SF 189-A.

(a) SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual. The prior execution of at least one of these agreements, as appropriate, by an individual is necessary before the United States Government may grant that individual access to classified information. From the effective date of this rule, the SF 312 shall be used in lieu of both the SF 189 and the SF 189-A for this purpose. In any instance in which the language in the SF 312 differs from the language in either the SF 189 or SF 189-A, agency heads shall interpret and enforce the SF 189 or SF 189-A in a manner that is fully consistent with the interpretation and enforcement of the SF 312.

(b) All employees of executive branch departments, and independent agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information. An employee who has previously signed the SF 189 is permitted, at his or her own choosing, to substitute a signed SF 312 for the SF 189. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(c) All Government contractor, licensee, and grantee employees, or other non-Government personnel requiring access to classified information in the performance of their duties, who have not previously signed either the SF 189 or the SF 189-A, must sign the SF 312 before being granted access to classified information. An employee who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF 189-A. In these instances, agencies, with the cooperation of the pertinent contractor, licensee or grantee, shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(d) Agencies may require other persons, who are not included under paragraphs (b) or (c) of this section, and who have not previously signed either the SF 189 or the SF 189-A, to execute SF 312 before receiving access to classified information. A person in such circumstances who has previously signed either the SF 189 or the SF 189-A is permitted, at his or her own choosing, to substitute a signed SF 312 for either the SF 189 or the SF

189-A. In these instances, agencies shall take all reasonable steps to dispose of the superseded nondisclosure agreement or to indicate on it that it has been superseded.

(e) The use of the "Security Debriefing Acknowledgement" portion of the SF 312 is optional at the discretion of the implementing agency.

(f) An authorized representative of a contractor, licensee, grantee, or other non-Government organization, acting as a designated agent of the United States, may witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States. Also, an employee of a United States agency may witness the execution of the SF 312 by an employee, contractor, licensee or grantee of another United States agency, provided that an authorized United States Government official or, for government employees only, a designated agent of the United States subsequently accepts by signature the SF 312 on behalf of the United States.

(g) The provisions of the SF 312, the SF 189, and the SF 189-A do not supersede the provisions of Section 2302, Title 5, United States Code, which pertain to the protected disclosure of information by Government employees, or any other laws of the United States.

(h) (1) Modification of the SF 189.

The second sentence of Paragraph 1 of every executed copy of this SF 189 is clarified to read:

As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1(c) and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security.

(2) Scope of "classified information"

As used in the SF 312, the SF 189, and the SF 189-A, "classified information" is marked or unmarked classified information, including oral communications and unclassified information that meets the standards for classification and is in the process of a classification determination, as provided in Section 1.1(c) and 1.2(e) of Executive Order 12356 or any other or Executive order that requires interim protection for certain information while a classification determination is pending. "Classified information" does not include unclassified information that may be subject to possible classification at some future date, but is not currently in the process of a classification determination.

(3) Basis for liability.

A party to the SF 312, SF 189, or SF 189-A may be liable for disclosing "classified information" only if he or she knows or reasonably should know that: (i) the marked or unmarked information is classified, or meets the standards for classification and is in the process of a classification determination; and (ii) his or her action will result, or reasonably could result in the unauthorized disclosure of that information. In no instance may a party to the SF 312, SF 189 or SF 189-A be liable for violating its nondisclosure provisions by disclosing information when, at the time of the disclosure, there is no basis to suggest, other than pure speculation, that the information is classified or in the process of a classification determination.

(4) Modification of the SF 312, SF 189, and SF 189-A

(i) Each executed copy of the SF 312, SF 189 and SF 189-A, whether executed prior to or after the publication of this rule, is amended to include the following Paragraphs 10 and 11.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302 (b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

(ii) The first sentence of Paragraph 7 of each executed copy of SF 312, SF 189 and SF 189-A, whether executed prior to or after the publication of this rule, is amended to read:

I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law.

The second sentence of Paragraph 7 of each executed copy of the SF 312 (September 1988 version), SF 189 and SF 189-A, which reads, "I do not now, nor will I ever, possess

any right, interest, title or claim whatsoever to such information," and whether executed prior to or after the publication of this rule is deleted.

(i) Points of clarification.

(1) As used in Paragraph 3 of SF 189 and SF 189-A, the word "indirect" refers to any situation in which the knowing, willful or negligent action of a party to the agreement results in the unauthorized disclosure of classified information even though the party to the agreement does not directly communicate, deliver or transmit classified information to a person who is not authorized to receive it.

(2) As used in Paragraph 7 of SF 189, "information" refers to "classified information," exclusively.

(3) As used in the third sentence of Paragraph 7 of SF 189 and 3-A, the words "all materials which have, or may have, come into my possession," refer to "all classified materials which have or may come into my possession," exclusively.

(j) Each agency must retain its executed copies of the SF 312, SF 189, and SF 189-A in file systems from which an agreement can be expeditiously retrieved in the event that the United States must seek its enforcement or a subsequent employer must confirm its prior execution. The original, or a legally enforceable facsimile that is retained in lieu of the original, such as microfiche, microfilm, computer disk, or electronic storage medium, must be retained for 50 years following its date of execution. A contractor, licensee or grantee of an agency participating in the Defense Industrial Security Program shall deliver the copy or legally enforceable facsimile of the executed SF 312, SF 189 or SF 189-A of a terminated employee to the Defense Industrial Security Clearance Office. Each agency shall inform ISOO of the file systems that it uses to store these agreements for each category of affected individuals.

(k) Only the National Security Council may grant an agency's request for a waiver from the use of the SF 312. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of ISOO, along with a justification for its use. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council.

APPENDIX F

MAJOR REVIEWS OF THE U.S. SECRECY SYSTEM¹²⁶

The following provides a summary of key studies on classification, declassification, and personnel security. This summary does not include numerous other studies that have indirectly addressed these issues in the course of more broad-based examinations of Federal information policies, or studies, such as those of the General Accounting Office, that have been more limited in their scope. Nor does it include the annual reports of the Information Security Oversight Office, which have, on occasion, put forth detailed recommendations for reform to classification practices.

Coolidge Committee - 1956

Created by Secretary of Defense Charles Wilson to investigate how to prevent future leaks of classified information, the Defense Department Committee on Classified Information undertook a three-month review of DoD classification practices and policies. The Committee, composed of representatives from the military services and chaired by former Assistant Secretary of Defense Charles Coolidge, declared the classification system “sound in concept,” but also found that vague classification standards and the failure to punish overclassification had caused overclassification to reach “serious proportions” and had resulted in diminishing public confidence in the classification system. Among the recommendations included in its November 8, 1956 report were: addressing overclassification from the top down, beginning with the Secretary of Defense; creating a Director for Declassification within the Office of the Secretary of Defense; and reducing the number of “Top Secret” original classifiers.

Wright Commission - 1957

The bipartisan Commission on Government Security, chaired by former American Bar Association President Loyd Wright, was the only previous Congressionally mandated review of the security system. The Commission held no public hearings, produced no press releases, and made no public statements during its eighteen-month study. In its June 23, 1957 report, the Commission stressed “the danger to national security that arises out

¹²⁶“Report of the Commission on Protecting and Reducing Government Secrecy 1997,” Appendix G; Senate Document 105-2, Pursuant to Public Law 236, 103rd Congress, U.S. Government Printing Office, Washington, DC: 1997. URL: <<http://www.dss.mil/seclib/govsec/secrecy.htm>>, accessed 13 June 2004.

of overclassification.” Its recommendations included: abolition of the “Confidential” level and corresponding security checks; restricting original classification authority to agencies already possessing it and limiting that authority to the agency heads; improvement of classification training for those with such authority; creation of a Central Security Office to review the management of the security system and to make recommendations for change when necessary; and legislation criminalizing the unauthorized disclosure of classified information, including by the press.

Moss Subcommittee - 1958

Although the efforts of the Special Government Information Subcommittee of the House Government Operations Committee spanned two decades, its early work under Chairman John Moss (including scores of hearings and over two dozen interim reports) was especially significant. Created in 1955, the Subcommittee began its efforts with a two-year examination of Federal classification policies, focusing in particular on the Defense Department. In its first report, issued on June 16, 1958, the Subcommittee attributed overclassification at DoD in large part to the lack of punishment for overclassification but not for underclassification. Citing the “loss of public confidence” when information is withheld “for any other reason than true military security,” it recommended: procedures for independent review of complaints about overclassification; mandatory marking of each classified document with the future date or event after which it is to be reviewed or automatically downgraded or declassified; establishment of a date by which the DoD would declassify classified material accumulating in agency files, with a “minimum of exceptions;” and disciplinary action against those who overclassify.

Seitz Task Force - 1970

The Department of Defense Science Board’s Task Force on Secrecy was prompted by DoD concerns over the effectiveness of its security measures. The Task Force, chaired by Dr. Frederick Seitz, found that DoD’s classification system required “major surgery” and noted negative aspects of classification such as its cost, “uncertainty in the public mind on policy issues,” and impediments to the free flow of information. Chief among its conclusions was that “perhaps 90 percent” of all classification of technical and scientific information could be eliminated. The July 1, 1970 report of the Task Force included the following recommendations: a maximum duration of five years for classification of scientific and technological information, with few exceptions; overhauling classification guides by considering the benefits to technological development that would result from greater public access to information; and review and declassification of classified DoD materials within two years.

Stilwell Commission - 1985

Established by Secretary of Defense Caspar Weinberger to identify “systemic vulnerabilities,” the Commission to Review DoD Security Policies and Practices found that “little scrutiny” was given decisions to classify. The Commission, chaired by Gen. Richard Stilwell (Ret.), concluded that shortcomings in the classification management arena were “primarily a matter of inadequate implementation of existing policy, rather than a matter of deficient policy.” Among the recommendations included in its report, issued on November 19, 1985, were the following: banning the retention of classified documents for more than five years unless the documents are “permanently valuable;” further reduction in the number of original classifiers; a one-time review and revalidation of all DoD Special Access Programs; minimum security standards for all DoD Special Access Programs; and placement of security responsibilities within a single staff element of DoD.

Joint Security Commission – 1994

Tasked by Secretary of Defense William Perry and Director of Central Intelligence R. James Woolsey with developing a new approach to security, the Joint Security Commission engaged in a nine-month review. Finding that the system had reached “unacceptable levels of inefficiency, inequity, and cost,” the Commission’s February 1994 report, *Redefining Security*, included the following recommendations: a “one-level classification system with two degrees of [physical] protection;” establishing a Joint Security Executive Committee to oversee the development of policies in its new system; use of a “risk management” philosophy when developing new security policies; and a single, consolidated policy and set of security standards for special access programs and sensitive compartmented information.

BIBLIOGRAPHY OF UNCLASSIFIED SOURCES

- Anderson, Martin E. "Counterterror Data Unsatisfactory, Locals Tell GAO." CQ *Homeland Security: Intelligence*, 27 August 2003. URL: <<http://homeland.cq.com/hs/display>>. Accessed 29 May 2004.
- _____. *Fear of the Unknown: Interest Groups Wary of Pending Information Sharing Rules*. CQ Homeland Security: Local Response, 2 October 2003. URL: <www.homeland.cq.com/hs/display>. Accessed 29 April 2004.
- Armor, Mildred. "Secret Sessions of Congress: A Brief Historical Overview." *CRS Report for Congress* RS20145. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, updated 5 August 2003. URL: <www.fas.org/man.crs/RS20145>. Accessed 28 May 2004.
- Bazen, Elizabeth B. "Intelligence Identities Protection Act." *CRS Report for Congress* RS20198. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, 3 October 2003. URL: <www.fas.org/man.crs/RS21636>. Accessed 2 March 2004.
- Best, Richard A. "Homeland Security: Intelligence Support." *CRS Report for Congress* RS21283. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, updated 23 February 2004. URL: <www.fas.org/man.crs/RS21283>. Accessed 28 May 2004.
- Bolkom, Christopher. "Homeland Security: Establishment and Implementation of Northern Command." *CRS Report for Congress* RS 21322. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, updated 14 May 2003. URL: <www.fas.org/man/crs/RS21322>. Accessed 10 January 2004.
- Bruce, James B. *Laws and Leaks of Classified Intelligence, The Consequences of Permissive Neglect*. Central Intelligence Agency Homepage. URL: <www.odci.gov/csi/studies.vol47no1/articl04.html>. Accessed 13 June 2004.
- Clark, Robert. *Intelligence Analysis: A Target-Centric Approach*. Washington, DC: CQ Press, 2004.
- Central Intelligence Agency. *Terrorist Threat Integration Center Information Sheet, 2004*. Langley, VA: CIA, 2004.
- _____. *World Factbook 2003*. Springfield, VA: National Technical Information Service, 2003.

- Cumming, Alfred. "FBI Intelligence Reform Since September, 11, 2001: Issues and Options for Congress." *CRS Report for Congress* RL 32366. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, 6 April 2004. URL: <www.fas.org/mon/crs/RL32411>. Accessed 28 May 2004.
- Davis, John W. "Deception – Magic!" *Military Intelligence* 29, no. 4 (2003): 20-22.
- Defense Intelligence Agency Regulation 59-1. "DoD Intelligence Dissemination Program." 12 June 1995.
- _____. 60-4. "Procedures Governing DIA Intelligence Activities That Affect U.S. Persons." 3 December 1997.
- Department of Defense Directive (DoDD) 5200.1-R. "Information Security Program." 1 January 1997.
- _____. 5200.2-R. "DoD Personnel Security Program." 9 April 1999.
- _____. 5240.1. "DoD Intelligence Activities." 25 April 1988.
- _____. 5525.5. "DoD Cooperation with Civilian Law Enforcement Officials." 15 January 1986 (Change 1, 20 December 1989).
- Department of Homeland Security. "Joint Regional Information Exchange System (JRIES)." Information paper. N.p., n.d. Provided on 23 May 2003 by Defense Intelligence Agency Joint Intelligence Task Force-Counterterrorism.
- _____. "Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security concerning Information Sharing." 24 March 2003.
- Department of Justice. "National Criminal Intelligence Sharing Plan Fact Sheet." DOJ Press Release, 14 May 2004. Washington, DC: DOJ, 2004. URL: www.fbi.gov/dojpressrel/factsheet/051404.htm. Accessed 21 May 2004.
- Eggen, Dan. "Letter With Ricin Vial Sent To White House: November Discovery Was Kept Quiet." *Washington Post*, 4 February 2004, A7.
- E-mail survey. "Information Sharing Survey." Conducted by the author, April - May 2004.
- Federal Bureau of Investigation. FBI Director, Letter to Deputy Secretary of Defense. Subject: "Policy for Law Enforcement Sensitive Marking." 19 January 2001.
- Foreign Intelligence Surveillance Act of 1978*. 50 U.S. Code § 1801.

Gharajedaghi, J. *Systems Thinking: Managing Chaos and Complexity*. Boston: Vice Chairman of the Director of Central Intelligence Foreign Denial and Deception Committee. Butterworth-Heinemann, 1999.

Fleischer, Ari, White House Spokesperson, Office of the Press Secretary. "White House Press Briefing." Briefing presented at the White House, Washington, DC, 20 June 2002. URL: <[www.whitehouse.gov/news/releases/2002/06/20020-2.html](http://www.whitehouse.gov/news/releases/2002/06/20020620-2.html)>. Accessed 15 April 2004.

Freedom of Information Act of 1966. 5 U.S. Code § 552.

Freedom of Information Act of 1974. 5 U.S. Code § 552a.

Hastedt, Glenn. *Espionage: A Reference Book*. California: Abc-Clio, 2003.

Homeland Security Act of 2002. Public Law 107-296 (2002).

Hughes-Wilson, John. *Military Intelligence Blunders*. New York: Carroll and Graf, 1999.

Intelligence Identities Protection Act. 50 U.S. Code §§421-426 (1984).

International Association of Chiefs of Police. "Criminal Intelligence Sharing Summit." Spring 2002. *Conference Proceedings*. Alexandria, VA: IACP, 2002. URL: <www.v-one.com/docs/national_criminal_intelligence_sharing_plan.pdf>. Accessed 15 January 2004.

Knezo, Genevieve J. "Sensitive But Unclassified and other Federal Security Controls on Scientific and Technical Information: Historical and Current Controversy." *CRS Report for Congress* RL 31845. CRS Report for Congress RL 31845. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress. Updated 20 February 2004. URL: <www.fas.org/man/crs/RL_31845>. Accessed 15 April 2004.

Kolodner, Janet L. "An Introduction to Case-Based Reasoning." *Artificial Intelligence Review* 6 (1992): 3-34.

Loescher, M.S. and others. *Proteus: Insights from 2020*. Utrecht, Netherlands: Copernicus Institute Press, 2000.

Lipowicz, Alice. "Ridge Proposes Plan to Link First Responder Radios." CQ Homeland Security: Local Response, 23 February 2004. URL: <<http://homeland.cq.com/hs/display>>. Accessed 29 April 2004.

Lowenthal, Mark. *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press, 2000.

Moynihan, Daniel Patrick. *Secrecy*. New Haven: Yale University Press, 1998.

Murphy, Gerard R. and Martha R. Plotkin. Police Executive Research Forum. "Protecting Your Community From Terrorism: The Strategies for Local Law Enforcement Series, Volume 1: Improving Local-Federal Partnerships." 2003.

Myer, Josh. "Fingers Point at an Intelligence Wall." *Los Angeles Times*, 14 April 2004.

National Security Act of 1947. 50 U.S. Code § 401 (1947).

Odom, William E. *Fixing Intelligence: For A More Secure America*. New Haven, Conn: Yale University Press, 2003.

O'Guin, Michael and Timothy Olgivie. "The Science, Not Art, of Business Intelligence." *Competitive Intelligence Review* 12, no. 4 (2001): 15-24.

Relyea, Harold C. "Homeland Security: The Presidential Coordination Office." *CRS Report for Congress* RL31148. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, updated 30 March 2004. URL: <www.fas.org/man/crs/RL31148>. Accessed 25 April 2004.

Shenon, Philip. "Local Officials Accuse FBI of Not Cooperating." *The New York Times*, 12 November 2001.

(b) (6). *Information Sharing Between Law Enforcement and the Intelligence Community*. MSSJ Thesis chaired by (b) (6). Washington, DC: Joint Military Intelligence College, July 2003.

Sollenberger, Mitchell A. "Sensitive Security Information (SSI) and Transportation Security: Background and Controversies." *CRS Report for Congress* RS 21727. CRS Military and National Security. Washington, DC: Congressional Research Service, Library of Congress, 5 February 2004. URL: <www.fas.org/man/crs/S21727>. Accessed 10 April 2004.

Stevens, Gina Marie. "Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws." *CRS Report for Congress* RL31730. Washington, DC: Congressional Research Service, Library of Congress. Updated 21 March 2003.

Tenet, George J, Director of Central Intelligence. "Iraq and Weapons of Mass Destruction." Speech presented at Georgetown University, Washington, DC, 5 February 2004. URL: <www.georgetownuniversity.edu/publicaffairs/tenet/05022004.html>. Accessed 8 March 2004.

Through Our Enemies' Eyes. Virginia: Brassey's, 2002.

Tuttle, Rich. "General Room For Improvement In Sharing Homeland Defense Info." *Aerospace Daily*, 29 January 2004.

USA Patriot Act of 2001. Public Law 107-56 (2001).

U.S. Army Regulation (AR) 331-10. U.S. Army Intelligence Activities. Washington, DC: Department of the Army, March 2003.

_____. 10-22. Access to and Release of Official Information. Washington, DC: Department of the Army, March 2003.

_____. 11-2. External Collaborative Computing Security Policy. Washington, DC: Department of the Army, 29 August 2003.

_____. 51-4. Coordination and Dissemination of Finished Intelligence Publications. Washington, DC: Department of the Army, 28 April 2000.

U.S. Attorney General. Memorandum, subject: "Guidelines for FBI National Security Investigations and Intelligence Collection. 31 October 2003.

U.S. Congress, House., Permanent Select Committee on Intelligence. *Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community*. 108th Cong., 1st sess., 2003. Committee Print.

_____. House. House of Representatives Rule (HR) 10-24. Accountability and Handling of Collateral Classified Material, 30 January 1989.

_____. House. House of Representative Rule (HR) 10-25. Accountability and Handling of Classified Material Requiring Special Control, 17 July 1986.

_____. Joint Hearings, Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. "Homeland Security: Information Sharing Activities Face Continued Management Challenges: Testimony Before the U.S. Congress September 23, 2002." *United States General Accounting Office*. Washington, DC: General Accounting Office, 1 October 2002.

_____. Senate. Committee on the Judiciary, Subcommittee on Immigrations. Hearing on Information Sharing: Testimony of Janice L. Jacobs, Deputy Assistant Secretary of State For Visa Services. 107th Cong., 2d sess., 15 July 2003. URL: <<http://travel.state.gov/testimony8.html>>. Accessed 22 March 2004.

_____. Senate. Committees on Appropriations Armed Services, and Select Committee on Intelligence. *Threat of Terrorism to the United States: Statement for the Record, Louis J. Freeh, Director, Federal Bureau of Investigation*. 99th Cong., 1st sess., 10 May 2001.

_____. Senate, Select Committee on Intelligence and House, Permanent Select Committee on Intelligence. *Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attack of September 11, 2001*. Hearings, 107th Cong., 2nd sess., 17 June 2004.

U.S. Constitution. IV and V Amendments.

U.S. Department of State, Bureau of Public Affairs. *Patterns of Global Terrorism 2003: Corrected Year in Review, Appendix A, and Appendix G*. Washington, DC: DOS Publication 31932, 2003. URL: <www.state.gov/s/ct/rls/pgtrpt/2003/>. Accessed 23 June 2004.

U.S. President. Executive Order 12333. "United States Intelligence Activities." 4 Dec 1981.

_____. Executive Order 12958. "Classified National Security Information." 17 Apr 1995.

_____. Executive Order 12968. "Access to Classified Information." 2 August 1995.

_____. Executive Order 13228. "Creation of Office of Homeland Security and Homeland Security Counsel." 8 October 2001. As amended by Executive Orders 13284 & 13286.

_____. Executive Order 13231. "Critical Infrastructure Protection in the Information Age." 16 Oct 2001.

_____. Executive Order 13292. "Further Amendment to the Executive Order 12958, as amended, Classified National Security Information." 25 March 2003.

_____. Further Amendment to Executive Order 12958, as amended. "Classified National Security Information." 25 March 2003, under "White House Releases." URL: <www.whitehouse.gov/news/releases/2003/20030325.html>. Accessed 25 April 2004.

Wilson, Clay. "Network Centric Warfare: Background and Oversight Issues for Congress." *CRS Report for Congress* RL 32411. "CRS Military and National Security." Washington, DC: Congressional Research Service, Library of Congress, 2 June 2004). URL: <[www.fas.org/man/crs/RL 32411](http://www.fas.org/man/crs/RL_32411)>. Accessed 20 March 2004.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

