Description of document:	Department of the Treasury (USDT) Office of Intelligence and Analysis (OIA) Office of Security Programs (OSP) quarterly self-inspection reports, 2017-2020
Requested date:	13-November-2020
Release date:	26-June-2024
Posted date:	08-July-2024
Source of document:	Freedom of Information Act Request Department of the Treasury Departmental Offices (DO) Director, FOIA and Transparency 1500 Pennsylvania Avenue NW Washington, DC 20220 Email: FOIA@treasury.gov?subject=FOIA Request Treasury FOIAXpress PAL Request FOIA.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

June 26, 2024

RE: Your FOIA Request to Treasury, Case Number 2021-FOIA-00182

This is the Office of Intelligence and Analysis's (OIA) final response to your Freedom of Information Act (FOIA) request to the U.S. Department of the Treasury, dated November 13, 2020. You requested copies of records related to:

"An electronic/digital copy of the Treasury Department Office of Security Programs quarterly self-inspection reports on Treasury Departmental Offices covering quarters during calendar years 2017, 2018, 2019, 2020."

Your request has been processed under the provisions of the FOIA, 5 U.S.C. § 552. A reasonable search was conducted for records responsive to your request. We have considered the foreseeable harm standard when reviewing records and applying FOIA exemptions." Treasury Departmental Offices conducted a search and located documents totaling 122 pages. After reviewing the information, 111 pages are partially released, and 3 pages are fully withheld pursuant to Exemptions (b)(5), (b)(6) and (b)(7)(e) as identified below:

FOIA Exemption 5 exempts from disclosure "inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency." This includes communications forming part of the deliberative process, attorney-client privilege, or attorney work product.

FOIA Exemption 6 exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

FOIA Exemption 7 E exempts from disclosure, techniques and procedures for law enforcement investigations or prosecutions, which, if disclosed, could reasonably be expected to risk circumvention of the law.

There are no fees assessed at this time since allowable charges fell below $25.

You have the right to appeal this decision within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and

reconsider your request and the agency's decision. Your appeal must be in writing, signed by you or your representative, and should contain the rationale for your appeal. Please also cite the FOIA reference number noted above. Your appeal should be addressed to:

FOIA Appeal
FOIA and Transparency
Office of Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you submit your appeal by mail, clearly mark the letter and the envelope with the words "Freedom of Information Act Appeal." Your appeal must be postmarked or electronically transmitted within 90 days from the date of this letter.

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact our FOIA Public Liaison for assistance via email at FOIAPL@treasury.gov, or via phone at (202) 622-8098. A FOIA Public Liaison is a supervisory official to whom FOIA requesters can raise questions or concerns about the agency's FOIA process. FOIA Public Liaisons can explain agency records, suggest agency offices that may have responsive records, provide an estimated date of completion, and discuss how to reformulate and/or reduce the scope of requests in order to minimize fees and expedite processing time.

If the FOIA Public Liaison is unable to satisfactorily resolve your question or concern, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may contact the agency directly by email at OGIS@nara.gov, by phone at (877) 684-6448, by fax at (202) 741-5769 or by mail at the address below:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001

Please note that contacting any agency official (including the FOIA analyst, FOIA Requester Service Center, FOIA Public Liaison) and/or OGIS is not an alternative to filing an administrative appeal and does not stop the 90-day appeal clock

You may reach me via telephone at 202-622-0930, extension 2; or via e-mail at FOIA@treasury.gov. Please reference FOIA case number 2021-FOIA-00182 when contacting our office about this request.

Sincerely,

Kate Amlin
Deputy Assistant Secretary
Office of Intelligence and Analysis

Enclosures
Responsive document set (122 pages)

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 18, 2017

(b)(5), (b)(6), (B)(7)(e)

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 4, 2017

MEMORANDUM FOR: Michael W. Mason
Deputy Assistant Secretary for Security

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: Self-Inspection Office of Security Programs 2nd Quarter FY 2017

During the 2nd Quarter FYI7, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury Organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

A security violation is any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. A security infraction includes any deviation from governing security regulations that does not result in an unauthorized disclosure or compromise of classified information nor otherwise constitutes a security violation.

On March 15, 2017, OSP inspected the office of Legislative Affairs, which is located in the Main Treasury building. During the inspection, the OSP randomly selected rooms (B)(7)(e) (B)(7)(e) to evaluate and ensure employees are complying with information security policy and procedures. A total of 11workstations, five security containers and five Treasury Secure Data Network (TSDN) terminals were inspected.

(B)(7)(e) is unoccupied. One security container (B)(7)(e) was located inside the office. The security container could not be opened because the responsible individual transferred from Treasury and did not notified (b)(6) Administrative Specialist for Legislative Affair is aware the security container needs to be reported to OSP Physical Security Branch and the combination and the SF 700 (Security Container Information Sheet) requires changing.

(B)(7)(e) is currently unoccupied. One security containers (B)(7)(e) was located inside the office. The security container could not be opened due to the responsible individual transferred from Treasury and did not notified (b)(6) is aware the security

container needs to be reported to OSP Physical Security Branch and the combination and the SF 700 (Security Container Information Sheet) requires changing.

(B)(7)(e) is occupied by Luke Ballman, Deputy Assistant Secretary for TFI and contains one TSDN terminal. Mr. Ballman was asked to logon to his TSDN terminal for OSP to review six random samplings of classification activity electronically were identified processed information (e.g. emails). No classification marking discrepancies were noted. Mr. Ballman was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. Mr. Ballman displayed a clear understanding of policies and procedures.

Rooms (B)(7)(e) were unoccupied. Both offices contained one TSDN terminal and both were disabled.

Room (B)(7)(e) is unoccupied. This room will be assigned to the incoming Assistant Secretary for Legislative Affairs. One security container is located in the room. The security container could not be opened due to the responsible individual transferred from Treasury and did not notified (b)(6) is aware the security container needs to be reported to OSP Physical Security Branch and the combination and the SF 700 requires changing.

(b) (6), (b) (7)(E) One security container (B)(7)(e) is located in the room. The security container is missing the General Service Approved (GSA) label. (b)(6) (b)(6) was told that the security container needs to be reported to physical security for proper decommissioning. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information (b)(6) displayed a clear understanding of policies and procedures.

(B)(7)(e) is unoccupied. This room will be assigned to the incoming Deputy Assistant Secretary for Legislative Affairs. The room has one TSDN terminal, but is currently disabled.

(B)(7)(e) is unoccupied. This room will be assigned to the Senior Advisor for Legislative Affairs. The room has one TSDN terminal, but is currently disabled. One security container (b) (7)(E) is located in the room. The security container could not be opened due to the responsible individual transferred from Treasury and did not notified (b)(6) (b)(6) is aware the security container needs to be reported to OSP Physical Security Branch and the combination and the SF 700 (Security Container Information Sheet) requires changing.

On March 16, 2017, OSP inspected the Office of Economic Policy, which is located in the Main Treasury building. During the inspection, the OSP randomly selected rooms (b) (7)(E) (b) (7)(E) to evaluate and ensure employees were complying with information security policy and procedures. Economic Policy has no TSDN terminals. A total of six workstations and four security containers were inspected.

(b) (7)(E), (b) (6) Economist for Legislative Affairs. (b)(6) has one security container located in his office. The security container is being used to store Sensitive, But Unclassified Information (SBU). (b)(6) was interviewed on the application

of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Director Microeconomics. (b)(6) has one security container in her office. The security container is being used to store SBU. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Economist. There is one security container in the office. The security container is being used to store SBU. Both employees' were interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. The employees' displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Economist (b)(6) has one security container with classified information. Ten classified documents were reviewed for proper classification and all had portion marking discrepancies, however, all documents were from outside agencies.(b)(6) (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Economist.(b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

On March 17, 2017, OSP inspected the office of Tax Policy, which is located in the Main Treasury building. During the inspection, the OSP selected randomly rooms (b) (7)(E) (b) (7)(E) to evaluate and ensure employees are complying with policy and procedures. Tax Policy did not have any TSDN terminals. A total of 12 workstations and two security containers were inspected.

(b) (6), (b) (7)(E) Director for Tax Policy. (b)(6) identified two security containers within the Office of Tax policy. One was located in her office room (b) (7)(E) (b) (7)(E) (b)(6) was teleworking and the room was locked, and the security container was not inspected. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Staff Assistant to the Tax Counsel and (b)(6) Staff Assistant to the Tax Counsel. Both employees' were interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. The employees' displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Staff Assistant and (b)(6) (b)(6) Staff Assistant. Both employees' were interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. The employees' displayed a clear understanding of policies and procedures.

(b) (7)(E) is occupied by Timothy Skud, Deputy Assistant Secretary Tax, Trade and Tariff Policy. Mr. Skud was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. Mr. Skud displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Staff Assistant. Both employees' were interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. The employees' displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Deputy Benefits Tax Counsel. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Financial Research. (b)(6) interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Financial Economist. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Deputy to International Tax Counsel. (b)(6) has one security container in his office. The container was not opened because (b)(6) was not in his office. (b)(6) said that the security container is being used to file SBU information.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 10, 2017

MEMORANDUM FOR: **Michael W. Mason**
Deputy Assistant Secretary for Security

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **Office of Security Programs Self-Inspection for 3rd Quarter FY 2017**

During the 3rd Quarter FYI7, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

A security violation is any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. A security infraction includes any deviation from governing security regulations that does not result in an unauthorized disclosure or compromise of classified information nor otherwise constitutes a security violation.

On April 13, 2017 OSP inspected the main office of Assistant Secretary for Management (ASM) located in the Main Treasury building and the Chief Information Office (CIO) located in building (b) (7)(E) Pennsylvania Avenue. During the inspection, OSP randomly selected ASM (b) (7)(E) to evaluate and ensure employees are complying with information security policy and procedures. (b) (7)(E) were inspected to evaluate and ensure employees are complying with information security policy and procedures. During the inspection, OSP interviewed two ASM employees, and inspected two workstations, one Treasury Secure Data Network (TSDN) terminal and reviewed zero classified documents. A total of six CIO employees were interviewed, and a kiosk with two workstations and one security container was inspected. A total of 37 classified documents were reviewed.

(b) (6), (b) (7)(E) Senior Advisor (b)(6) does not have a TSDN terminal however was was interviewed on the application of original and derivative

classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Principal Advisor. (b)(6) has a TSDN terminal however was unable to log into his accoun during the inspection due to an error message message on his account. (b)(6) reported the log in problem to the TSDN helpdesk. OSP discovered there was no Standard Form 701 Activity Security Checklist displayed by the main door to the ASM main office and informed (b)(6) OSPinterviewed (b)(6) on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information and he displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Supervisory Information Technology (IT) Specialist. There was no TSDN terminal or security container located in (b)(6) workstation area (b)(6) (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information and shedisplayed a clear understanding of policies and procedures. OSP requested (b)(6) to log into her TSDN located in the kiosk (b) (7)(E) however due to a prior engagement she informed OSP she was unable to do so during the time of the review.

(b) (6), (b) (7)(E) IT Specialist. There was no TSDN terminal or security container located in his work area. (b)(6) was able to log into his TSDN using the the TSDN kiosk in (b) (7)(E) o his review classification activity. OSP reviewed ten classified emails. The following discrepancies identifiedall emails did not include portion markings and classification authority block was missing. (b)(6) was interviewed on the application of original and derivative classification, and while he admitted not usingsome of the required classification marking procedures, he acknowledges the lack of following them (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (6), (b) (7)(E) IT Specialist. There was noTSDN terminal or security container located in her work area. (b)(6) attempted to log into her TSDN using the the kiosk in (b) (7)(E) but was unsuccessful due to her her account being disabled. (b)(6) (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Information Security Cyber. There was no TSDN terminal or security container located in his work area. (b)(6) was asked to log into his TSDN using the kiosk in (B)(7)(e) OSP reviewed seven classified emails The following discrepancies discovered were, all emails did not include portion markingsand the classification authority block was missing. (b)(6) was interviewed on the application of original and derivative classification, and while he does not utilize some of the required classified marking procedures, he acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (7)(E) kiosk accredited at the Secret level. Two TSDN terminals and one security container (b) (7)(E) are in the kiosk. The kiosk is accessed by all individuals within Information Systems, CIO. Standard Form (SF) 702 Security container Check Sheet is not being used properly to record open/close the security containers. The SF 700 Security Container Information Sheet was outdated and required updating. The security container combination also needs changing.

(b) (6), (b) (7)(E) IT Specialist. There was no TSDN terminal or security container located in her work area. (b)(6) was asked to log into her TSDN using the the kiosk located in (b) (7)(E) OSP reviewed ten classified emails. All the classified emails reviewed during this assessment indicated that all emails were not being portion marked and the classification authority block was missing (b)(6) was asked to open the security container located in the kiosk (b) (7)(E) OSP reviewed ten classified documents. Documents reviewed during this assessment indicated portion markings and the classification authority block was missing. (b)(6) was interviewed on the application of original and derivative classification, and while she does not utilize some of the required making procedures, she acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

On May 10, 2017, OSP inspected the Office of Financial Stability Oversight Council (FOSC), located in the Main Treasury building. During the inspection, OSP randomly selected rooms (b) (7)(E) to evaluate and ensure employees are complying with information security policy and procedures. A total of two workstations were inspected. FOSC did not have any TSDN terminals or security containers located in rooms (b) (7)(E) No classified documents were reviewed.

(b) (6), (b) (7)(E), Policy Advisor. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (7)(E) was occupied by Bimal Patel, Deputy Assistant Secretary. Mr. Patel was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. Mr. Patel displayed a clear understanding of policies and procedures.

On May 17, 2017 OSP inspected the Office of Foreign Assets and Control (OFAC) located in the Freedmans Bank Building. OSP randomly selected rooms (b) (7)(E) (b) (7)(E) to evaluate and ensure employees are complying with information security program policy and procedures. A total of six workstations, two security containers, and five TSDN terminals were inspected. 64 classified documents were reviewed.

(b) (6), (b) (7)(E) Sanction Policy Analyst. (b)(6) was asked to log into her TSDN. OSP reviewed ten classifled emails. All emails were not portion marked and the classification authority block was missing. (b)(6) was asked to open her security container (b) (7)(E) Ten classified documents were reviewed. The documents did not contain proper portion markings and the classification authority block was missing. The SF 700 personnel information was outdated and the safe security combination requires changing. (b)(6) was interviewed on the application of original and derivative classification, and while she does not utilize some of the required marking procedures, she acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (6), (b) (7)(E) Assistant Director Regulatory Affairs. (b)(6) was asked to log into her TSDN. OSP reviewed seven classified emails. All emails were not being portion marked and the classification authority block was missing (b)(6) was asked to open her security container (b) (7)(E) and ten classifled documents were reviewed. Seven out of the ten documents did not contain proper portion markings and the classified authority block was missing. The security container SF 700 was missing and requires to be updated, along with combination change. (b)(6) was interviewed on the application of original and derivative classification, and while she does not utilize some of the required marking procedures, she acknowledges the lack of following them (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (6), (b) (7)(E) Sanction Regulations Advisor. (b)(6) was asked to log into her TSDN. OSP reviewed seven classified emails were reviewed. All emails did not contain proper portion markings and the classified authority block was missing (b)(6) (b)(6) was interviewed on the application of original and derivative classification, and while she does not utilize some of the required marking procedures, she acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (6), (b) (7)(E) Operations Analyst (Automation). (b)(6) does not have a TSDN terminal in his work area. (b)(6) was interviewed on the application of original and derivative classification, marking procedures, use of classification guides, and safeguarding classified information. (b)(6) displayed a clear understanding of policies and procedures.

(b) (6), (b) (7)(E) Administrative Management Specialist. (b)(6) (b)(6) was asked to log into her TSDN. OSP reviewed ten classifled emails. All emails did not contain proper portion markings and the classified authority block was missing. (b)(6) was interviewed on the application of original and derivative classification, and while she does not utilize some of the required making procedures, she acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

(b) (7)(E) is occupied by (b)(6) Associate Director Resource Management. (b)(6) was asked to log into his TSDN. OSP reviewed ten classified emails. No classified marking discrepancies were discovered. The SF 700 ws not properly updated (b)(6) was interviewed on the application of original and derivative classification, and while (b)(6) does not utilize some of the required marking procedures (b)(6) acknowledges the lack of following them. (b)(6) does have an understanding of policies and procedures and the use of classification guides, and safeguarding classified information.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 17, 2017

MEMORANDUM FOR: **Michael W. Mason** (b)(6)
Deputy Assistant Secretary for Security

FROM: (b)(6) (b)(6)
Director, Office of Security Programs

SUBJECT: **Office of Security Programs Self-Inspection for 1st Quarter FY 2017**

During the 1st Quarter of FY17, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury Organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

A security violation is any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. A security infraction includes any deviation from governing security regulations that does not result in an unauthorized disclosure or compromise of classified information nor otherwise constitutes a security violation.

On December 29, 2016 OSP inspected the Office of General Counsel located in the Main Treasury building. During the inspection, OSP randomly selected (b) (7)(E) (b) (7)(E) to evaluate and ensure employees are complying with information security policy and procedures. A total of five workstations with Treasury Security Data Network (TSDN) terminals were inspected in order to review random samplings of derivative classified documents generated electronically. Four security containers were (b)(6) inspected for proper use of safeguarding classified information and random samplings of derivative classified in hard copy paper documents. OSP reviewed 24 random samplings of classified documents generated by Office of General Council employees to include electronically processed information (e.g. emails). OSP reviewed the classified documents to ensure proper classification, marking, downgrading and declassification was administered.

(b) (7)(E) contained one TSDN and one security container. OSP requested (b)(6) (b)(6) log on the TSDN, however she was having issues with logging on the system and was unsuccessful. OSP was unable to review random samplings of classification activity via electronic email. (b)(6) did contact the DO IT service desk to report her log on issues. OSP inspected the security container in (b) (7)(E) and discovered the SF 700 Security Container Information sheet contained outdated information of employees with access to the security container and requires updating. Four hard copy paper classified documents were reviewed for proper classification, marking, downgrading and declassification. No discrepancies were identified. (b)(6) was interviewed on the practical application of original and derivative classification, marking procedures, use of classification guides and safeguarding classified information. She displayed a clear understanding of policies and procedures.

(b) (7)(E) contained one TSDN. OSP requested (b)(6) to log on the TSDN to review random samplings of classification activity via electronic email. OSP inspected five classified emails with attachments and discovered no use of portion markings on derivative emails generated. OSP conducted on the spot classification marking training to educate the employee on the proper use of portion markings on classified generated emails and attachments and provided the Information Security Oversight Office (ISOO) Marking Guide. (b)(6) was interviewed on the practical application of original and derivative classification, marking procedures, use of classification guides and safeguarding classified information. She displayed a clear understanding of policies and procedures.

OSP inspected one security container located in (b) (6), (b) (7)(E) office and discovered all security forms were completed as required. Four hard copy paper classified documents were reviewed for proper classification, marking, downgrading and declassification. No discrepancies were identified.

(b) (7)(E) contained one TSDN. OSP requested (b)(6) to log on TSDN to review random samplings of classification activity via electronic email. Four classified emails with attachments were reviewed for proper classification, marking, downgrading and declassification. No discrepancies were identified. (b)(6) was interviewed on the practical application of original and derivative classification, marking procedures, use of classification guides and safeguarding classified information. She displayed a clear understanding of policies and procedures.

(b) (7)(E) contained one TSDN. OSP requested (b)(6) to log on TSDN to review random samplings of classification activity via electronic email. Three classified emails with attachments were reviewed for proper classification, marking, downgrading and declassification. No discrepancies were discovered. (b)(6) was interviewed on the practical application of original and derivative classification, marking procedures, use of classification guides and safeguarding classified information. He displayed a clear understanding of policies and procedures.

(b) (7)(E) contained one TSDN. OSP requested (b)(6) to log on the TSDN to review random samplings of classification activity via electronic email. Four classified emails with attachments were reviewed for proper classification, marking, downgrading and declassification. No discrepancies were identified. (b)(6) was interviewed on the practical application of original and derivative classification, marking procedures, use of classification guides and safeguarding classified information. He displayed a clear understanding of policies and procedures.

OSP inspected the security container located in (b) (6), (b) (7)(E) office and discovered the SF 700 Security Container Information sheet contained outdated information of employees with access to the security container and requires updating.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

December 28, 2017

MEMORANDUM FOR: **Michael W. Mason** (b)(6)
Deputy Assistant Secretary for Security

FROM: (b)(6) (b)(6)
Director, Office of Security Programs

SUBJECT: **Office of Security Programs Self-Inspection for 4th Quarter FY 2017**

I. INTRODUCTION

During the 4th Quarter FYI7, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

The Departmental Offices inspected this quarter were International Affairs (IA) and the Global Security Operations Center (GSOC), Office of the Chief Information Officer (OCIO). The inspectors were (b)(6) Deputy Director, Office of Security Programs, and (b)(6) (b)(6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

A. International Affairs

On August 8, 2017 OSP inspected the offices of IA located in the Main Treasury building. During the inspection, OSP randomly selected IA rooms (b) (7)(E) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of five (5) employees, and inspected five (5) workstations and four (4) security containers. A total of 28 classified documents consisting of memoranda/letters, e-mails, reports, and a slide presentation were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, Transmission and Transportation, and Performance Evaluations met the standards outlined in the

Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, and Classification and Marking, and are detailed below.

1. **Safeguarding.**

a. **Observation:** Standard Form (SF) 700 Security Container Information Sheets were not properly updated and the combinations changed for the security containers in rooms (b) (7)(E) (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared.

b. **Observation:** SF 702 Security Container Check Sheet for the safe located in room (b) (7)(E) was not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment. (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

c. **Observation:** End-of-day security checks are not documented on the SF 701 Activity Security Checklist for rooms (b) (7)(E)

Requirement: TD P 15-71, Chapter III, Section 3.5 does not specifically require the completion of the SF 701 for offices or secure work areas that are not an Open Storage Area or Sensitive Compartmented Information Facility. However, this is a "Best Security Practice" that enhances the security-in-depth posture of the Department of the Treasury.

Corrective Action: OSP recommends that the SF 701 be completed.

2. **Classification and Marking.**

a. **Observation:** Eight (8) memoranda/letters, one (1) slide presentation, and ten (10) classified emails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information

in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

b. **Observation:** Seven (7) memoranda/letters and one (1) slide presentation were missing the proper classification authority block.

Requirement: Classified documents shall identify either the Original Classification Authority, Reason for Classification, and Declassification Instruction or the Derivative Classifier, Source(s), and Declassification Date/Event (TD P 15-71 Chapter III, Section 6.3 and 6.4).

Corrective Action: Ensure employees apply the proper classification authority block per the requirement.

c. **Observation:** One (1) slide presentation was missing the Derivative Classifier, Source, and Declassification Date/Event.

Requirement: Documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. Derivative classifiers shall identify the source(s) and date(s) of the source(s) of derivative classification in the "Derived From" line, and carry forward instructions for declassification date/event in the "Declassify On" line (TD P 15-71, Chapter III, Section 6.4).

Corrective Action: Ensure employees identify the Derivative Classifier, Source(s), and Declassification Date/Event in all slide presentations per the requirement.

B. Global Security Operations Center, Office of the Chief Information Officer

On September 27, 2017, OSP inspected the offices of GSOC, OCIO, (b) (7)(E) (b) (7)(E) OSP conducted a physical walk-through of 23 GSOC work stations, inspected two (2) security containers, and randomly selected four (4) employees to interview in order to evaluate and ensure compliance with information security policy and procedures. A total of 16 classified documents consisting of reports, slide presentations and e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, Transmission and Transportation, Safeguarding, and Performance Evaluations met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed area of Classification and Marking, and are detailed below.

1. **Classification and Marking.**

a. **Observation:** Two (2) e-mails were overclassified. The emails did not contain attachments, and the contents of the email were "For Official Use Only".

Requirement: When users modify existing electronic entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information (TD 15-71, Chapter III, Section 6.d).

Corrective Action: Ensure employees apply the correct overall classification markings to their e-mails per the requirement.

b. **Observation:** One (1) report, one (1) slide presentation, and six (6) e-mails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

c. **Observation:** One (1) slide presentation was missing the identifying Derivative Classifier and did not list the Multiple Sources used as basis for classification. The classification authority block was not in the proper location on the slide presentation.

Requirement: Derivative classifiers are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. When a document is classified derivatively on the basis of more than one source, the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4).

Corrective Action: Ensure all slide presentations identify the Derivative Classifier and Multiple Sources used per the requirement.

d. **Observation:** One (1) email was under-classified. The email was marked "FOUO" but contained an attached report classified as Secret.

Requirement: Emails used as transmittal documents must bear proper classification markings to alert users of the highest classification level of any classified information attached or enclosed. The transmittal email shall also include conspicuously on its face the statement "upon Removal of Attachments, this Document is (indicate Unclassified or correct classification level)" (TD P 15-71, Chapter III, Sections 6.8).

Corrective Action: Ensure emails used as transmittal documents are marked per the requirement.

III. SUMMARY OF OBSERVATIONS

A. Classification Management. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information.

B. Equipment. All survey equipment that processes classified information was properly marked with the appropriate classification labels.

C. Safeguarding. Classified documents were stored in GSA approved security containers (safes). However, in one instance the SF 702, Security Container Check Sheet, was not being completed correctly. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Additionally, the SF 700, Security Container Information sheets, were not being updated and the combinations changed as persons knowing the combinations no longer required access to the security containers. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security containers.

D. Transmission and Transportation. Collateral classified information/material was assessed as being properly transmitted only on the Treasury Secure Data Network (TSDN). None of the individuals interviewed ever had any requirement to courier classified documents.

E. Performance Evaluations. The employee performance plans reviewed contained the required critical element for security.

F. Classification and Marking. 44 classified documents consisting of memoranda/letters, reports, slide presentations, and emails were reviewed. Of these, 29 were assessed as being improperly marked. The most common error was that portion markings were not applied. Only in one (1) instance was a classified document not marked as classified: an email used to transmit a classified attachment. In all instances these deficiencies occurred in documents maintained and transmitted in TSDN, which affords some degree of protection from inadvertent disclosure or spillage. However, failure to properly mark classified documents in the TSDN environment makes it difficult for document owners and recipients to readily identify the proper document handling and transmission requirements.

Document Review Totals	
Total number of documents reviewed	44
Number of documents with discrepancies	29
Percentage of documents with discrepancies	65%
Total number of discrepancies	43
Average number of discrepancies per document	1.5

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 25, 2018

MEMORANDUM FOR: (b)(6)
Associate Chief Information Officer for Cyber Security

FROM: (b)(6)
Director, Office of Security Program (b)(6)

SUBJECT: **FY17 4Q Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on September 27, 2017, a self-inspection of the offices of the Government Security Operations Center (GSOC) located (b) (7)(E) (b) (7)(E) The purpose of this inspection was to review, evaluate and assess GSOC's collateral classification activities and employees' compliance with information security practices and procedures in order to ensure that GSOC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP conducted a physical walk-through of 23 GSOC work stations, inspected two (2) security containers, and randomly selected four (4) employees to interview in order to evaluate and ensure compliance with information security policies and procedures. A total of 16 classified documents consisting of reports, slide presentations and e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, Transmission and Transportation, Safeguarding, and Performance Evaluations met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed area of Classification and Marking, and are detailed below.

Classification and Marking.

1. Observation: Two (2) e-mails were overclassified. The emails did not contain attachments, and the contents of the email were "For Official Use Only".

Requirement: When users modify existing electronic entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information (TD 15-71, Chapter III, Section 6.d).

Corrective Action: Ensure employees apply the correct overall classification markings to their e-mails per the requirement.

2. **Observation:** One (1) report, one (1) slide presentation, and six (6) e-mails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

3. **Observation:** One (1) slide presentation was missing the identifying Derivative Classifier and did not list the Multiple Sources used as basis for classification. The classification authority block was not in the proper location on the slide presentation.

Requirement: Derivative classifiers are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. When a document is classified derivatively on the basis of more than one source, the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4).

Corrective Action: Ensure all slide presentations identify the Derivative Classifier and Multiple Sources used per the requirement.

4. **Observation:** One (1) email was under-classified. The email was marked "FOUO" but contained an attached report classified as Secret.

Requirement: Emails used as transmittal documents must bear proper classification markings to alert users of the highest classification level of any classified information attached or enclosed. The transmittal email shall also include conspicuously on its face the statement "upon Removal of Attachments, this Document is (indicate Unclassified or correct classification level)" (TD P 15-71, Chapter III, Sections 6.8).

Corrective Action: Ensure emails used as transmittal documents are marked per the requirement.

GSOC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above have been completed. GSOC is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

If you have any questions regarding this memorandum, please contact (b)(6) Information Security Specialist, at (b)(6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 25, 2018

MEMORANDUM FOR: (b)(6)
Associate Director, International Affairs

FROM: (b)(6) (b)(6)
Director, Office of Security Programs

SUBJECT: **FY17 4Q Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on August 8, 2017, a self-inspection of the offices of International Affairs (IA) located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess IA's collateral classification activities as well as employees' compliance with information security practices and procedures in order to ensure that IA met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected IA rooms (b) (7)(E) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed a total of five (5) employees, and inspected five (5) workstations and four (4) security containers. A total of 28 classified documents consisting of memoranda/letters, e-mails, reports, and a slide presentation were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, Transmission and Transportation, and Performance Evaluations met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, and Classification and Marking, and are detailed below.

A. Safeguarding.

1. **Observation:** Standard Form (SF) 700 Security Container Information Sheets were not properly updated and the combinations changed for the security containers in rooms (b) (7)(E) (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared.

2. Observation: SF 702 Security Container Check Sheet for the safe located in room (b) (7)(E) was not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment. (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

3. Observation: End-of-day security checks are not documented on the SF 701 Activity Security Checklist for rooms (b) (7)(E)

Requirement: TD P 15-71, Chapter III, Section 3.5 does not specifically require the completion of the SF 701 for offices or secure work areas that are not an Open Storage Area or Sensitive Compartmented Information Facility. However, this is a "Best Security Practice" that enhances the security-in-depth posture of the Department of the Treasury.

Corrective Action: OSP recommends that the SF 701 he completed.

B. Classification and Marking.

1. Observation: Eight (8) memoranda/letters, one (1) slide presentation, and ten (10) classified emails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

2. Observation: Seven (7) memoranda/letters and one (1) slide presentation were missing the proper classification authority block.

Requirement: Classified documents shall identify either the Original Classification Authority, Reason for Classification, and Declassification Instruction or the Derivative Classifier, Source(s), and Declassification Date/Event (TD P 15-71 Chapter III, Section 6.3 and 6.4).

Corrective Action: Ensure employees apply the proper classification authority block per the requirement.

3. Observation: One (1) slide presentation was missing the Derivative Classifier, Source, and Declassification Date/Event.

Requirement: Documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. Derivative classifiers shall identify the source(s) and date(s) of the source(s) of derivative classification in the "Derived From" line, and carry forward instructions for declassification date/event in the "Declassify On" line (TD P 15-71, Chapter III, Section 6.4).

Corrective Action: Ensure employees identify the Derivative Classifier, Source(s), and Declassification Date/Event in all slide presentations per the requirement.

IA is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above have been completed. IA is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

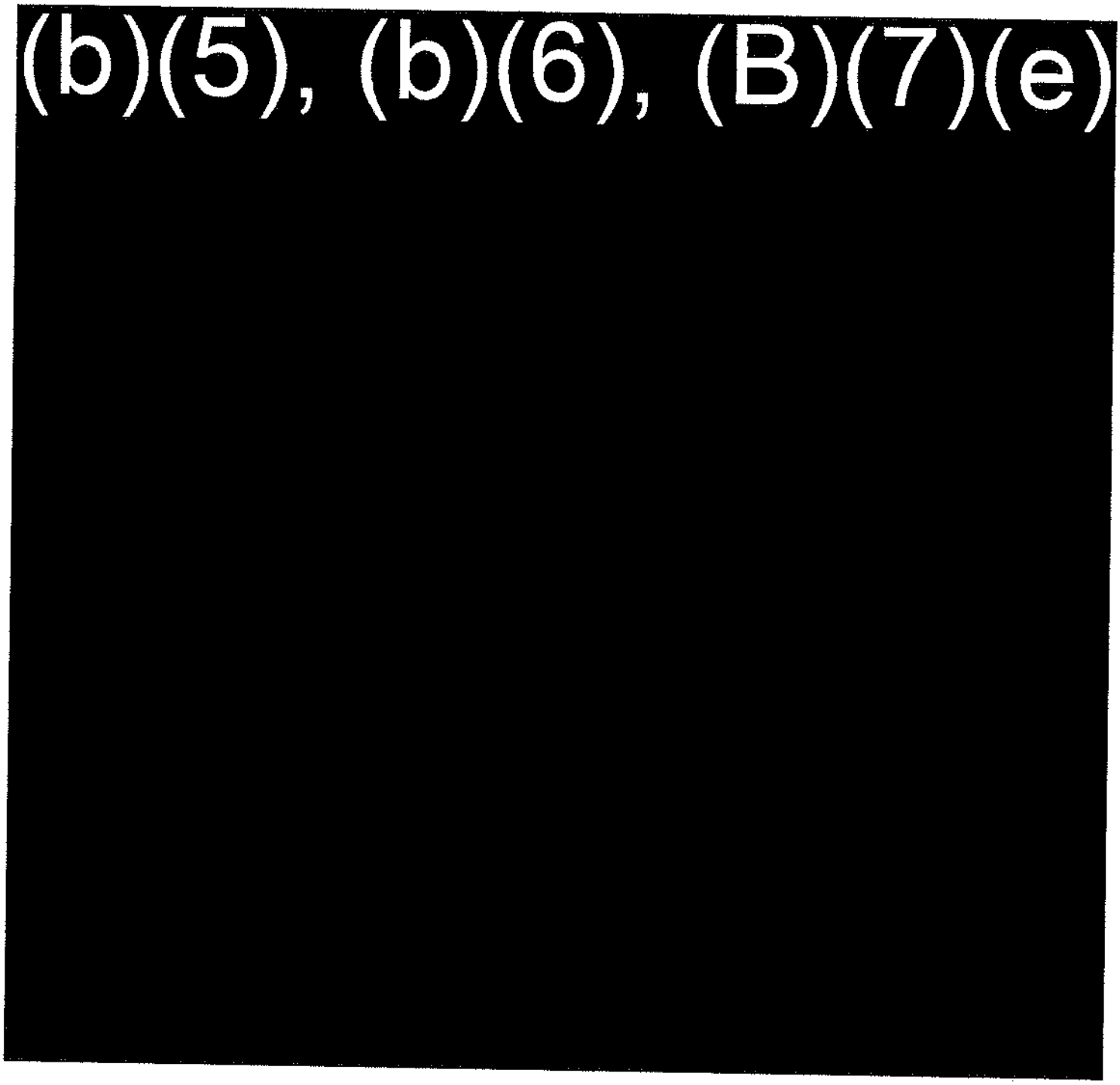
If you have any questions regarding this memorandum, please contac(b)(6)
Information Security Specialist, at(b)(6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 18, 2017

(b)(5), (b)(6), (B)(7)(e)

[redacted]


(b)(5), (b)(6), (B)(7)(e)

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 31, 2017

MEMORANDUM FOR: (b)(6)
Assistant General, Office of General Counsel

FROM: (b)(6)
Deputy Director, Office of Security Programs (b)(6)

SUBJECT: **Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted a self-inspection on the Office of General Counsel (OGC) on December 29, 2016 in accordance with Executive Order 13526 and the Treasury Security Manual TD P 15-71. OSP inspected (b) (7)(E) (b) (7)(E) and interviewed random OGC's cleared employees. The purpose of the inspection was to evaluate and ensure employees are complying with information security policy and procedures, inspect for proper use of safeguarding classified information, review samplings of employees classification activity (derivative and original), ensure use of proper classification, marking, downgrading, declassification, classification authority on electronic and hard copy information and inspect security containers.

OSP reviewed 24 random samplings of derivative classified documents generated by OGC personnel to include electronic and hard copy documents. OSP discovered very minor discrepancies regarding not using portion markings on classified generated emails. OSP conducted on-the-spot training relating to classification marking requirements to educate and reinforce the policies on the proper use of portion markings on classified generated email and attachments.

OSP discovered several security discrepancies during the inspection, relating to security containers. Our security findings are provided below, to include the corrective actions required.

Security Finding 1/Corrective Actions – Standard Form 700 (SF 700) Security Container Information sheet does not reflect current names of cleared employees requiring access to the security container. The security containers identified below require updating and new combinations set. The personnel below were informed to contact the OSP, Physical Security Branch to schedule a time/date to update their SF 700 form and change security container combination.

(b) (6), (b) (7)(F) (one security container).
(b) (6), (b) (7)(E) one security container).

OGC is required to report within 45 days of this memorandum; security findings/corrective actions identified above have been completed. Provide a formal response via memorandum to OSP to close out these security findings.

If you have any questions, please contact my point of contact, (b)(6) Information Security Specialist at (b)(6) @treasury.gov for assistance.

[redacted]

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 23, 2018

MEMORANDUM FOR: [redacted]
Director of Operations
Domestic Finance

FROM: [redacted]
Director, Office of Security Programs

SUBJECT: **Domestic Finance Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on May 16 and 17, 2018, a self-inspection of Domestic Finance (DF) workspaces located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess DF's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that DF met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected DF cubicles in rooms [redacted] to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of eight (8) employees, and inspected five (5) Treasury Secure Data Network (TSDN) workstations and one (1) security container. Of the five (5) TSDN workstations inspected, three (3) were not able to be assessed due to either network connectivity issues or equipment not functioning. A total of 15 e-mails on TSDN were reviewed for proper classification and markings. The assessed areas of Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Classification Management.

(U) Observation: Two (2) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

[redacted]

(U) Corrective Action: The employees received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Safeguarding.

1. ~~(CUI)~~ **Observation:** The SF 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in (b) (7)(E)

(U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

2. ~~(CUI)~~ **Observation:** The SF 702 Security Container Check Sheets for the safe located in (b) (7)(E) was not completed correctly. The last date of entry was September 23, 2016.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement.

C. Performance Evaluations.

(U) Observation: Of the eight (8) employees interviewed, four (4) employees were unable to provide copies of their performance evaluation records for review. The four (4) performance evaluation records that were reviewed contained the required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all DF employees have a critical element for security in their performance evaluation records.

D. Classification and Marking.

1. **(U) Observation:** Thirteen (13) classified emails were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks,

bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) to the employees.

2. (U) Observation: One (1) email marked as "Secret" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified.

(U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

(U) Corrective Action: On-the-spot training regarding safeguarding from over-classification was provided by (b) (6) to the employee.

3. (U) Observation: Six (6) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These six (6) emails were unclassified when separated from the classified attachments.

(U) Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails used as transmittal documents for classified attachments was provided by (b) (6) to the employee.

(U) DF is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. DF is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b) (6) Information Security Specialist, at (b) (6) or email (b) (6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 24, 2018

MEMORANDUM FOR: (b)(6)
Acting Director, Economic Policy

FROM: (b) (6)
Director, Office of Security Programs

(b)(6)

SUBJECT: **Economic Policy Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on March 13, 2018, a self-inspection of the offices of Economic Policy (EP) located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess EP's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that EP met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected EP rooms (b) (7)(E) and (b)(7)(E) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed six (6) employees cleared for access to classified national security information; and inspected four (4) security containers. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents, to include emails. There were no TSDN terminals in any of the inspected rooms. Documents contained in the four security containers were randomly selected for review; no documents were discovered that post-dated October 2016. All documents reviewed were not created by EP employees. Additionally, based on interviews with the custodians of the security containers, they were not sure of the continued need to maintain the documents. EP claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. Discrepancies were observed in the assessed areas of Classification Management and Safeguarding, and are detailed below.

A. Classification Management

1. Observation: Two (2) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

Corrective Action: Both employees received on-the-spot training by Information Security Specialist (b)(6) on the differenees between original and derivative classification, and were given a copy of the current ISOO handbook "Marking Classified National Security Information".

2. Observation: Two (2) employees were aware of the requirement to report security incidents/violations, but did not know the reporting procedures.

Requirement: Departmental Offices employees knowledgeable of the loss or possible compromise of classified information shall immediately report the circumstances to DO security officials (TD P 15-71 Chapter III, Section 18.1).

Corrective Action: Both employees received on-the-spot training by Information Security Specialist (b) (6) on "spill" handling procedures and on the procedures for reporting security incidents/violations.

B. Safeguarding.

1. **Observation:** The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in rooms (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

2. Observation: The SF 702 Security Container Check Sheets for the safes located in rooms (B)(7)(e) were not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

3. Observation: Security (B)(7)(e) located in (b) (7)(E) and used to store classified information designated Confidential and Secret, is a bar-lock cabinet not authorized for storing classified information.

Requirement: Bar-lock cabinets are required to be phased out for storing Secret and Confidential information by DO/bureaus by October 1, 2012 (TD P 15-71, Chapter V, Section 2.10).

Corrective Action: All classified documents contained in the bar-lock cabinet must be removed and stored in a GSA-approved security container.

EP is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified in section B, Safeguarding, have been completed. EP is to provide a formal memorandum to OSP with actions taken in order to close out all security observations.

If you have any questions regarding this memorandum, please contact (b)(6) Information Security Specialist, at (b) (6) or email (b) (6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Michael W. Mason**
Deputy Assistant Secretary for Security

FROM: (b) (6)
Director, Office of Security Programs

SUBJECT: **(U) Office of Security Programs Self-Inspection for 4th Quarter FY 2018**

I. INTRODUCTION

(U) During the 4th Quarter FYI8, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual (TD P 15-71), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter was International Affairs (IA). The inspector was (b) (6) (b) (6), Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

~~(CUI)~~ On August 28, 29, and September 12, 2018, OSP inspected the offices of IA located in the Main Treasury Building and at 1750 Pennsylvania Ave, NW, Washington, DC, 20006. During the inspection, OSP randomly selected IA cubicles in rooms (b) (7)(E) , and of the Main Treasury Building, and rooms (b) (7)(E) of the Office of Technical Assistance (OTA) at 1750 Pennsylvania Ave, NW, to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of 11 employees, and inspected six Treasury Secure Data Network (TSDN) workstations and nine security containers. A total of 28 classified documents consisting of five memoranda, two reports, and 21 e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Safeguarding.

1. ~~(CUI)~~ **Observation:** The SF 700, Security Container Information forms, were not properly updated and the combinations were not changed for the security containers in Main Treasury (b) (7)(E) (container numbers (b) (7)(E)), and for security container number (b) (7)(E) located in (b) (7)(E) of the OTA facility at 1750 Pennsylvania Ave, NW.

(U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

2. ~~(CUI)~~ **Observation:** The SF 702, Security Container Check Sheets, for the safes located in Main Treasury (b) (7)(E) (container numbers (b) (7)(E) , (b) (7)(E)) (b) (7)(E) (container number (b) (7)(E)), and (b) (7)(E) (container number (b) (7)(E)); and for security container (b) (7)(E) in (b) (7)(E) of the OTA facility at 1750 Pennsylvania Ave, NW, were not completed correctly.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and place his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and initial the document. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed, per the requirement.

B. Performance Evaluations.

(U) Observation: Of the 11 employees interviewed, two employees were unable to provide copies of their performance evaluation records for review, one had not yet been issued a performance work plan, and one did not occupy a position requiring the critical performance element for security. Out of the seven performance evaluation records that were reviewed only one contained the required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all IA employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. **Classification and Marking.**

1. (U) Observation: One email and one memorandum used as transmittal documents to forward classified attachments did not include the proper instructions for the classification of the documents when separated from the classified attachments. These two documents were unclassified when separated from the classified attachments.

(U) Requirement: Transmittal documents shall indicate, within the text, the highest level of classified information it transmits. Where the transmittal itself is unclassified, the document shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails used as transmittal documents for classified attachments was provided by (b) (6) to the employee.

2. (U) Observation: 17 classified emails, one classified memorandum, and one report were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) to the employees.

3. (U) Observation: One classified memorandum was missing the "Classified By" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b) (6) to the employee.

4. (U) Observation: One classified memorandum was missing the "Derived From" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b) (6) to the employee.

5. (U) Observation: One classified memorandum was missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify On" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b) (6) to the employee.

6. (U) Observation: Four classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials were used. Eight emails were missing the titles of the classifiers.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b) (6) to the employees.

7. (U) Observation: Three memoranda citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b) (6) to the employees.

III. SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the DO inspected, 11 assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information.

B. (U) Equipment. The SF 710, Unclassified Label, was applied by (b) (6) to all unclassified equipment not properly labelled within the cubicles and offices surveyed, such as photocopiers, printers, and computers, used only for unclassified processing in mixed environments where both classified and unclassified information processing occurred.

C. (U) Safeguarding. Nine GSA approved security containers were in the immediate vicinity of the cubicles/offices inspected. However, only three were able to be opened for review; the SF

700, Security Container Information forms, in these three containers had not been updated and the combinations changed as persons knowing the combinations no longer required access to the security containers, or the combinations had not been changed within the past three years. Additionally, in nine instances the SF 702, Security Container Check Sheet, was not correctly completed. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security containers. As a side note, most of the safes were not in active use, and contained classified documents of unknown value or need for continued retention. None of the documents in the safes were reviewed for classification markings as none of the individuals with access to the safes were the authors of those documents.

D. (U) Transmission and Transportation. Collateral classified information/material was assessed as being properly transmitted only on TSDN. All of the individuals interviewed were familiar with the requirements for properly packaging collateral classified documents for transportation.

E. (U) Performance Evaluations. Of the 11 employees interviewed, two were unable to provide copies of their performance evaluation records for review, one had not yet been issued a performance work plan, and one did not occupy a position requiring the critical performance element for security. Out of the seven performance evaluation records that were reviewed only one (1) contained the required critical element for security.

F. (U) Classification and Marking. 28 classified documents consisting of memoranda, emails, and reports were reviewed. All of these documents were reviewed on TSDN. Of these, 22 were assessed as being improperly marked. The most common error was that portion markings were not properly applied to 19 documents. Twelve documents did not properly identify the derivative classifiers by either full name or were missing the title of the classifier. One email used as a transmittal document to forward classified attachments did not include the proper instructions for the classification of these documents when separated from the classified attachments. Additionally, one memorandum was missing the classification authority block identifying the derivative classifier, source(s) of derivation, and the declassification instructions. Failure to properly mark classified documents makes it difficult for document owners and recipients to readily identify the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	28
Number of documents with discrepancies	22
Percentage of documents with discrepancies	79%
Total number of discrepancies	38
Average number of discrepancies per document	1.7

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 2, 2018

MEMORANDUM FOR: Michael W. Mason (b)(6)
Deputy Assistant Secretary for Security

FROM: (b) (6)
Director, Office of Security Program (b)(6)

SUBJECT: **Office of Security Programs Self-Inspection for 1st Quarter Fiscal Year (FY) 2018**

I. INTRODUCTION

During the 1st Quarter FYI8, the Office of Security Programs (OSP) conducted a self-inspection during regular working hours to review, evaluate and assess individual Departmental Offices collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

The Departmental Office inspected this quarter was the Office of General Counsel (OGC). The inspectors were (b) (6) Deputy Director, Office of Security Programs, and (b)(6) (b) (6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used to assess the following areas: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

Office of General Counsel

On December 20, 2017, OSP inspected the offices of OGC located in the Main Treasury building. During the inspection, OSP randomly selected OGC rooms (b) (7)(E) and (b)(7)(E) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of four (4) employees, and inspected two (2) Treasury Secure Data Network (TSDN) workstations and two (2) security containers. Ten (10) classified documents consisting of a cable/message, memoranda/letters, and e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, and Transmission and Transportation, met the standards outlined in the Treasury Security Manual (TD P 15-71). Performance Evaluations were not assessed as none were available for review.

Discrepancies were observed in the assessed areas of Equipment, Safeguarding, Transmission and Transportation, and Classification and Marking, and are detailed below.

A. Equipment

1. Observation: The Standard Form (SF) 710, Unclassified Label, was not used to label equipment, such as photocopiers, printers, and computers, used only for unclassified processing in mixed environments where both classified and unclassified information processing occurred.

Requirement: The SF 710, Unclassified Label, shall be used in a mixed environment in which classified and unclassified materials are being processed or stored (TD P 15-71, Chapter III, Section 3.9).

Corrective Action: Obtain and label all unclassified equipment in those workspaces/offices where either classified materials or information are processed or stored.

B. Safeguarding.

1. **Observation:** The Standard Form (SF) 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combination changed and a new SF 700 prepared.

2. **Observation:** The SF 702 Security Container Check Sheets for the safes located in rooms (b) (7)(E) were not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment. (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

3. **Observation:** End-of-day security checks were not documented on the SF 701 Activity Security Checklist for (b) (7)(E)

Requirement: TD P 15-71, Chapter III, Section 3.5 does not specifically require the completion of the SF 701 for offices or secure work areas that are not an Open Storage Area or Sensitive Compartmented Information Facility. However, this is a "Best Security Practice" that enhances the security-in-depth posture of the Department of the Treasury.

Corrective Action: OSP recommends that the SF 701 be completed.

4. **Observation:** Window blinds were not closed in offices while classified information was processed on classified information systems.

Requirement: In TSDN work areas all windows which might reasonably afford visual observation of personnel, documents, material, or activities within the space, shall be made opaque or equipped with blinds, drapes, or other coverings to preclude observation (TD P 15-71, Chapter V, Sections 1 and 8.2.e).

Corrective Action: Ensure all exterior windows are made opaque or the blinds/drapes closed while classified information is processed within office spaces.

C. **Classification and Marking.**

1. **Observation:** Four (4) classified emails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

2. **Observation:** Two (2) memoranda/letters and one (1) email were missing the Derivative Classifier, Source, and Declassification Date/Event.

Requirement: Documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. Derivative classifiers shall identify the source(s) and date(s) of the source(s) of derivative classification in the "Derived From" line, and carry forward instructions for declassification date/event in the "Declassify On" line (TD P 15-71, Chapter III, Section 4).

Corrective Action: Ensure employees identify the Derivative Classifier, Source(s), and Declassification Date/Event in all slide presentations per the requirement.

3. **Observation:** Two (2) emails used as transmittal documents were not properly marked. The emails were marked as classified based on the classification level of the attachment, but were unclassified without the attachment.

Requirement: Emails used as transmittal documents must bear proper classification markings to alert users of the highest classification level of any classified information attached or enclosed. The transmittal email shall also include conspicuously on its face the statement "upon Removal of Attachments, this Document is (indicate Unclassified or correct classification level)" (TD P 15-71, Chapter III, Sections 6.8).

Corrective Action: Ensure emails used as transmittal documents are marked per the requirement.

III. SUMMARY OF OBSERVATIONS

A. Classification Management. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information.

B. Equipment. The Standard Form (SF) 710, Unclassified Label, was not used to label equipment, such as photocopiers, printers, and computers, used only for unclassified processing in mixed environments where both classified and unclassified information processing occurred. Failure to label unclassified equipment, particularly Information Technology equipment, increases the risk for data spillages or inadvertent disclosures of classified information.

C. Safeguarding. Classified documents were stored in GSA approved security containers (safes). However, the SF 702, Security Container Check Sheets, were not being completed correctly. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Additionally, in one instance, the SF 700, Security Container Information sheet, was not being updated and the safe combination changed as persons knowing the combination no longer required access to the security container. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security container.

D. Transmission and Transportation. Collateral classified information/material was assessed as being properly transmitted only on the TSDN. None of the individuals interviewed ever had any requirement to courier classified documents.

E. Performance Evaluations. Performance evaluation plans were not available for review.

F. Classification and Marking. Ten (10) classified documents consisting of a cable/message, memoranda/letters, and e-mails were reviewed. Of these, six (6) were assessed as being improperly marked. The most common error was that portion markings were not applied. In all instances these deficiencies occurred in documents maintained and transmitted in TSDN, which affords some degree of protection from inadvertent disclosure or spillage. However, failure to properly mark classified documents in the TSDN environment makes it difficult for document owners and recipients to readily identify the proper document handling and transmission requirements, which increases the risk for inadvertent disclosures.

Document Review Totals	
Total number of documents reviewed	10
Number of documents with discrepancies	6
Percentage of documents with discrepancies	60%
Total number of discrepancies	9
Average number of discrepancies per document	1.5

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 24, 2018

MEMORANDUM FOR: **Luke Ballman**
Deputy Assistant Secretary, Legislative Affairs

FROM: (b) (6)
Director, Office of Security Programs (b)(6)

SUBJECT: **Legislative Affairs Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on March 26, 2018, a self-inspection of the offices of Legislative Affairs (LA) located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess LA's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that LA met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected LA (b) (7)(E) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed six (6) employees cleared for access to classified national security information; and inspected four (4) security containers. The three security containers located in (b) (7)(E) were unable to be opened and inspected as the current custodians did not have a record of the combinations and had themselves never accessed the safes. The security container located in (B)(7)(e) was opened and the classified documents reviewed; none of the classified documents were prepared by LA personnel, and the newest document was prepared in 2013. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents. (b) (7)(E) is the only room in LA containing a TSDN terminal. However, emails were not reviewed for Classification and Marking since the employee was unable to connect to the server. LA claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. The assessed area of Equipment met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management and Safeguarding, and are detailed below.

A. Classification Management

Observation: Three (3) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

Corrective Action: All three employees received on-the-spot training by Information Security Specialist (b) (6) on the differences between original and derivative classification, and were given a copy of the current ISOO handbook "Marking Classified National Security Information".

B. Safeguarding

1. Observation: The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

2. Observation: The SF 702 Security Container Check Sheets for the safes located in rooms (b) (7)(E) were not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

LA is required to report to OSP within 45 days of this memorandum that all corrective actions the two security observation identified in section B, Safeguarding, have been completed. LA is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

If you have any questions regarding this memorandum, please contact (b) (6) Information Security Specialist, at (b) (6) or email (b)(6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 25, 2018

MEMORANDUM FOR: **Paul Ahern**
Assistant General, Office of General Counsel

FROM: (b) (6)
Director, Office of Security Programs

SUBJECT: **FY18 1Q Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on December 20, 2017, a self-inspection of the Office of General Counsel (OGC) located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess OGC's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that OGC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected OGC (b) (7)(E) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed a total of four (4) employees, and inspected two (2) Treasury Secure Data Network (TSDN) workstations and two (2) security containers. Ten (10) classified documents consisting of a cable/message, memoranda/letters, and e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, and Transmission and Transportation, met the standards outlined in the Treasury Security Manual (TD P 15-71). Performance Evaluations were not assessed as none were available for review. Discrepancies were observed in the assessed areas of Equipment, Safeguarding, Transmission and Transportation, and Classification and Marking, and are detailed below.

A. Equipment

1. Observation: The Standard Form (SF) 710, Unclassified Label, was not used to label equipment, such as photocopiers, printers, and computers, used only for unclassified processing in mixed environments where both classified and unclassified information processing occurred.

Requirement: The SF 710, Unclassified Label, shall be used in a mixed environment in which classified and unclassified materials are being processed or stored (TD P 15-71, Chapter III, Section 3.9).

Corrective Action: Obtain and label all unclassified equipment in those workspaces/offices where either classified materials or information are processed or stored.

B. Safeguarding.

1. **Observation:** The Standard Form (SF) 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combination changed and a new SF 700 prepared.

2. **Observation:** The SF 702 Security Container Check Sheets for the safes located in rooms (b) (7)(E) were not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment. (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

3. **Observation:** End-of-day security checks were not documented on the SF 701 Activity Security Checklist for (b) (7)(E)

Requirement: TD P 15-71, Chapter III, Section 3.5 does not specifically require the completion of the SF 701 for offices or secure work areas that are not an Open Storage Area or Sensitive Compartmented Information Facility. However, this is a "Best Security Practice" that enhances the security-in-depth posture of the Department of the Treasury.

Corrective Action: OSP recommends that the SF 701 be completed.

4. **Observation:** Window blinds were not closed in offices while classified information was processed on classified information systems.

Requirement: In TSDN work areas all windows which might reasonably afford visual observation of personnel, documents, material, or activities within the space, shall be made opaque or equipped with blinds, drapes, or other coverings to preclude observation (TD P 15-71, Chapter V, Sections 1 and 8.2.c).

Corrective Action: Ensure all exterior windows are made opaque or the blinds/drapes closed while classified information is processed within office spaces.

C. **Classification and Marking.**

1. **Observation:** Four (4) classified emails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

2. **Observation:** Two (2) memoranda/letters and one (1) email were missing the Derivative Classifier, Source, and Declassification Date/Event.

Requirement: Documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line. Derivative classifiers shall identify the source(s) and date(s) of the source(s) of derivative classification in the "Derived From" line, and carry forward instructions for declassification date/event in the "Declassify On" line (TD P 15-71, Chapter III, Section 4).

Corrective Action: Ensure employees identify the Derivative Classifier, Source(s), and Declassification Date/Event in all slide presentations per the requirement.

3. **Observation:** Two (2) emails used as transmittal documents were not properly marked. The emails were marked as classified based on the classification level of the attachment, but were unclassified without the attachment.

Requirement: Emails used as transmittal documents must bear proper classification markings to alert users of the highest classification level of any classified information attached or enclosed. The transmittal email shall also include conspicuously on its face the statement "upon Removal of Attachments, this Document is (indicate Unclassified or correct classification level)" (TD P 15-71, Chapter III, Sections 6.8).

Corrective Action: Ensure emails used as transmittal documents are marked per the requirement.

OGC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above have been completed. OGC is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

If you have any questions regarding this memorandum, please contact (b) (6) Information Security Specialist, at (b) (6) or email (b) (6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: Michael W. Mason (b)(6)
Deputy Assistant Secretary for Security

FROM: (b) (6)
Director, Office of Security Programs (b)(6)

SUBJECT: (U) Office of Security Programs Self-Inspection for 3rd Quarter FY 2018

I. INTRODUCTION

(U) During the 3rd Quarter FYI8, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

(U) The DO inspected this quarter were Domestic Finance (DF), and the Office of Terrorist Financing and Financial Crimes (TFFC). The inspector was (b)(6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

A. Domestic Finance

~~(CUI)~~ On May 16 and 17, 2018, OSP inspected the offices of DF located in the Main Treasury building. During the inspection, OSP randomly selected DF cubicles in (b) (7)(E) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of eight (8) employees, and inspected five (5) Treasury Secure Data Network (TSDN) workstations and one (1) security container. Of the five (5) TSDN workstations inspected, three (3) were not able to be assessed due to either network connectivity issues or equipment not functioning. A total of 15 e-mails on TSDN were reviewed for proper classification and markings. The assessed areas of Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71).

Discrepancies were observed in the assessed areas of Classification Management, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

1. **Classification Management.**

   (U) Observation: Two (2) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

   (U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

   (U) Corrective Action: The employees received on-the-spot training by (b) (6) on the differences between original and derivative classification.

2. **Safeguarding.**

   a. ~~(CUI)~~ Observation: The SF 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in room 3312.

   (U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

   (U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

   b. ~~(CUI)~~ Observation: The SF 702 Security Container Check Sheets for the safe located in (b) (7)(E) was not completed correctly. The last date of entry was September 23, 2016.

   (U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

   (U) Corrective Action: Ensure the SF 702 is completed per the requirement.

3. **Performance Evaluations.**

   (U) Observation: Of the eight (8) employees interviewed, four (4) employees were unable to provide copies of their performance evaluation records for review. The four (4) performance evaluation records that were reviewed contained the required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all DF employees have a critical element for security in their performance evaluation records.

4. **Classification and Marking.**

a. **(U) Observation:** Thirteen (13) classified emails were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) to the employees.

b. **(U) Observation:** One (1) email marked as "Secret" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified.

(U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

(U) Corrective Action: On-the-spot training regarding safeguarding from over-classification was provided by (b) (6) to the employee.

c. **(U) Observation:** Six (6) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These six (6) emails were unclassified when separated from the classified attachments.

(U) Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails used as transmittal documents for classified attachments was provided by (b) (6) to the employee.

B. Office of Terrorist Financing and Financial Crimes

~~(CUI)~~ On May 22, 2018, OSP inspected the offices of TFFC, located in the Main Treasury Building. During the inspection, OSP randomly selected cubicles in rooms (b) (7)(E) (b) (7)(E) in order to evaluate and ensure compliance with information security policy and procedures. OSP interviewed nine (9) employees cleared for access to national security information; and inspected eight (8) Treasury Secure Data Network (TSDN) workstations and inspected five (5) security containers. A total of 49 classified documents consisting of 19 memoranda, one (1) PowerPoint presentation, and 29 e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, and Transmission and Transportation and met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

1. **Safeguarding.**

a. ~~(CUI)~~ **Observation:** The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in rooms (b) (7)(E) (b) (7)(E)

(U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

b. ~~(CUI)~~ **Observation:** The SF 702 Security Container Check Sheets for the safes located in (b) (7)(E) were not completed correctly.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement.

2. **Performance Evaluations.**

(U) Observation: Of the nine (9) employees interviewed, only four (4) employees were able to provide copies of their performance evaluation records for review. All four (4) performance evaluation records did not contain a required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all TFFC employees have a critical element for security in their performance evaluation records.

3. **Classification and Marking.**

a. **(U) Observation:** 23 classified emails, nine (9) classified memoranda, and one (1) PowerPoint presentation were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) to the employees.

b. **(U) Observation:** Seven (7) classified memorandum and three (3) classified emails were missing the "Classified by" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71 Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by (b) (6) to the employees.

c. **(U) Observation:** Seven (7) classified memorandum were missing the "Derived from" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived from" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b) (6) to the employees.

d. **(U) Observation:** Seven (7) classified memoranda were missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify on" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71 Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b) (6) to the employee.

e. **(U) Observation:** Ten (10) classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71 Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by (b) (6) to the employees.

f. **(U) Observation:** Three (3) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These five emails were either classified as "Confidential" or "Unclassified" when separated from the classified attachments.

(U) Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training regarding use of emails as transmittal documents was provided by (b) (6) to the employees.

III. SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the Departmental Offices inspected, 17 assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information. However, the highest level of awareness was amongst the TFFC personnel, who routinely reviewed and processed classified information. Two (2) DF personnel could not recall the distinction between original and derivative classification; but these individuals had limited exposure to classified information within the past 12 months. All employees interviewed were provided a copy of the current ISOO handbook "Marking Classified National Security Information".

B. (U) Equipment. The SF 710, Unclassified Label, was applied by (b) (6) to all unclassified equipment not properly labelled, such as photocopiers, printers, and computers, used

only for unclassified processing in mixed environments where both classified and unclassified information processing occurred.

C. (U) Safeguarding. Classified documents were stored in GSA approved security containers (safes). However, in five (5) instances the SF 702, Security Container Check Sheet, was not correctly completed. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Additionally, for these five (5) safes, the SF 700, Security Container Information sheets, had not been updated and the combinations changed as persons knowing the combinations no longer required access to the security containers or the combinations had not been changed within the past three (3) years. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security containers.

D. (U) Transmission and Transportation. Collateral classified information/material was assessed as being properly transmitted only on the TSDN. All of the individuals interviewed were familiar with the requirements for properly packaging collateral classified documents for transportation.

E. (U) Performance Evaluations. Out of the 17 individuals interviewed, nine (9) were unable to produce documentation verifying they had a critical element for security in their individual performance evaluations. Out of the remaining, four (4) performance evaluations met the standard and four (4) did not.

F. (U) Classification and Marking. 64 classified documents consisting of memoranda, emails, and a PowerPoint presentation were reviewed. Of these, 58 were assessed as being improperly marked. The most common error was that portion markings were not properly applied to 46 memoranda, emails, and the PowerPoint presentation. Nine (9) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. One (1) email marked as "Secret" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified. In all instances these deficiencies occurred in emails maintained and transmitted in TSDN, which affords some degree of protection from inadvertent disclosure or spillage. However, failure to properly mark classified documents in the TSDN environment makes it difficult for document owners and recipients to readily identify the proper document handling and transmission requirements. Additionally, seven (7) memoranda were missing the classification authority block identifying the derivative classifier, source(s) of derivation, and the declassification instructions.

Classified Document Review Totals	
Total number of documents reviewed	64
Number of documents with discrepancies	58
Percentage of documents with discrepancies	91%
Total number of discrepancies	90
Average number of discrepancies per document	1.6

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

SEP 2 8 2018

(b)(6)

MEMORANDUM FOR: (b)(6)
Associate Director, International Affairs

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) International Affairs Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on May 22, 2018, a self-inspection of International Affairs (IA) workspaces located in the Main Treasury building, and 1750 Pennsylvania Ave, NW, Washington, DC, 20006. The purpose of this inspection was to review, evaluate and assess IA's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that IA met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP randomly selected IA cubicles in (b) (7)(E) (b) (7)(E) of the Main Treasury Building, and (b) (7)(E) of the Office of Technical Assistance (OTA) at 1750 Pennsylvania Ave, NW, to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of eleven (11) employees, and inspected six (6) Treasury Secure Data Network (TSDN) workstations and nine (9) security containers. A total of 28 classified documents consisting of five (5) memoranda, two (2) reports, and 21 e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Safeguarding.

1. ~~(CUI)~~ Observation: The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in Main Treasury (B)(7)(e) (container (b) (7)(E) and for security container (b) (7)(E) located in room (b)(7)(e) of the OTA facility at 1750 Pennsylvania Ave, NW.

~~CONTROLLED~~

(U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov. NOTE: OTA provided documentation to OSP that this request was submitted for security (b) (7)(E)

2. ~~(CUI)~~ Observation: The SF 702 Security Container Check Sheets for the safes located in Main Treasury (b) (7)(E) container (b) (7)(E) (b) (7)(E) container number (B)(7)(e) and (B)(7)(e) container number (B)(7)(e) and for security container (b) (7)(E) in (b) (7)(E) of the OTA facility at 1750 Pennsylvania Ave., NW, were not completed correctly.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement.

B. Performance Evaluations.

(U) Observation: Of the eleven (11) employees interviewed, two (2) employees were unable to provide copies of their performance evaluation records for review, one (1) had not yet been issued a performance work plan, and one (1) did not occupy a position requiring the critical performance element for security. Out of the seven (7) performance evaluation records that were reviewed only one (1) contained the required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all IA employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. Classification and Marking.

1. (U) Observation: One (1) email and one (1) memorandum used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of

the documents when separated from the classified attachments. These two (2) documents were unclassified when separated from the classified attachments.

(U) Requirement: Transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the document shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (FD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails used as transmittal documents for classified attachments was provided by (b) (6) to the employee.

2. (U) Observation: 17 classified emails, one (1) classified memorandum, and one (1) report were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) to the employees.

3. (U) Observation: One (1) classified memorandum was missing the "Classified by" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by Mr. Corson to the employee.

4. (U) Observation: One (1) classified memorandum was missing the "Derived from" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived from" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b) (6) to the employee.

5. (U) Observation: One (1) classified memorandum was missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify on" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b) (6) to the employee.

6. (U) Observation: Four (4) classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials were used. Eight (8) emails were missing the titles of the classifiers.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by (b)(6) to the employees.

7. **(U) Observation:** Three (3) memoranda citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived from" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b) (6) to the employees.

(U) IA is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. IA is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b) (6) Information Security Specialist, at (b)(6) or email (b)(6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Michael W. Mason** (b)(6)
Deputy Assistant Secretary for Security

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **Office of Security Programs Self-Inspection for 2nd Quarter FY 2018**

I. INTRODUCTION

During the 2nd Quarter FY18, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information".

The Departmental Offices inspected this quarter were Office of the Chief Information Officer (OCIO) Treasury Secure Data Network (TSDN) Program, Tax Policy (TP), Economic Policy (EP), and Legislative Affairs (LA). The inspector was (b)(6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

A. Office of the Chief Information Officer Treasury Secure Data Network Program

On February 6, 2018 OSP inspected the offices of OCIO TSDN Program located in the Main Treasury building. During the inspection, OSP randomly selected TSDN Program cubicles in (b) (7)(E) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of four (4) employees (two (2) federal civilian and two (2) contractor employees), and inspected four (4) workstations and one (1) security container. A total of 22 classified e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the

assessed areas of Equipment, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

1. **Equipment.**

   Observation: The Standard Form (SF) 710, Unclassified Label, was not consistently used to label all unclassified DO LAN terminals used for processing unclassified information in a work environment containing classified equipment.

   Requirement: The SF 710, Unclassified Label, shall be used in a mixed environment in which classified and unclassified materials are processed or stored (TD P 15-71, Chapter III, Sections 3.8 and 3.9).

   Corrective Action: Obtain SF 710s and label all unclassified equipment in those workspaces/offices where classified materials or information are processed or stored.

2. **Safeguarding.**

   Observation: The SF 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in (B)(7)(e)

   Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

   Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdr@treasury.gov.

3. **Performance Evaluations.**

   Observation: Of the two (2) federal civilian employees interviewed, one (1) had a performance work plan available for review; the other was a new employee and had yet to be issued a performance work plan. The performance work plan reviewed did not include the critical element required for personnel whose duties involve significant creation, generation or handling/processing of classified information.

   Requirement: Employees having regular, hands-on work with classified information in any type of capacity shall include the critical performance element for the management of classified information (TD P 15-71, Chapter III, Section 22.2).

   Corrective Action: Amend the employee's performance work plan with the required critical element.

4. **Classification and Marking.**

   a. **Observation:** Nineteen (19) classified emails were missing portion markings.

   Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks,

bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

b. **Observation:** One (1) email marked as "Confidential" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

Corrective Action: Ensure employees apply the proper classification level to emails.

c. **Observation:** Five (5) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These five emails were unclassified when separated from the classified attachments.

Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

Corrective Action: Ensure employees properly mark emails used as transmittal documents.

B. Tax Policy

On February 12, 2018, OSP inspected the offices of TP, located in the Main Treasury Building. OSP conducted an inspection of (b) (7)(E) interviewed four (4) employees cleared for access to national security information; and inspected one (1) security container in order to evaluate and ensure compliance with information security policy and procedures. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents, to include emails. There were no TSDN terminals in any of the inspected rooms. Additionally, the sole security container in room (b) (7)(E) was not used to store classified documents; only documents containing Personal Identifying Information (PII) were contained therein. TP claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of

classified information. Discrepancies were observed in the areas of Classification Management and Transmission and Transportation.

1. **Classification Management.**

   Observation: One (1) employee was unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

   Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

   Corrective Action: The employee received on-the-spot training by (b)(6) Information Security Specialist on the differences between original and derivative classification, and was given a copy of the current ISOO handbook "Marking Classified National Security Information".

2. **Transmission and Transportation.**

   Observation: Two (2) employees were unable to recall the proper packaging and transmission procedures.

   Requirement: Classified documents and information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipients (TD P 15-71, Chapter III, Section 11.4).

   Corrective Action: Both employees received on-the-spot training by (b)(6) Information Security Specialist on the proper procedures for packaging and transmitting classified information.

C. Economic Policy

On March 13, 2018, OSP inspected the offices of EP, located in the Main Treasury Building. OSP conducted an inspection of (b)(7)(E) interviewed six (6) employees cleared for access to national security information; and inspected four (4) security containers in order to evaluate and ensure compliance with information security policy and procedures. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents, to include emails. There were no TSDN terminals in any of the inspected rooms. Documents contained in the four security containers were randomly selected for review; no documents were discovered that post-dated October 2016. All documents reviewed were not created by EP employees. Additionally, based on interviews with the custodians of the security containers, they were not sure of the continued need to maintain the documents. EP claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified

information. Discrepancies were observed in the assessed areas of Classification Management and Safeguarding, and are detailed below.

1. **Classification Management.**

   a. Observation: Two (2) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

   Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

   Corrective Action: Both employees received on-the-spot training by (b)(6) Information Security Specialist on the differences between original and derivative classification, and were given a copy of the current ISOO handbook "Marking Classified National Security Information".

   b. Observation: Two (2) employees were aware of the requirement to report security incidents/violations, but did not know the reporting procedures.

   Requirement: Departmental Offices employees knowledgeable of the loss or possible compromise of classified information shall immediately report the circumstances to DO security officials (TD P 15-71 Chapter III, Section 18.1).

   Corrective Action: Both employees received on-the-spot training by (b) (6) Information Security Specialist on "spill" handling procedures and on the procedures for reporting security incidents/violations.

2. **Safeguarding.**

   a. Observation: The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in (b) (7)(E) and (b) (7)(E)

   Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

   Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

   b. Observation: The SF 702 Security Container Check Sheets for the safes located in (B)(7)(e) were not completed correctly.

   Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days,

regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

c. **Observation:** Security (B)(7)(e) located in (B)(7)(e) and used to store classified information designated Confidential and Secret, is a bar-lock cabinet not authorized for storing classified information.

Requirement: Bar-lock cabinets are required to be phased out for storing Secret and Confidential information by DO/bureaus by October 1, 2012 (TD P 15-71, Chapter V, Section 2.10).

Corrective Action: All classified documents contained in the bar-lock cabinet must be removed and stored in a GSA-approved security container.

D. Legislative Affairs

On March 26, 2018, OSP inspected the offices of LA, located in the Main Treasury Building. OSP conducted an inspection of rooms (b) (7)(E) interviewed six (6) employees cleared for access to national security information; and inspected four (4) security containers in order to evaluate and ensure compliance with information security policy and procedures. The three security containers located in (B)(7)(e) were unable to be opened and inspected as the current custodians did not have a record of the combinations and had themselves never accessed the safes. The security container located in (b) (7)(E) was opened and the classified documents reviewed; none of the classified documents were prepared by LA personnel, and the newest document was prepared in 2013. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents. (B)(7)(e) is the only room in LA containing a TSDN terminal. However, emails were not reviewed for Classification and Marking since the employee was unable to connect to the server. LA claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. The assessed area of equipment met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management and Safeguarding, and are detailed below.

1. **Classification Management.**

Observation: Three (3) employees were unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

Corrective Action: Both employees received on-the-spot training by (b) (6) Information Security Specialist on the differences between original and derivative classification, and were given a copy of the current ISOO handbook "Marking Classified National Security Information".

2. **Safeguarding.**

a. Observation: The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in (b) (7)(E) and (B)(7)(e)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

b. Observation: The SF 702 Security Container Check Sheets for the safes located in (b) (7)(E) were not completed correctly.

Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.h and c).

Corrective Action: Ensure the SF 702 is completed per the requirement.

III. SUMMARY OF OBSERVATIONS

A. Classification Management. Within the Departmental Offices inspected, 20 assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information. However, the highest level of awareness was amongst the TSDN Program personnel, who routinely reviewed and processed classified information. Not all TP, EP, and LA personnel could recall the distinction between original and derivative classification; but these individuals had limited or no exposure to any classified information within the past 12 months.

B. Equipment. The SF 710, Unclassified Label, was not used to label equipment, such as photocopiers, printers, and computers, used only for unclassified processing in mixed environments where both classified and unclassified information processing occurred. Failure to label unclassified equipment, particularly Information Technology equipment, increases the risk for data spillages or inadvertent disclosures of classified information.

C. Safeguarding. Classified documents were stored in GSA approved security containers (safes). However, in nine (9) instances the SF 702, Security Container Check Sheet, was not correctly completed. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Additionally, for nine (9) safes, the SF 700, Security Container Information sheets, were not being updated and the combinations changed as persons knowing the combinations no longer required access to the security containers or the combinations had not been changed within the past three (3) years. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security containers. Furthermore, the security containers located in the offices of TP, EP, and LA should be reviewed to determine the continued need for all of their security containers. The sole security container in TP was not used to store classified documents. The custodians for the three (3) safes used in EP had no familiarity with the documents contained in them. The safes contained classified documents dating back to 1994. Three of the safes located in LA were unable to be opened by the current custodians as they never used them and did not have the combinations; therefore, it is not known if the safes even contained classified documents. The sole safe within LA that could be opened did not have any documents that post-dated 2013. The classified documents maintained in the EP and LA security containers should be reviewed for continued retention and all un-needed documents disposed of in accordance with Treasury's records management and classified document destruction policies. The bar-lock cabinet used for storing classified documents in EP (b) (7)(E) should be immediately cleaned out, classified documents appropriately disposed of, and the cabinet removed from the inventory. Excess safes should be either be decommissioned or returned to the Treasury's inventory for reuse elsewhere.

D. Transmission and Transportation. Collateral classified information/material was assessed as being properly transmitted only on the TSDN. None of the individuals interviewed ever had any requirement to courier classified documents or send/receive classified mail.

E. Performance Evaluations. Out of the 20 individuals interviewed, only the two (2) individuals assigned to the TSDN Program clearly had duties that involved the significant creation, generation or handling/processing of classified information. However, only one had a performance work plan available for review and it lacked the required performance element. The other employee had yet to be issued a performance work plan. With regards to the remaining employees in TP, EP, and LA, their respective DOs should conduct position sensitivity reviews in accordance with TD P 15-71, Chapter I, Section 1, to determine their continued need for access to classified information as well as to determine more accurately whether the provisions of TD P 15-71, Chapter III, Section 22 apply to them.

F. Classification and Marking. 22 classified documents consisting of emails were reviewed. Of these, 20 were assessed as being improperly marked. The most common error was that portion markings were not applied within the bodies of the emails or in the subject lines. Five (5) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These five emails were unclassified when separated from the classified attachments. One (1) email marked as "Confidential" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified. In all instances these deficiencies occurred in emails maintained and transmitted in TSDN, which affords some degree of protection from inadvertent disclosure or spillage. However, failure to properly mark classified documents in the TSDN environment makes it difficult for document owners and recipients to readily identify the proper document handling and transmission requirements.

Classified Document Review Totals	
Total number of documents reviewed	22
Number of documents with discrepancies	20
Percentage of documents with discrepancies	91%
Total number of discrepancies	25
Average number of discrepancies per document	1.25

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 24, 2018

MEMORANDUM FOR: (b)(6)
Director, Management and Services
Tax Policy

FROM: (b)(6)
Director, Office of Security Programs

(b)(6)

SUBJECT: **Tax Policy Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on February 12, 2018, a self-inspection of the offices of Tax Policy (TP) located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess TP's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that TP met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected TP (b) (7)(E) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed four (4) employees cleared for access to classified national security information, and inspected one (1) security container. No classified documents were assessed for Classification and Marking as none of the employees interviewed prepared classified documents, to include emails. There were no TSDN terminals in any of the inspected rooms. Additionally, the sole security container in (b) (7)(E) was not used to store classified documents; only documents containing Personal Identifying Information (PII) were contained therein. TP claimed no derivative classification decisions in its Agency Security Classification Management Program Data (SF 311) report submitted in FY 2017. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. Discrepancies were observed in the areas of Classification Management and Transmission and Transportation.

A. Classification Management

Observation: One (1) employee was unable to recall the difference between original and derivative classification, or of the related guidance for derivative classification authority.

Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

Corrective Action: The employee received on-the-spot training by Information Security Specialist (b) (6) on the differences between original and derivative classification, and was given a copy of the current ISOO handbook "Marking Classified National Security Information".

B. Transmission and Transportation

Observation: Two (2) employees were unable to recall the proper packaging and transmission procedures.

Requirement: Classified documents and information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipients (TD P 15-71, Chapter III, Section 11.4).

Corrective Action: Both employees received on-the-spot training by Information Security Specialist (b) (6) on the proper procedures for packaging and transmitting classified information.

No further actions are required of TP since the corrective actions for each security observation identified above have been completed.

If you have any questions regarding this memorandum, please contact (b) (6) Information Security Specialist, at (b)(6) or email (b) (6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 23, 2018

MEMORANDUM FOR: **Marshall Billingslea**
Assistant Secretary for Terrorist Financing

FROM: (b)(6)
Director, Office of Security Programs (b)(6)

SUBJECT: **Terrorist Financing and Financial Crimes Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on May 22, 2018, a self-inspection of Terrorist Financing and Financial Crimes (TFFC) workspaces located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess TFFC's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that TFFC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected TFFC cubicles in (b) (7)(E) (b) (7)(E) in order to evaluate and ensure compliance with information security policy and procedures. OSP interviewed nine (9) employees cleared for access to national security information; and inspected eight (8) Treasury Secure Data Network (TSDN) workstations and inspected five (5) security containers. A total of 49 classified documents consisting of 19 memoranda, one (1) PowerPoint presentation, and 29 e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management, Equipment, and Transmission and Transportation and met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Safeguarding.

1. ~~(CUI)~~ **Observation:** The SF 700 Security Container Information Sheets were not properly updated and the combination changed for the security containers in (b) (7)(E) and (b) (7)(E)

~~CONTROLLED~~

(U) Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

2. ~~(U)~~ **Observation:** The SF 702 Security Container Check Sheets for the safes located in rooms (B)(7)(e) were not completed correctly.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement.

B. Performance Evaluations.

(U) Observation: Of the nine (9) employees interviewed, only four (4) employees were able to provide copies of their performance evaluation records for review. All four (4) performance evaluation records did not contain a required critical element for security.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all TFFC employees have a critical element for security in their performance evaluation records.

C. Classification and Marking.

1. (U) Observation: 23 classified emails, nine (9) classified memoranda, and one (1) PowerPoint presentation were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall he marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

2. (U) Observation: Seven (7) classified memorandum and three (3) classified emails were missing the "Classified by" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71 Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by (b) (6) to the employees.

3. (U) Observation: Seven (7) classified memorandum were missing the "Derived from" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived from" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b) (6) to the employees.

4. (U) Observation: Seven (7) classified memoranda were missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify on" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71 Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b) (6) to the employee.

5. (U) Observation: Ten (10) classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified by" line (TD P 15-71 Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified by" line was provided by (b) (6) to the employees.

6. (U) Observation: Three (3) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These five emails were either classified as "Confidential" or "Unclassified" when separated from the classified attachments.

(U) Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

(U) Corrective Action: On-the-spot training regarding use of emails as transmittal documents was provided by (b) (6) to the employees.

(U) TFFC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. TFFC is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b)(6) Information Security Specialist, at (b) (6) or email (b) (6) @treasury.gov.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

May 24, 2018

MEMORANDUM FOR: **Tony Arcadi**
Associate Chief Information Officer
Enterprise Infrastructure Operations Services

THRU: (b)(6)
Director, Infrastructure Operations

FROM: (b) (6) (b)(6)
Director, Office of Security Programs

SUBJECT: **Treasury Secure Data Network Program Self-Inspection Findings and Corrective Actions**

The Office of Security Programs (OSP) conducted on February 6, 2018, a self-inspection of the Office of the Chief Information Officer, Enterprise Infrastructure Operations Services (EIOS), Treasury Secure Data Network (TSDN) Program located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess the TSDN Program's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that the TSDN Program met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

During the inspection, OSP randomly selected TSDN Program cubicles located in (B)(7)(e) to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed a total of four (4) employees (two (2) federal civilian and two (2) contractor employees), and inspected four (4) workstations and one (1) security container. A total of 22 classified e-mails were reviewed for proper classification and markings. The assessed areas of Classification Management and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Equipment, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Equipment

Observation: The Standard Form (SF) 710, Unclassified Label, was not consistently used to label all unclassified DO LAN terminals used for processing unclassified information in a work environment containing classified equipment.

Requirement: The SF 710, Unclassified Label, shall be used in a mixed environment in which classified and unclassified materials are processed or stored (TD P 15-71, Chapter III, Sections 3.8 and 3.9).

Corrective Action: Obtain SF 710s and label all unclassified equipment in those workspaces/offices where classified materials or information are processed or stored.

B. Safeguarding.

Observation: The SF 700 Security Container Information Sheet was not properly updated and the combination changed for the security container in (b) (7)(E)

Requirement: Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it (TD P 15-71, Chapter V, Section 4.3).

Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and new SF 700s prepared. Request for this service may be submitted to wdr@treasury.gov.

C. Performance Evaluations.

Observation: Of the two (2) federal civilian employees interviewed, one (1) had a performance work plan available for review; the other was a new employee and had yet to be issued a performance work plan. The performance work plan reviewed did not include the critical element required for personnel whose duties involve significant creation, generation or handling/processing of classified information.

Requirement: Employees having regular, hands-on work with classified information in any type of capacity shall include the critical performance element for the management of classified information (TD P 15-71, Chapter III, Section 22.2).

Corrective Action: Coordinate with the Office of Human Resources and the employee's EIOS supervisor to amend the performance work plan with the required critical element.

D. Classification and Marking.

1. Observation: Nineteen (19) classified emails were missing portion markings.

Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

Corrective Action: Ensure portion markings are used in all classified documents in accordance with the requirement.

2. Observation: One (1) email marked as "Confidential" was overclassified. The email did not have any attachments and the information contained in the text of the email was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

Corrective Action: Ensure employees apply the proper classification level to emails.

3. Observation: Five (5) emails used as transmittal documents forwarding classified attachments did not include the proper instructions for the classification of the emails when separated from the classified attachment. These five emails were unclassified when separated from the classified attachments.

Requirement: Emails used as transmittal documents shall indicate within the text the highest level of classified information it transmits. Where the transmittal itself is unclassified, the email shall be marked as either: Unclassified When the Classified Enclosure (for letters), is Detached; or Unclassified When Classified Attachment (for memos) is Detached (TD P 15-71, Chapter III, Section 5.24 and 6.8).

Corrective Action: Ensure employees properly mark emails used as transmittal documents.

EIOS is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above have been completed. EIOS is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

If you have any questions regarding this memorandum, please contact (b)(6) Information Security Specialist, at (b)(6) or email (b)(6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 16, 2019

MEMORANDUM FOR: (b)(6)
Director of Operations
Domestic Finance

FROM: (b)(6)
Director, Office of Security Program

(b)(6)

SUBJECT: **(U) Domestic Finance Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on June 11 and 13, 2019 a self-inspection of Domestic Finance (DF) workspaces located in the Main Treasury building. The purpose of this inspection was to review, evaluate and assess DF's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that DF met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP randomly selected DF cubicles in rooms (b) (7)(E) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed five employees cleared for access to national security information, inspected two Treasury Secure Data Network (TSDN) workstations, and inspected one security container. A total of twelve documents were reviewed for proper classification and markings. The security container held two classified documents which appeared to be over nine years old. These documents should be reviewed to determine their continued need for retention. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter III, Section 16, Destruction of Classified and Sensitive Information. The assessed areas of, Equipment and Safeguarding met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Transmission and Transportation, Performance Evaluations, and Classification and Marking as detailed below.

A. Classification Management.

(U) Observation: One employee was unable to recall the difference between original and derivative classification.

~~CONTROLLED~~

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Transmission and Transportation

(U) Observation: Four employees were unable to recall the proper packaging and transmission procedures.

(U) Requirement: Classified documents and information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipients (TD P 15-71, Chapter III, Section 11.4).

(U) Corrective Action: All of the employees received on-the-spot training by (b)(6) Information Security Specialist on the proper procedures for packaging and transmitting classified information.

C. Performance Evaluations

(U) Observation: Of the five employees interviewed, no performance work plans were available for review. These employees stated that to the best of their recollection, their performance evaluations last year did not contain the required critical performance element for security. Of these employees, at least two performed duties likely requiring this performance element as they accessed TSDN, created and sent classified emails, and reviewed or prepared classified documents.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all DF employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

D. Classification and Marking

1. (U) Observation: Five emails marked as "Secret" were overclassified. These email were unclassified replies to emails used as transmittal documents for "Secret" level attachments, and the attachments were not appended to the replies; in all instances the information contained in the text of the emails was unclassified.

(U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized

disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

2. **(U) Observation:** Four classified emails, one classified memorandum, and one PowerPoint presentation did not identify the derivative classifier by name and position title; rather, only the employee's initials, or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by first and last name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

3. **(U) Observation:** Four classified emails and one classified PowerPoint presentation were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

(U) DF is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. The only remaining observation requiring corrective action is to ensure that all DF employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records. DF is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b)(6), Deputy Director, at (b)(6) or email (b)(6)@treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Thomas J. Wolverton**
Deputy Assistant Secretary for Security& Counterintelligence

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) Office of Security Programs Self-Inspection for 2nd Quarter FY 2019**

I. INTRODUCTION

(U) During the 2nd Quarter Fiscal Year (FY) 2019, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual (TD P 15-71), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter were Legislative Affairs (LA), Office of Foreign Assets Control (OFAC), and Office of the General Counsel (OGC). The inspector was (b)(6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

A. Legislative Affairs

~~(CUI)~~ On March 19, 2019 OSP inspected the workspaces of LA located in the Main Treasury Building. OSP conducted an inspection of rooms (b) (7)(E) interviewed five employees cleared for access to national security information; and inspected one security container in order to evaluate and ensure compliance with information security policy and procedures. The security container located in room (b) (7)(E) was unable to be opened and inspected as the current custodian was newly assigned to the safe, did not have a record of the combination, and had never accessed the safe. However, according to (b)(6), Senior Advisor, the only change to the contents of that safe since it was last inspected by OSP on March 26, 2018 was the addition of classified documents removed from other LA safes that were decommissioned in FY 2018. These documents were legacy documents that were prepared in FY's outside of the scope of this inspection. Classification and Marking was not assessed as none of the employees interviewed prepared any derivatively classified

~~CONTROLLED~~

documents. Since LA's last inspection by OSP on March 26, 2018, the TSDN terminal located in (b) (7)(E) had been removed. Emails were not reviewed for Classification and Marking since none of LA's current employees had accessed TSDN. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. The assessed areas of Classification Management, Equipment, Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). A discrepancy was observed in the assessed area of Safeguarding as detailed below.

Safeguarding.

~~(CUI)~~ **Observation:** The SF 700, Security Container Information form, was not properly updated and the combination was not changed for the security container in Main Treasury (b) (7)(E) (container (b) (7)(E)).

(U) Requirement: The SF 700 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for its classified contents. Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter III, Section 3.4, and Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and a new SF 700 prepared. Request for this service may be submitted to wdf@treasury.gov.

(U) Recommendation: Conduct a review of the legacy files contained within the security container to determine which documents require continued retention. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter III, Section 16, Destruction of Classified and Sensitive Information.

B. Office of Foreign Assets Control

~~(CUI)~~ On March 20, 2019 OSP inspected the offices of OFAC, located in the Freedman's Bank Building. During the inspection, OSP inspected offices in (b) (7)(E) (b) (7)(E) in order to evaluate and ensure compliance with information security policy and procedures. OSP interviewed eight employees cleared for access to national security information; and inspected seven TSDN workstations and six security containers. A total of 51 classified documents consisting of 14 memoranda, two PowerPoint presentations, and 35 e-mails were reviewed for proper classification and markings. The assessed areas of Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

1. Classification Management

(U) Observation: One employee was unable to recall the difference between original and derivative classification.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the differences between original and derivative classification.

2. **Safeguarding**

a. ~~(CUI)~~ **Observation:** A security container located in a hallway on the second floor with (B)(7)(e) and used to store classified information is a bar-lock cabinet not authorized for storing classified information.

(U) Requirement: Bar-lock cabinets were required to be phased out for storing Secret and Confidential information by DO/bureaus by October 1, 2012 (TD P 15-71, Chapter V, Section 2.10).

(U) Corrective Action: All classified documents contained in the bar-lock cabinet must be removed and stored in a GSA-approved security container.

b. ~~(CUI)~~ **Observation:** The SF 702 Security Container Check Sheets for the safes (b) (7)(E) contained no annotations. The concern is that these security containers are not being checked daily or the required documentation is not annotated each time the safe is opened.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement. While the "checked by" column is not required to be annotated, OSP recommends as a best security practice that this column be used to document that the safe was checked on normal business days regardless of whether the equipment was opened or not.

c. ~~(CUI)~~ **Observation:** The SF 700 Security Container Information Sheets were not properly updated and the combinations changed. Security (b) (7)(E) was assigned to a new custodian who did not know its combination and was unable to access it. Security (b) (7)(E) was missing its SF 700.

(U) Requirement: The SF 700 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for its classified contents. Combinations on in-service equipment shall be changed whenever a person knowing the

combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter III, Section 3.4, and Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combination changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

d. (U) Observation: Two employees were unaware of the requirement to close window blinds in offices that process classified information on classified information systems.

(U) Requirement: All windows which might reasonably afford visual observation of personnel, documents, material, or activities within the space shall be made opaque or equipped with blinds, drapes or other coverings to preclude observation (TD P 15-71, Chapter V, Section 8.2.e)

(U) Corrective Action: On-the-spot training on the requirement to close window blinds while using TSDN was provided by (b)(6) to the employees.

2. Performance Evaluations

(U) Observation: Of the eight employees interviewed, five performance work plans were available for review. Only one contained the required critical element for security, four did not; the remaining employees were unsure if this element was present.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all OFAC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

3. Classification and Marking

a. Observation: Two emails marked as "Secret" were overclassified. One email was used as a transmittal document for a "Secret" level attachment, and one email did not have any attachments; in both instances the information contained in the text of the emails was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

b. (U) Observation: Twenty-nine classified emails, one memorandum, and two PowerPoint presentations were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

c. (U) Observation: Ten memoranda and two classified PowerPoint presentations were missing the "Classified By" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

d. (U) Observation: Ten memoranda and two classified PowerPoint presentations were missing the "Derived From" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b)(6) to the employee.

e. (U) Observation: Ten memoranda and two classified PowerPoint presentation were missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify On" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b)(6) to the employee.

f. (U) Observation: Sixteen classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials, or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

g. (U) Observation: One memorandum citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

h. (U) Observation: One email marked "Confidential" was underclassified; the email was used as a transmittal document for a "Secret" level attachment.

(U) Requirement: A transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is classified, the document shall be marked "Upon Removal of Attachment this Document is Classified (fill in appropriate level) (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training regarding the use of transmittal documents for classified attachments was provided by (b)(6) to the employee.

C. Office of the General Counsel

~~(CUI)~~ On March 27, 2019 OSP inspected the offices of OGC located in the Main Treasury Building and the Freedman's Bank Building. During the inspection, OSP inspected OGC rooms (b) (7)(E) located in the Main Treasury Building, and rooms (b) (7)(E) located in the Freedman's Bank Building to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed a total of five employees, and inspected three TSDN workstations and two security containers. Twelve classified e-mails were reviewed for proper classification and markings. The assessed areas of Equipment, Safeguarding, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Performance Evaluations were not assessed as none were available for review and the interviewed employees were unable to recall whether their performance work plans contained the required critical performance element for security.

Discrepancies were observed in the assessed areas of Classification Management and Classification and Marking, and are detailed below.

1. **Classification Management**

(U) Observation: One employee was unable to recall the requirements for hand-carrying classified information within the office/department.

(U) Requirement: Within a DO/bureau facility, classified information may be hand-carried between offices by direct contact of the officials/employees involved or via cleared support staff. The information shall have the appropriate classified document cover sheet affixed to it and be placed inside a single, sealed, opaque envelope/file folder or security locking bag (TD P 15-71, Chapter III, Section 12.3).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the requirements for hand-carrying classified information within the office/department.

2. **Classification & Marking**

a. (U) Observation: Twelve classified emails were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

b. (U) Observation: Seven classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials, or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

c. (U) Observation: Two emails marked "Secret" were overclassified; the emails were used as a transmittal document for "Secret" level attachments, but the text of the emails were unclassified.

(U) Requirement: A transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training regarding the use of transmittal documents for classified attachments was provided by (b)(6) to the employee.

d. (U) Observation: One email citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

III. SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the DO inspected, 18 assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information. Two minor discrepancies were that one employee could not recall the difference between original and derivative classification and one employee could not recall the specific requirements for hand-carrying classified information within the office/department.

B. (U) Safeguarding. Nine GSA approved security containers were inspected; however, only three were able to be opened for review. The remainder were not opened due to the custodians not being available to open the safes or the custodians not knowing the safe combinations. The SF 700, Security Container Information forms, in two of these containers had not been updated to include the required information for the current custodians, and the combinations changed as persons knowing the combinations no longer required access to the security containers, or the combinations had not been changed within the past three years. Additionally, in four instances the SF 702, Security Container Check Sheet, was not correctly completed. The most common error was that the daily opened by/closed by/checked by blocks were not filled in. Collectively, these deficiencies make it difficult to assess whether proper open/close procedures are being followed and make it difficult to determine who actually is responsible for the contents of the security containers. Also, one safe was discovered that is a bar-lock cabinet not authorized for storing classified information. As a side note, most of the safes contained classified documents of unknown value or need for continued retention.

C. (U) Performance Evaluations. Of the 18 employees interviewed, only five were available for review; of these, only one contained the required critical element for security. Five

individuals in LA did not likely occupy positions requiring the critical performance element for security. Four employees' performance work plans did not contain the required critical element for security, and eight were uncertain.

D. (U) Classification and Marking. Sixty-three classified documents consisting of 47 emails, 14 memoranda, and two PowerPoint presentations were reviewed. Sixty of these were assessed as being improperly marked. The most common error was that portion markings were not properly applied to 44 documents. Sixteen documents did not properly identify the derivative classifiers by either full name and were missing the title of the classifier. Four emails were overclassified and one email was underclassified. One email and one memorandum citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used. Additionally, ten memoranda and two PowerPoint presentation were missing the classification authority block identifying the derivative classifier, source(s) of derivation, and the declassification instructions. Failure to properly mark classified documents makes it difficult for document owners and recipients to readily identify the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	63
Number of documents with discrepancies	60
Percentage of documents with discrepancies	95%
Total number of discrepancies	111
Average number of discrepancies per document	1.85

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

JUN 0 4 2019

MEMORANDUM FOR: **Andrew Eck**
Deputy Assistant Secretary, Legislative Affairs

FROM: (b)(6)
Director, Office of Security Programs

(b)(6)

SUBJECT: **(U) Legislative Affairs Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on March 19, 2019 a self-inspection of the workspaces of Legislative Affairs (LA) located in the Main Treasury Building. The purpose of this inspection was to review, evaluate, and assess LA's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that LA met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP inspected (b) (7)(E) interviewed five employees cleared for access to national security information; and inspected one security container in order to evaluate and ensure compliance with information security policy and procedures. The security container located in (b) (7)(E)) was unable to be opened and inspected as the current custodian was newly assigned to the safe, did not have a record of the combination, and had never accessed the safe. However, according to (b)(6) , Senior Advisor, the only change to the contents of that safe since it was last inspected by OSP on March 26, 2018 was the addition of classified documents removed from other LA safes that were decommissioned in FY 2018. These documents were legacy documents that were prepared in FY's outside of the scope of this inspection. Classification and Marking was not assessed as none of the employees interviewed prepared any derivatively classified documents. Since LA's last inspection by OSP on March 26, 2018, the TSDN terminal located in (b) (7)(E) had been removed. Emails were not reviewed for Classification and Marking since none of LA's current employees had accessed TSDN. Performance Evaluations were not assessed as none of the interviewed employees performed duties involving the significant creation, generation or handling/processing of classified information. The assessed areas of Classification Management, Equipment, Transmission and Transportation met the standards

~~CONTROLLED~~

outlined in the Treasury Security Manual (TD P 15-71). A discrepancy was observed in the assessed area of Safeguarding as detailed below.

Safeguarding.

~~(CUI)~~ **Observation:** The SF 700, Security Container Information form, was not properly updated and the combination was not changed for the security container in Main Treasury room (b) (7)(E)

(U) Requirement: The SF 700 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for its classified contents. Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter III, Section 3.4, and Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combinations changed and a new SF 700 prepared. Request for this service may be submitted to wdf@treasury.gov.

(U) Recommendation: Conduct a review of the legacy files contained within the security container to determine which documents require continued retention. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter III, Section 16, Destruction of Classified and Sensitive Information.

(U) LA is required to report to OSP within 45 days of this memorandum that the corrective action listed above has been completed. Although not required, OSP recommends that LA complete the recommended review of legacy classified documents to verify the need for their continued retention. LA is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b)(6), Information Security Specialist, at (b)(6) or email (b)(6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

JUN 0 4 2019

MEMORANDUM FOR: **Paul Ahern**
Assistant General Counsel, Office of the General Counsel

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) Office of the General Counsel Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on March 27, 2019 a self-inspection of the Office of General Counsel (OGC) workspaces located in the Main Treasury Building and the Freedman's Bank Building. The purpose of this inspection was to review, evaluate, and assess OGC's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that OGC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP inspected OGC (b) (7)(E) located in the Main Treasury Building, and (b) (7)(E) located in the Freedman's Bank Building to evaluate and ensure employees were complying with information security policies and procedures. OSP interviewed a total of five employees, and inspected three TSDN workstations and two (2) security containers. Twelve classified e-mails were reviewed for proper classification and markings. The assessed areas of Equipment, Safeguarding, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Performance Evaluations were not assessed as none were available for review and the interviewed employees were unable to recall whether their performance work plans contained the required critical performance element for security. Discrepancies were observed in the assessed areas of Classification Management and Classification and Marking, and are detailed below.

A. Classification Management

(U) Observation: One employee was unable to recall the requirements for hand-carrying classified information within the office/department.

(U) Requirement: Within a DO/bureau facility, classified information may be hand-carried between offices by direct contact of the officials/employees involved or via cleared support staff.

~~CONTROLLED~~

The information shall have the appropriate classified document cover sheet affixed to it and be placed inside a single, sealed, opaque envelope/file folder or security locking bag (TD P 15-71, Chapter III, Section 12.3).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the requirements for hand-carrying classified information within the office/department.

B. Classification & Marking

1. (U) Observation: Twelve classified emails were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

2. (U) Observation: Seven classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials, or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

3. (U) Observation: Two emails marked "Secret" were overclassified; the emails were used as a transmittal document for "Secret" level attachments, but the text of the emails were unclassified.

(U) Requirement: A transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training regarding the use of transmittal documents for classified attachments was provided by (b)(6) to the employee.

4. (U) Observation: One email citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) **Requirement:** When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) **Corrective Action:** On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

(U) OGC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. The only remaining corrective action not corrected is for Performance Evaluations, item B, above. OGC is to provide a formal memorandum to OSP with actions taken in order to close out the security finding.

(U) If you have any questions regarding this memorandum, please contact (b)(6), Information Security Specialist, at (b)(6) or email (b)(6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Thomas J. Wolverton** (b)(6)
Acting Deputy Assistant Secretary for Security&
Counterintelligence

FROM: (b)(6)
Director, Office of Security Programs

(b)(6)

SUBJECT: **(U) Office of Security Programs Self-Inspection for 3rd Quarter FY 2019**

I. INTRODUCTION

(U) During the 3rd Quarter Fiscal Year (FY) 2019, the Office of Security Programs (OSP) conducted a self-inspection during regular working hours to review, evaluate and assess Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual (TD P 15-71), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter was Domestic Finance (DF). The inspector was (b)(6) Information Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

~~(CUI)~~ On June 11 and 13, 2019 OSP inspected the workspaces of DF located in the Main Treasury Building. OSP conducted an inspection of rooms (b) (7)(E) interviewed five employees cleared for access to national security information; inspected two Treasury Secure Data Network (TSDN) workstations; and inspected one security container in order to evaluate and ensure compliance with information security policy and procedures. A total of twelve documents were reviewed for proper classification and markings. The security container held two classified documents which appeared to be over nine years old. These documents should be reviewed to determine their continued need for retention. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter III, Section 16, Destruction of Classified and Sensitive Information. The assessed areas of, Equipment and Safeguarding met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Transmission and Transportation, Performance Evaluations, and Classification and Marking as detailed below.

A. Classification Management.

(U) Observation: One employee was unable to recall the difference between original and derivative classification.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Transmission and Transportation

Observation: Four employees were unable to recall the proper packaging and transmission procedures.

Requirement: Classified documents and information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipients (TD P 15-71, Chapter III, Section 11.4).

Corrective Action: All of the employees received on-the-spot training by (b)(6) Information Security Specialist on the proper procedures for packaging and transmitting classified information.

C. Performance Evaluations

(U) Observation: Of the five employees interviewed, no performance work plans were available for review. These employees stated that to the best of their recollection, their performance evaluations last year did not contain the required critical performance element for security. Of these employees, at least two performed duties likely requiring this performance element as they accessed TSDN, created and sent classified emails, and reviewed or prepared classified documents.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all DF employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

D. Classification and Marking

1. Observation: Five emails marked as "Secret" were overclassified. These email were unclassified replies to emails used as transmittal documents for "Secret" level attachments,

and the attachments were not appended to the replies; in all instances the information contained in the text of the emails was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) **Corrective Action:** On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

2. (U) Observation: Four classified emails, one classified memorandum, and one PowerPoint presentation did not identify the derivative classifier by name and position title; rather, only the employee's initials, or first initial and last name were used.

(U) **Requirement:** DO/bureau documents are required to identify the derivative classifier by first and last name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) **Corrective Action:** On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

3. (U) Observation: Four classified emails and one classified PowerPoint presentation were missing portion markings.

(U) **Requirement:** Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) **Corrective Action:** On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

III. SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the DO inspected, five assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information. A minor discrepancy was that one employee could not recall the difference between original and

derivative classification. This employee, however, was a consumer of classified products and had not exercised derivative classification authority in at least three years.

B. (U) Transmission and Transportation. Four employees were unable to recall the proper packaging and transmission procedures. However, none of these employees were required to hand-carry classified information, which likely contributed to their lack of familiarity with these procedures.

C. (U) Performance Evaluations. Of the five employees interviewed, none of their performance work plans contained the required critical performance element for security. Of these, at least two employees likely occupy positions requiring the critical performance element for security.

D. (U) Classification and Marking. Twelve classified documents consisting of nine emails, two memoranda, and one PowerPoint presentation were reviewed. Seven of these were assessed as being improperly marked. Portion markings were not properly applied to five documents. Six documents did not properly identify the derivative classifiers by full name and were missing the title of the classifier. Five emails were overclassified. Failure to properly mark classified documents makes it difficult for document owners and recipients to readily identify the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	12
Number of documents with discrepancies	7
Percentage of documents with discrepancies	58%
Total number of discrepancies	16
Average number of discrepancies per document	1.3

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Michael W. Mason** (b)(6)
Deputy Assistant Secretary for Security

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) Office of Security Programs Self-Inspection for 1st Quarter FY 2019**

I. INTRODUCTION

(U) During the 1st Quarter FY 2019, the Office of Security Programs (OSP) conducted self-inspections during regular working hours to review, evaluate and assess individual Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual (TD P 15-71), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter was the Government Security Operations Center (GSOC), Office of the Associate Chief Information Officer, Cyber Security. The inspector was (b)(6), Information Security Specialist. The OSP Self-Inspectioo Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. INSPECTION RESULTS

(U) On December 4 and 20, 2018, OSP inspected the workspaces of GSOC located in (B)(7)(e) (B)(7)(e) During the inspection, OSP randomly selected GSOC cubicles and offices located within (B)(7)(e) to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of nine employees, and inspected two Treasury Secure Data Network (TSDN) workstations and two security containers. A total of seven classified documents consisting of five e-mails and two PowerPoint presentations were reviewed for proper classification and markings. The assessed areas of Equipment, Safeguarding, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Performance Evaluations, and Classification and Marking, and are detailed below.

~~CONTROLLED~~

A. Classification Management.

1. (U) Observation: One employee was unaware of the requirement for properly using cover sheets.

(U) Requirement: Classified document cover sheets are used to alert personnel that a document, file, or folder to which it is affixed, respectively contains Top Secret, Secret, or Confidential classified information and must be protected. Classified document cover sheets shall be placed on all classified documents or classified folders when withdrawn from secure storage for internal and external transmission and handling/processing (TD P 15-71 Chapter III, Section 3.7).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the proper use of cover sheets.

2. (U) Observation: Two employees were unable to recall the difference between original and derivative classification.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

(U) Corrective Action: The employees received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Performance Evaluations.

(U) Observation: Of the nine employees interviewed, only three were federal employees. None of the federal employees were able to provide copies of their performance evaluation records for review; however, all stated that their FY 2018 performance evaluations did not contain the required critical element for security. The GSOC Associate Chief Information Security Officer confirmed that none of the federal employees assigned to GSOC had the required critical element for security in their performance evaluation records.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all GSOC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. Classification and Marking.

1. Observation: Two emails marked as "Secret" were overclassified. The emails did not have any attachments and the information contained in the text of the email was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

(U) **Corrective Action:** On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

2. (U) **Observation:** Five classified emails and two PowerPoint presentations were missing portion markings.

(U) **Requirement:** Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) **Corrective Action:** On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

3. (U) **Observation:** One classified PowerPoint presentation was missing the "Classified By" line.

(U) **Requirement:** DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) **Corrective Action:** On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

4. (U) **Observation:** One classified PowerPoint presentation used "Derived By" instead of "Classified By" to identify the derivative classifier.

(U) **Requirement:** Derivatively classified documents shall use "Classified By" to identify the derivative classifier (TD P 15-71, Chapter III, Section 6.4.a).

(U) **Corrective Action:** On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

5. (U) **Observation:** One classified PowerPoint presentation was missing the "Derived From" line.

(U) **Requirement:** The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b)(6) to the employee.

6. (U) Observation: One classified PowerPoint presentation was missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify On" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b)(6) to the employee.

7. (U) Observation: Three classified emails did not identify the derivative classifier by name and position title; rather, only the employees' first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

8. (U) Observation: One email citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

III. SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the DO inspected, nine assigned individuals cleared for access to classified information were interviewed. One employee could not identify the precise requirements for using classified document cover sheets. Additionally, two employees could not recall the distinction between original and derivative classification.

B. (U) Performance Evaluations. None of the three federal employees interviewed had the required critical performance element for security in their FY 2018 performance appraisals.

C. (U) Classification and Marking. Seven classified documents consisting of five emails and two PowerPoint presentations were reviewed. All of these were assessed as being improperly

marked. The most common error was that portion markings were not properly applied to all seven documents. Three documents did not properly identify the derivative classifiers by either full name or were missing the title of the classifier. Two emails were overclassified and one email citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used. Additionally, one PowerPoint presentation was missing the classification authority block identifying the derivative classifier, source(s) of derivation, and the declassification instructions. Failure to properly mark classified documents makes it difficult for document owners and recipients to readily identify the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	7
Number of documents with discrepancies	7
Percentage of documents with discrepancies	100%
Total number of discrepancies	15
Average number of discrepancies per document	2.1

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MAR 1 4 2019

MEMORANDUM FOR: (b)(6)
Associate Chief Information Officer for Cyber Security

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) Government Security Operations Center Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on December 4 and 20, 2018 a self-inspection of the Government Security Operations Center (GSOC) workspaces located in Suite 485, Vienna, Virginia. The purpose of this inspection was to review, evaluate, and assess GSOC's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that GSOC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP randomly selected GSOC cubicles and rooms located in [redacted] to evaluate and ensure employees were complying with information security policy and procedures. OSP interviewed a total of nine employees, and inspected two Treasury Secure Data Network (TSDN) workstations and two security containers. A total of seven classified documents consisting of five e-mails and two PowerPoint presentations were reviewed for proper classification and markings. The assessed areas of Equipment, Safeguarding, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Classification Management.

1. (U) Observation: One employee was unaware of the requirement for properly using cover sheets.

(U) Requirement: Classified document cover sheets are used to alert personnel that a document, file, or folder to which it is affixed, respectively contains Top Secret, Secret, or Confidential classified information and must be protected. Classified document cover sheets shall be placed on all classified documents or classified folders when withdrawn from secure

~~CONTROLLED~~

storage for internal and external transmission and handling/processing (TD P 15-71 Chapter III, Section 3.7).

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the proper use of cover sheets.

2. (U) Observation: Two employees were unable to recall the difference between original and derivative classification.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

(U) Corrective Action: The employees received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Performance Evaluations.

(U) Observation: Of the nine employees interviewed, only three were federal employees. None of the federal employees were able to provide copies of their performance evaluation records for review; however, all stated that their FY 2018 performance evaluations did not contain the required critical element for security. The GSOC Associate Chief Information Security Officer confirmed that none of the federal employees assigned to GSOC had the required critical element for security in their performance evaluation records.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all GSOC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. Classification and Marking.

1. (U) Observation: Two emails marked as "Secret" were overclassified. The emails did not have any attachments and the information contained in the text of the email was unclassified.

(U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

2. (U) Observation: Five classified emails and two PowerPoint presentations were missing portion markings.

(U) **Requirement:** Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) **Corrective Action:** On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

3. (U) Observation: One classified PowerPoint presentation was missing the "Classified By" line.

(U) **Requirement:** DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) **Corrective Action:** On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

4. (U) Observation: One classified PowerPoint presentation used "Derived By" instead of "Classified By" to identify the derivative classifier.

(U) **Requirement:** Derivatively classified documents shall use "Classified By" to identify the derivative classifier (TD P 15-71, Chapter III, Section 6.4.a).

(U) **Corrective Action:** On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

5. (U) Observation: One classified PowerPoint presentation was missing the "Derived From" line.

(U) **Requirement:** The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) **Corrective Action:** On-the-spot training regarding identification of derivative sources was provided by (b)(6) to the employee.

6. (U) Observation: One classified PowerPoint presentation was missing the declassification instructions.

(U) **Requirement:** Derivative classifiers shall carry forward instructions on the "Declassify On" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b)(6) to the employee.

7. **(U) Observation:** Three classified emails did not identify the derivative classifier by name and position title; rather, only the employees' first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

8. **(U) Observation:** One email citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

(U) GSOC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. The only remaining corrective action not corrected is for Performance Evaluations, item B, above. GSOC is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b)(6), Information Security Specialist, at (b)(6) or email (b)(6) @treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

JUN 0 4 2019

MEMORANDUM FOR: **Andrea Gacki**
Director, Office of Foreign Assets Control

FROM: (b)(6)
Director, Office of Security Programs

(b)(6)

SUBJECT: **(U) Office of Foreign Assets Control Self-Inspection Findings and Corrective Actions**

(U) The Office of Security Programs (OSP) conducted on March 20, 2019 a self-inspection of the Office of Foreign Assets Control (OFAC) workspaces located in the Freedman's Bank Building. The purpose of this inspection was to review, evaluate, and assess OFAC's collateral classification activities as well as employees' compliance with information security policies and procedures in order to ensure that OFAC met the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual TD P 15-71, Chapter III, Section 21, "Self-Inspection Program for Classified Information". The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

~~(CUI)~~ During the inspection, OSP inspected offices in rooms (b) (7)(E) in order to evaluate and ensure compliance with information security policy and procedures. OSP interviewed eight employees cleared for access to national security information; and inspected seven TSDN workstations and six security containers. A total of 51 classified documents consisting of 14 memoranda, two PowerPoint presentations, and 35 e-mails were reviewed for proper classification and markings. The assessed areas of Equipment, and Transmission and Transportation met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Classification Management, Safeguarding, Performance Evaluations, and Classification and Marking, and are detailed below.

A. Classification Management

(U) Observation: One employee was unable to recall the difference between original and derivative classification.

(U) Requirement: Employees cleared for access to classified information shall receive training on the principles of derivative classification, identification, and required markings (TD P 15-71, Chapter III, Section 2.9).

~~CONTROLLED~~

(U) Corrective Action: The employee received on-the-spot training by (b)(6) on the differences between original and derivative classification.

B. Safeguarding

1. ~~(CUI)~~ **Observation:** A security container located in a hallway on the second floor with (b)(7)(e) and used to store classified information is a bar-lock cabinet not authorized for storing classified information.

(U) Requirement: Bar-lock cabinets were required to be phased out for storing Secret and Confidential information by DO/bureaus by October 1, 2012 (TD P 15-71, Chapter V, Section 2.10).

(U) Corrective Action: All classified documents contained in the bar-lock cabinet must be removed and stored in a GSA-approved security container.

2. ~~(CUI)~~ **Observation:** The SF 702 Security Container Check Sheets for the safes (b)(7)(E) contained no annotations. The concern is that these security containers are not being checked daily or the required documentation is not annotated each time the safe is opened.

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Section 3.6.b and c).

(U) Corrective Action: Ensure the SF 702 is completed per the requirement. While the "checked by" column is not required to be annotated, OSP recommends as a best security practice that this column be used to document that the safe was checked on normal business days regardless of whether the equipment was opened or not.

3. ~~(CUI)~~ **Observation:** The SF 700 Security Container Information Sheets were not properly updated and the combinations changed. Security container (b)(7)(E) was assigned to a new custodian who did not know its combination and was unable to access it. Security container (b)(7)(E) was missing its SF 700.

(U) Requirement: The SF 700 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for its classified contents. Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter III, Section 3.4, and Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch, to have the security container combination changed and new SF 700s prepared. Request for this service may be submitted to wdf@treasury.gov.

4. (U) Observation: Two employees were unaware of the requirement to close window blinds in offices that process classified information on classified information systems.

(U) Requirement: All windows which might reasonably afford visual observation of personnel, documents, material, or activities within the space shall be made opaque or equipped with blinds, drapes or other coverings to preclude observation (TD P 15-71, Chapter V, Section 8.2.e)

(U) Corrective Action: On-the-spot training on the requirement to close window blinds while using TSDN was provided by (b)(6) to the employees.

C. Performance Evaluations

(U) Observation: Of the eight employees interviewed, five performance work plans were available for review. Only one contained the required critical element for security, four did not; the remaining employees were unsure if this element was present.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all OFAC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

D. Classification and Marking

1. Observation: Two emails marked as "Secret" were overclassified. One email was used as a transmittal document for a "Secret" level attachment, and one email did not have any attachments; in both instances the information contained in the text of the emails was unclassified.

Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails was provided by (b)(6) to the employees.

2. (U) Observation: Twenty-nine classified emails, one memorandum, and two PowerPoint presentations were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2.a.(4) and 6.6.a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b)(6) to the employees.

3. (U) Observation: Ten memoranda and two classified PowerPoint presentations were missing the "Classified By" line.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employee.

4. (U) Observation: Ten memoranda and two classified PowerPoint presentations were missing the "Derived From" line.

(U) Requirement: The identification of the source(s) and date(s) of the source(s) shall be listed on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide used (TD P 15-71, Chapter III, Section 6.4.b).

(U) Corrective Action: On-the-spot training regarding identification of derivative sources was provided by (b)(6) to the employee.

5. (U) Observation: Ten memoranda and two classified PowerPoint presentation were missing the declassification instructions.

(U) Requirement: Derivative classifiers shall carry forward instructions on the "Declassify On" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training regarding declassification instructions was provided by (b)(6) to the employee.

6. (U) Observation: Sixteen classified emails did not identify the derivative classifier by name and position title; rather, only the employees' initials, or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position or by personal identifier, in a manner that is immediately apparent on each

derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4.a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b)(6) to the employees.

7. (U) Observation: One memorandum citing "Multiple Sources" in the "Derived From" portion of the classification authority block did not identify the sources used.

(U) Requirement: When a document is classified derivatively on the basis of more than one source document or security classification guide, the "Derived From" line shall show the phrase "Multiple Sources" and the derivative classifier shall include a listing of the source materials either on, or attached to, each derivatively classified document (TD P 15-71, Chapter III, Section 6.4.c).

(U) Corrective Action: On-the-spot training regarding the use of "Multiple Sources" was provided by (b)(6) to the employee.

8. (U) Observation: One email marked "Confidential" was underclassified; the email was used as a transmittal document for a "Secret" level attachment.

(U) Requirement: A transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is classified, the document shall be marked "Upon Removal of Attachment this Document is Classified (fill in appropriate level) (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training regarding the use of transmittal documents for classified attachments was provided by (b)(6) to the employee.

(U) OFAC is required to report to OSP within 45 days of this memorandum that all corrective actions for each security observation identified above and not corrected on-the-spot have been completed. OFAC is to provide a formal memorandum to OSP with actions taken in order to close out all security findings.

(U) If you have any questions regarding this memorandum, please contact (b)(6), Information Security Specialist, at (b)(6) or email (b)(6)@treasury.gov.

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Thomas J. Wolverton** (b)(6)
Deputy Assistant Secretary for Security and Counterintelligence

FROM: (b)(6)
Director, Office of Security Programs

SUBJECT: **(U) Office of Security Programs Self-Inspection for 4th Quarter FY 2019**

I. (U) INTRODUCTION

(U) During the 4th Quarter of Fiscal Year (FY) 2019, the Office of Security Programs (OSP) conducted a self-inspection during regular working hours to review, evaluate and assess Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order (EO) 13526 and the Treasury Security Manual (TD P 15-71), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter was the Office of Terrorist Financing and Financial Crimes (TFFC). The inspectors were (b) (6), Information Security Specialist, and (b) (6) (b) (6) Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. (U) INSPECTION RESULTS

~~(CUI)~~ On September 26 and 27, 2019 OSP inspected the workspaces of TFFC located in the Main Treasury Building. OSP conducted an inspection of rooms (b) (7)(E) (b) (7)(E); interviewed eight employees cleared for access to national security information; inspected seven Treasury Secure Data Network (TSDN) workstations; and four security containers (b) (7)(E) in order to evaluate and ensure compliance with information security policy and procedures. All security containers held classified documents that appeared to be over nine years old. These documents should be reviewed to determine their continued need for retention. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter

~~CONTROLLED~~

III, Section 16, Destruction of Classified and Sensitive Information. The assessed areas of Classification Management and Equipment met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking as detailed below.

A. (U) Safeguarding

1. (U) Observation: The SF 700 Security Container Information form was not properly updated and the combination changed for the security container (b) (7)(E)

(U) Requirement: The SF 700 shall be completed in its entirety to reflect the name, address, and telephone number of DO/bureau employees responsible for its classified contents. Combinations on in-service equipment shall be changed whenever a person knowing the combination no longer requires access to it or at least every three years, unless conditions dictate sooner (TD P 15-71, Chapter III, Section 3.4 and Chapter V, Section 4.3).

(U) Corrective Action: Coordinate with the Office of Security Programs, Physical Security Branch to have the security container combinations changed and a new SF 700 prepared. Request for this service may be submitted to wdf@treasury.gov.

2. (U) Observation: The SF 702 Security Container Check Sheets for safes (b) (7)(E) are not being properly annotated. During the on-sight OSP self-inspection an employee failed to annotate the opening of their safe (b) (7)(E).

(U) Requirement: When an authorized person first opens the container on a given day, he or she shall record the date, the actual time, and his or her initials on the SF 702. When the container is finally locked at the close of business, the same person or another cleared employee shall record the actual time and their own initials. On normal business days, regardless of whether the equipment was opened or not, the security container shall be checked by its primary or alternate custodians who have access to the equipment to ensure no surreptitious attempt has been made to penetrate the security equipment (TD P 15-71, Chapter III, Sections 3.6b and c).

(U) Corrective Action: Ensure the SF 702 is complete per the requirement. While the "checked by" column is not required to be annotated, OSP recommends as a best security practice that this column be used to document that the safe was checked on normal business days regardless of whether the equipment was opened or not.

3. (U) Observation: During the review of the security (b) (7)(E) on September 26, 2019 in (b) (7)(E) a sensitive compartmented information (SCI) document (b)(1) (b)(1) was found stored in the safe. (b) (7)(E) is not a Sensitive Compartment Information Facility (SCIF). The Office of Special Security Programs (SSP) was immediately notified and retrieved the SCI document from the OSP inspectors. (Note: (b)(6) (b) (6) are cleared up to and including the level of information found.)

(U) Requirement: All SCI must be processed, stored, used, or discussed in an accredited SCIF (Intelligence Community Directive (ICD) 703, Section E, paragraph 3b; and ICD 705, Section D, paragraph 1).

(U) Corrective Action: SSP will conduct a preliminary inquiry into the circumstances surrounding the storage of SCI material in a space not accredited for the storage of SCI material.

B. (U) Performance Evaluations

(U) Observation: Of the eight employees interviewed, no performance work plans were available for review. These employees stated that to the best of their recollection, their performance evaluations last year did not contain the required critical performance element for security. Of these employees, all performed duties likely requiring this performance element as they accessed TSDN, created and sent classified emails, and reviewed or prepared classified documents.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all TFFC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. (U) Classification and Marking

1. (U) Observation: Seven documents, one PowerPoint presentation, and five e-mails missing the classification authority block (this includes the required elements: "Classified By:", "Derived From:", and "Declassify On:").

(U) Requirement: Identifying the Derivative Classifier, Source(s), and Declassification Date/Event: Derivative classifiers shall carry forward instructions on the "Declassify on" line from the source document to the derivative document, or the declassification instruction from an approved security classification guide. When a document is classified derivatively on the basis of more than one source or more than one element from a classification guide, the "Declassify on" line shall reflect the longest duration of any of its sources (TD P 15-71, Chapter III, Section 6.4).

(U) Corrective Action: On-the-spot training on the required markings was provided by (b) (6) to the employees.

2. (U) Observation: Two emails marked as "Secret" were overclassified. These emails

were unclassified replies to emails used as transmittal documents for "Secret" level attachments, and the attachments were not appended to the replies; in all instances the information contained in the text of the emails was unclassified.

(U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

(U) Corrective Action: On-the-spot training on the proper marking of unclassified emails was provided by (b) (6) to the employees.

3. (U) Observation: Two classified emails, one classified memorandum, and one PowerPoint presentations did not identify the derivative classifier by name and position title; rather, only the employee's initials or first initial and last name were used.

(U) Requirement: DO/bureau documents are required to identify the derivative classifier by first and last name and position or by personal identifier, in a manner that is immediately apparent on each derivatively classified document on the "Classified By" line (TD P 15-71, Chapter III, Section 6.4a).

(U) Corrective Action: On-the-spot training regarding the "Classified By" line was provided by (b) (6) and (b) (6) to the employees.

4. (U) Observation: Three classified memorandum and one PowerPoint presentation were missing portion markings.

(U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2a(4) and 6.6a).

(U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) and (b) (6) to the employees.

5. (U) Observation: One classified memorandum was missing a banner line.

(U) Requirement: The overall marking is determined by the highest classification level of any one portion within the document. The highest overall level shall appear at the top and

bottom of the front/back covers (if any), on the title page (if any) and the first page of each classified document. This marking shall be clearly distinguished from the written text (TD P 15-71, Chapter III, Section 6.2a(1)).

(U) Corrective Action: On-the-spot training regarding the proper application of banner line markings was provided by (b) (6) and (b) (6) to the employees.

6. (U) Observation: One classified memorandum was missing the date of origin.

(U) Requirement: The date of origin of the document shall be indicated in a manner that is immediately apparent (TD P 15-71, Chapter III, Section 6.2b).

(U) Corrective Action: On-the-spot training regarding the proper application of required markings was provided by (b) (6) and (b) (6) to the employees.

7. (U) Observation: One classified working paper was missing two of the three required marking elements – date of origin and banner lines.

(U) Requirement: A working paper is any document or material (regardless of media) expected to be revised as a finished product retention or dissemination. Working papers containing classified information shall be dated when created, marked with the highest level of classified information it contains and include portion/paragraph, subject line markings to indicate those sections that are classified (the level thereof) and those parts which are unclassified, and declassification instructions (TD P 15-71, Chapter III, Section 27).

(U) Corrective Action: On-the-spot training regarding the proper application of required markings was provided by (b) (6) and (b) (6) to the employees.

III. (U) SUMMARY OF OBSERVATIONS

A. (U) Classification Management. Within the DO inspected, eight assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information.

B. (U) Performance Evaluations. Of the employees interviewed, none of their performance work plans contained the required critical performance element for security. Of these, every employee interviewed likely occupies a position requiring the critical performance element for security.

C. (U) Classification and Marking. 17 classified documents consisting of seven emails, nine memorandums, and one PowerPoint presentation were reviewed. Of those documents assessed, a majority of these did not properly identify the derivative classifiers by full name and were missing the title of the classifier, source information, and declassification instructions. Failure to mark properly classified documents makes it difficult for document owners and recipients to

identify readily the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	17
Number of documents with discrepancies	17
Percentage of documents with discrepancies	100
Total number of discrepancies	27
Average number of discrepancies per document	1.59

~~CONTROLLED~~

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

MEMORANDUM FOR: **Thomas J. Wolverton**
Deputy Assistant Secretary for Security and Counterintelligence

FROM: (b) (6)
Director, Office of Security Programs (Acting)

SUBJECT: **(U) Office of Security Programs Self-Inspection for 1st Quarter Fiscal Year 2020**

I. (U) INTRODUCTION

(U) During the 1st quarter of Fiscal Year (FY) 2020, the Office of Security Programs (OSP) conducted a self-inspection during regular working hours to review, evaluate and assess Departmental Offices' (DO) collateral classification activities and assess employees' compliance with information security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections are conducted to ensure that Treasury organizations meet the minimum standards for safeguarding collateral classified information. OSP's self-inspections are conducted in accordance with Executive Order 13526 and TD P 15-71 (the Treasury Security Manual), Chapter III, Section 21, "Self-Inspection Program for Classified Information."

(U) The DO inspected this quarter was the Office of Foreign Assets Control (OFAC). The inspectors were (b) (6), Information Security Specialist, and (b) (6), Security Specialist. The OSP Self-Inspection Program Checklist was used with the following areas being assessed: Classification Management, Equipment, Safeguarding, Transmission and Transportation, Performance Evaluations, and Classification and Marking.

II. (U) INSPECTION RESULTS

~~(CUI)~~ From December 30, 2019 to January 22, 2020 OSP inspected the workspaces of OFAC located in the Freedman's Bank Building (the Treasury Annex). OSP conducted an inspection of (B)(7)(e) interviewed 10 employees cleared for access to classified national security information; inspected four Treasury Secure Data Network (TSDN) workstations; evaluated 31 documents (both electronic and in hard copy), of which 6 were free of any errors; and one GSA-approved security container (76370) in order to evaluate and ensure compliance with information security policy and procedures. The security containers held two classified documents (working papers) that were over 180 days old. These documents should be reviewed to determine their continued need for retention. If retention is required, these documents must be

marked as final documents, in accordance with 32 CFR 2001.22 and TD P 15-71, Chapter III, Section 6.10. Classified documents no longer needed should be destroyed in accordance with the standards outlined in TD P 15-71, Chapter III, Section 16, Destruction of Classified and Sensitive Information. The assessed areas of Classification Management and Equipment met the standards outlined in the Treasury Security Manual (TD P 15-71). Discrepancies were observed in the assessed areas of Safeguarding, Performance Evaluations, and Classification and Marking as detailed below.

(U) During the inspection it was noted that two GSA-approved security containers (safe) – a (B)(7)(e) located in the vacant cube (b) (7)(E) and a (B)(7)(e) (b) (7)(E) located in vacant cube (b) (7)(E) – did not have an SF 702. Additionally, a third safe, a (B)(7)(e) located adjacent to cube (b) (7)(E), had a SF 702 dated 2011 (Oct-Dec). Finally, safe (b) (7)(E) located in vacant cube (b) (7)(E) had a potted plant and a number of file folders on top of it.

A. (U) Safeguarding

1. **(U) Observation:** A printer – HP Color LaserJet (B)(7)(e) (B)(7)(e) – located in a common area space adjacent to third floor (b) (7)(E) is connected to the TSDN. The area in which the printer is located does not meet 32 CFR 2001.43(b)(2) (requirements for physical protection) and 2001.53 (open storage area construction) requirements.

   (U) Requirement: Secret information shall be stored in the same manner as Top Secret information. Except for storage in a GSA-approved container or a vault built to FED STD 832, one of the following supplemental controls is required: (i) Inspection of the container or open storage area every four hours by an employee cleared at least to the Secret level; or (ii) An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation (TD P 15-71, Chapter V, Section 2.4b).

   (U) Corrective Action: Coordinate with the TSDN Program Manager to have the printer immediately removed.

2. **(U) Observation:** A Top Secret document was stored in a GSA-approved security container in an area not meeting 32 CFR 2001.43(b)(1) requirements.

   (U) Requirement: Top Secret information shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53. In addition, supplemental controls are required as follows: (1) In a GSA-approved security container with one of the following supplemental controls: Secret-level cleared guard/duty personnel shall inspect the security container once every two hours; An Intrusion Detection System (IDS) with responders arriving within 15 minutes of the alarm annunciation; (3) Security-in-depth when the GSA-approved security container is equipped with a lock meeting Federal Specification FF-L-2740; or (2) In either of the following: An open storage area (secure

room) or vault which is equipped with an IDS with responders arriving within 15 minutes of the alarm annunciation if the area is covered by security-in-depth or a five-minute alarm response if it is not (TD P 15-71, Chapter V, Section 2.4a(1)).

(U) Corrective Action: Store all classified Top Secret material in a GSA-approved security container located in a room meeting 32 CFR 2001.43 storage requirements and 2001.53 construction standards.

B. **(U) Performance Evaluations**

(U) Observation: Four of the 10 employees interviewed were able to access their performance plans. None of those employees could show where the requirement was written into their performance plan. Of the remaining six employees, to the best of their recollection, none believed the requirement was part of their last performance evaluation. Of these employees, all performed duties likely requiring this performance element as they accessed TSDN, created and sent classified emails, and/or reviewed or prepared classified documents.

(U) Requirement: Employees cleared for access to classified information whose duties involve significant creation, generation, or handling/processing of classified information shall have a critical element for security in their individual performance evaluations (TD P 15-71, Chapter III, Section 22).

(U) Corrective Action: Ensure all OFAC employees occupying positions designated in TD P 15-71, Chapter III, Section 22, have a critical element for security in their performance evaluation records.

C. **(U) Classification and Marking**

1. **(U) Observation:** 12 documents missing the classification authority block (this includes the required elements: "Classified By:", "Derived From:", and "Declassify On:").

   (U) Requirement: All classified documents must show the information identifying the derivative classifier, source(s), and declassification date/event (TD P 15-71, Chapter III, Section 6.4).

   (U) Corrective Action: On-the-spot training on the required markings was provided by (b) (6) and (b) (6) to the employees.

2. **(U) Observation:** One document was missing the required information of the "Classified By:" line and one e-mail identified the derivative classified by first initial and last name only.

   (U) Requirement: DO/bureau documents are required to identify the derivative classifier by name and position, or by personal identifier, in a manner that is immediately

apparent on each derivatively classified document on the "Classified by" line (TD P 15-71, Chapter III, Section 6.4a).
(U) Corrective Action: On-the-spot training on the required markings was provided by (b) (6) and (b) (6) to the employees.

3. **(U) Observation:** Two emails marked as "Secret" were overclassified. One e-mail was an unclassified response to a classified e-mail; the second e-mail was an unclassified reply which was supposed to have a (b)(1) attachment which was missing from the e-mail.

   (U) Requirement: Information shall not be classified unless it has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure (TD P 15-71 Chapter III, Sections 5.4 and 5.6). Emails used as a transmittal document shall indicate the highest level of classified information it transmits on its first and last page. Where the transmittal document itself is unclassified, the document shall be marked "Unclassified When Classified Attachment is Detached" (TD P 15-71, Chapter III, Section 5.24).

   (U) Corrective Action: On-the-spot training on the proper marking of unclassified an email was provided by (b) (6) and (b) (6) to the employees.

4. **(U) Observation:** Six classified documents and 11 e-mails were missing portion markings.

   (U) Requirement: Each portion of a document, ordinarily a paragraph, but including subject, titles, graphics, tables, charts, bullet statements, subparagraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which are unclassified. Markings on classified information in cables, message traffic, and maintained in electronic format such as e-mail, shall conform to the same requirements as for hard-copy documents (TD P 15-71, Chapter III, Section 6.2a(4) and 6.6a).

   (U) Corrective Action: On-the-spot training regarding the proper application of portion markings was provided by (b) (6) and (b) (6) to the employees.

5. **(U) Observation:** Two e-mails were incorrectly marked with the dissemination control "NOFORN." Neither e-mail contained material portion marked as "NF."

   (U) Requirement: The banner line shall specify the highest level of classification of information contained within the document and the most restrictive control markings applicable to the overall document (TD P 15-71, Chapter III, Section 6.2a(1)).

   (U) Corrective Action: On-the-spot training regarding the proper application of banner line markings was provided by (b) (6) and (b) (6) to the employees.

6. **(U) Observation:** Two classified working papers exceeded the 180-day time limit and were marked in the same manner prescribed for a finished document at the same classification level.

   (U) Requirement: A working paper is any document or material (regardless of media) expected to be revised as a finished product retention or dissemination. Working papers containing classified information shall be dated when created, marked with the highest level of classified information it contains and include portion/paragraph, subject line markings to indicate those sections that are classified (the level thereof) and those parts which are unclassified, and declassification instructions (TD P 15-71, Chapter III, Section 27).

   (U) Corrective Action: On-the-spot training regarding the proper application of required markings was provided by (b) (6) and (b) (6) to the employees.

III. (U) SUMMARY OF OBSERVATIONS

A. **(U) Classification Management.** Within the DO inspected, 10 assigned individuals cleared for access to classified information were interviewed. All personnel interviewed demonstrated a fundamental level of awareness regarding their responsibilities to properly handle, store, transmit, and derivatively classify national security information.

B. **(U) Performance Evaluations.** Of the employees interviewed, none of their performance work plans contained the required critical performance element for security. Of these, every employee interviewed likely occupies a position requiring the critical performance element for security.

C. **(U) Classification and Marking.** 31 classified documents consisting of 15 emails and 16 documents were reviewed. Of those documents assessed, a majority of these did not contain all of the required markings for a classified document, specifically, portion markings, derivative classifier by name or personal identifier, source information, and declassification instructions. Failure to mark properly classified documents makes it difficult for document owners and recipients to identify readily the proper document safeguarding, handling and transmission requirements, increasing the risk of either a data spillage or inadvertent disclosure of classified information.

Classified Document Review Totals	
Total number of documents reviewed	31
Number of documents with discrepancies	25
Percentage of documents with discrepancies	81%
Total number of discrepancies	37
Average number of discrepancies per document	1.48