Description of document:	Department of the Treasury Office of Security Programs (OSP) Quarterly Self Inspection Reports, 2013-2016
Requested date:	19-February-2017
Release date:	08-March-2021
Posted date:	21-February-2022
Source of document:	FOIA Request Department of the Treasury 1500 Pennsylvania Ave. NW Washington D.C. 20220 Submit a FOIA Request Online Email: FOIA@treasury.gov FOIAonline

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

3/8/2021

RE: Your FOIA Request to Treasury, Case Number 2017-02-218

This is the Department of the Treasury's (Treasury) final response to your Freedom of Information Act (FOIA) request submitted on February 19, 2017. You requested:

"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 2013, 2014, 2015 and 2016."

Your request has been processed under the provisions of the FOIA, 5 U.S.C. § 552. Treasury Departmental Offices conducted a search and located 40 pages. After reviewing the information, 40 pages are partially withheld pursuant to Exemptions 5, 6, 7C and 7E.

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

5 U.S.C. § 552(b)(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."

5 U.S.C. § 552(b)(6) exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

5 U.S.C. § 552(b)(7)(C) exempts from disclosure "personal information in law enforcement records."

5 U.S.C. § 552(b)(7)(E) exempts from disclosure "techniques and procedures for law enforcement investigations or prosecutions."

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.

If any questions arise, you may contact Kristen Kontinopoulos at 202-622-1143 or email Kristen.Kontinopoulos@treasury.gov. Please reference FOIA case number 2017-02-218 when contacting our office about this request

Sincerely,

Jacqueline J. Scott
Digitally signed by Jacqueline J. Scott
Date: 2021.03.08 14:53:46 -05'00'
FOIA and Transparency
Office of Privacy, Transparency, and Records

Enclosure:
Responsive Document (40 Pages)

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 15, 2013

MEMORANDUM FOR: **CHARLES J. CAVELLA, Jr.**
DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs
(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**

Office of Security Programs 3rd Quarter Self Inspections

During the 3rd quarter of FY13, the Office of Security Programs (OSP) conducted non-working hours self-inspections to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. These were conducted in compliance 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 involves 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 June 24, 2013, a non-working hours inspection was conducted of the [redacted] Floor of the Main Treasury Building. The majority of the [redacted] work spaces inspected belonged to the Office of (b) (7)(A), (b) (7)(E) while the remainder belonged to the following entities: (b) (7)(E) [redacted]

There were a total of (b) (7)(E) terminals. A total of two security violations were discovered in (b) (7)(E) and (b) (7)(E) . In (b) (7)(E), an (b) (7)(E) The (b) (7)(E) at the OSP and returned to its owner along with a security violation form (TD F 15-05.6). (b) (7)(E) The OSP inspection team was advised who the (b) (7)(E) at the OSP. They were

subsequently returned to the (b) (7)(E) along with a security violation form. No other security violations or infractions were noted.

OSP reviewed 121 (b) (7)(E) emails and, where present, the accompanying classified attachment(s). Emails with attached classified text dated after April 13, 2013 included the correct date of Treasury's Security Classification Guide, i.e., March 2, 2012. Classified email attachments before April 13, 2013 show the old date of the guide.

Declassification instructions did not appear on classified documents included as attachments; these instructions appear on the accompanying transmittal emails. Additionally employees are not portion marking emails where the message text appears to be unclassified but still bears an overall marking subject and page classification of Secret or Secret//NOFORN. Where portion marking does appear is only on the actually classified text.

Office of Special Security 1st Quarter Self Inspections (b) (5)

Third quarter inspections included the (b) (7)(E) (b) (7)(E) Suite (b) (7)(E), and Suite (b) (7)(E) Main Treasury (b) (7)(E) with (b) (7)(E) workstations and [redacted] offices with [redacted] workstations were inspected by SSP Facility Security Officer. A total of 2 security infractions were found, of which all were corrected on-site. The infractions found were (b) (7)(E). No infractions resulted in the disclosure of classified information. All findings will be included and emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 23, 2013

MEMORANDUM FOR: **MICHAEL W. MASON, ACTING (b) (6), (b) (7)(C)**
DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Director, Office Security Programs

(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**

Office of Security Programs 4th Quarter Self Inspections

During the 4th quarter of FY13, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 involves 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 September 24, 2013, OSP's non-working-hours self-inspection was conducted of the (b) (7)(E) of the Main Treasury Building. The majority of the (b) (7)(E) work spaces inspected belonged (b) (7)(E) while the remainder belonged to the following entities: (b) (7)(E) (b) (7)(E)

There were a total of (b) (7)(E) and (b) (7)(E) terminals in work spaces subject to examination during the self-inspection. No securi were observed. However, a barlock cabinet was discovered in the (b) (7)(E) that will have to be replaced and action has been taken to ensure this. Barlock cabinets, as of October 1, 2012, are no longer authorized for use in storing classified information. In addition, a (b) (7)(E) (b) (7)(E) This information was brought to the attention of the two OCIO personnel who by their request had accompanied us during the inspection to observe

the process. The OCIO personnel did not express interest in (b) (7)(E) but were asked and responded to our questions on identifying DO-issued thumb drives. We followed up with OCIO senior management the following day to report the finding and location of the (b) (7)(E) (b) (7)(E) We also contacted Facilities Management concerning a work space (b) (7)(E) that appeared to be a possible fire/safety hazard due to extensive piles of loose newspapers and boxed material the employee has accumulated and forming narrowly navigated "path" through the cubicle.

OSP did not review any (b) (7)(E) classified information documentation this quarter. We had requested OCIO to provide select (b) (7)(E) classified email and accompanying classified attachments (if any) but they were unable to meet our normal deadline. With the subsequent Government shutdown, we did not wish to further delay this report. We have since reengaged with OCIO (since they discontinued services of the contractor we had previously worked with and knew our requirements) to continue to obtain the (b) (7)(E) classified data for our analyses. We expect to have particulars re-established in time for completion of the first quarter FY 2014 report.

Office of Special Security 4th Quarter Self Inspections

The fourth quarter SSP inspections included the [redacted] Floor Treasury Annex, Suite [redacted], Suite [redacted], and Suite [redacted] of Main Treasury which were inspected over a three day period by a SSP Facility Security Officer. Inspections covered [redacted] workstations, a conference room, communications closet, and multiple offices. A total of 55 findings were noted of which all were corrected on-site. The findings were [redacted] (b) (7)(E) (b) (7)(E) No security findings resulted in the disclosure of classified information. All findings were identified to affected members and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 13, 2014

MEMORANDUM FOR: **MICHAEL W. MASON, ACTING DEPUTY ASSISTANT SECRETARY FOR SECURITY**

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs

(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**

Office of Security Programs 1st Quarter FY 2014 Self Inspections

During the 1st quarter of FY14, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 involves 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 November 5, 2013, OSP's non-working-hours self-inspection was conducted of the (b) (7)(E) of the Main Treasury Building. The majority of the (b) (7)(E) work spaces inspected belonged to the (b) (7)(E) while the remainder belonged to the following entities: (b) (7)(E)

There were a total of (b) (7)(E) terminals in work spaces subject to examination during the self-inspection. One security violation was discovered in (b) (7)(E) in the (b) (7)(E) A security container containing Secret//NF was discovered unsecured. Although the general office was occupied, the work space with the unlocked security container was unoccupied and accessible. A security violation was processed

and the container containing the classified documents was secured. The possibility of compromise is remote to non-existent. (b) (7)(E) [redacted] No other security violations or infractions were observed.

On December 18, 2013, a non-working hours self-inspection was conducted of the [redacted] (b) (7)(E) [redacted] of the (b) (7)(E) [redacted] The approximately [redacted] work spaces belong to the (b) (7)(E) [redacted] None of the work spaces contained (b) (7)(E) [redacted] or (b) (7)(E) terminals. One of the unlocked offices (b) (7)(E) [redacted] A security violation was written and sent to the subject and (b) (7)(E) [redacted] No other security violations or infractions were observed.

OSP examined 452 electronically processed classified emails prepared by selected (b) (7)(E) [redacted] employees. Less than 11% contained required paragraph/portion markings mandated by Executive Order 13526 and 32 CFR Part 2001. Only four employees consistently included portion markings in their various email messages; another employee did so about 50% of the time.

In all instances, users had the correct date (March 2, 2012) when citing Treasury's Security Classification Guide as the derivative classification source. However, users routinely cited 25 years as the declassification date instead of a lesser amount of time; no one cited an identifiable event for declassification. Section 3 of the Terrorism and Financial Intelligence section of Treasury's Security Classification Guide contains 64 item descriptions for derivative classification. Of these, 50 item descriptions identify 10 years as the prescribed time frame for declassification. The remaining 14 require consultation with OIA when citing paragraph 1.4(c), EO 13526 as rationale for classification. This suggests rote application of the 25 year default option by the first person sending the email and subsequent recipients following suit. Users are unable to downgrade to a lower classification but they do have the ability to change the declassification instructions to select a lesser, e.g., 10 year or earlier time frame for declassification as warranted.

Several users continue to rely on lengthy email strings transmitting clearly unclassified information. Additionally, we found such unclassified information such as "?", "yep" and "urggh" or "looping in someone else" on emails when these only contained subject lines labeled Secret//NF. This suggests a lack of attention to properly marking paragraphs/portions on classified email documentation. This may also be complicated by non-Treasury agencies not applying proper paragraph/portion markings and Treasury recipients not challenging the incomplete markings they forward emails internally and/or respond externally.

Office of Special Security 1st Quarter Self Inspections

The first quarter SSP inspections included the [redacted] floor Treasury Annex, Suite [redacted], Suite [redacted], and Suite [redacted] of Main Treasury which were inspected over a three day period by a SSP Facility Security Officer. Inspections covered [redacted] workstations, a conference room, communications closet, and multiple offices. A total of 55 findings were noted of which all were corrected on-site. The findings were (b) (7)(E) [redacted] No security findings resulted in the disclosure of classified information. All findings were identified to affected members and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

April 15, 2014

MEMORANDUM FOR: MICHAEL W. MASON, ACTING
DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs

(b) (6), (b) (7)(C)
Acting Director, Office of Special Security Programs

SUBJECT: After-hours Security Inspections

Office of Security Programs 2nd Quarter FY 2014 Self Inspections

During the 2nd quarter of FY14, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 involves 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 February 25, 2014, OSP's self-inspection was conducted of the (b) (7)(E) The approximately (b) (7)(E) work spaces inspected belonged to the (b) (7)(E) The 4-person OSP team included (b) (6), (b) (7)(C) to develop the skill-set needed to regularly participate in self-inspections along with (b) (6), (b) (7)(C).

There are a total of (b) (7)(E) on the (b) (7)(E) These are located in a secured room and could not be inspected. Two (2) security violations were discovered in Rooms (b) (7)(E) and (b) (7)(E). (b) (7)(E) Two (2) security violations were processed. (b) (7)(E) No other security violations or infractions were observed.

OSP selected (b) (7)(E) user accounts at random belonging to employees in the (b) (7)(E) for review. Two of the (b)(7)(E) account holders had no activity for the time frame covering the reviewed material. We subsequently examined 1005 Treasury-generated and electronically processed classified emails/documents (and 77 classified attachments). Other agencies classified email/documents and attachments were excluded in the review process. Thirteen (13) individual emails had all the required markings mandated by EO 13526 and 32 CFR Part 2001. The remaining 992 emails did not have all the required portion markings and often omitted marking the unclassified portions.

There were far fewer lengthy classified email strings observed than in prior self-inspections. Lengthy strings were cited in earlier reviews and had resulted in OSP issuing a training piece to encourage users to "cut the cord" and be brief. Users however, continue to send classified emails with obviously unclassified (and unmarked portions) in soliciting further details for their use, venting, or in thanking senders of requested items.

For the above 77 attachments, five (5) were fully compliant with required classification markings. The remaining 72 largely excluded required declassification instructions, i.e. "Classified by, Derived from and Declassification date/event" line markings. Where the declassification instructions did appear, several did not identify the date of Treasury's Classification Guide (March 2, 2012) or referred to 1.4(d) and (e). The latter is the marking for original classified documents on the "Reason" line which does not apply on derivatively classified information; all Treasury email/documents subject to this review were derivatively classified. Some classified documents included as attachments cited the previous E.O. 12958 in what appeared to be an outdated template for preparing classified information.

Incoming classified emails/documents did not always contain the required markings under E.O. 13526 and (b) (7)(E) user's appeared to follow the incorrect markings in responding or sharing such material with colleagues. However, users did not always properly mark their email/documents when the other agencies correctly marked their own material.

All classified email/documents were reviewed in electronic format instead of hard copy. This allowed OSP to email individual derivative classifiers about their particular items and cite direct examples where markings were absent. We advised users to discontinue the "1.4(d) and (e)" and "12958" citations and to cite the March 2, 2012 date of the current Classification Guide. For the latter we alerted them that an updated Guide is coming in the near term (April or early May 2014). (b) (7)(E) account holders overwhelmingly responded positively to the OSP's email "training" we provided and in realizing the importance of not omitting portion markings or were now much better attuned to the marking requirement.

OSP has already approached the (b) (7)(E) to request access to the (b) (7)(E) to allow review of classified documents generated by both components in lieu of classified email. The next two quarters are expected to include such material for review once we obtain approval for such access. Future reports of reviewed classified documents will keep statistics on the volume of omitted portion markings, incomplete

markings, absent overall markings, missing declassification instructions and inappropriate markings.

Office of Special Security Programs 2nd Quarter Self Inspections

The second quarter FY14 inspections conducted by the Office of Special Security Programs encompassed rooms (b) (7)(E) in the Main Treasury Building. Inspections covered (b) (7)(E). A total of 17 findings were noted. No security finding resulted in the disclosure of classified information. All findings were identified to members and will be emphasized during annual training. The actual findings involved:

1. (b) (7)(E)

2. (b) (7)(E) An investigation was conducted and determined there was no compromise of classified information.

3. (b) (7)(E) and area employees so notified.

4. (b) (7)(E) and this was corrected on the spot.

5. (b) (7)(E) and rectified onsite.

6. (b) (7)(E) and corrected on the spot.

7. (b) (7)(E) Individuals were so notified and counseled as to appropriate procedures.

July 10, 2014

MEMORANDUM FOR: CHARLES J. CAVELLA, Jr.
DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Acting Director, Office of Security Programs

SUBJECT: After-hours Security Inspections

Office of Security Programs 3rd Quarter FY 2014 Self Inspections

During the 3rd quarter of FY14, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 involves 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 May 14, 2014, OSP's non-working-hours self-inspection was conducted of floors (b) (7)(E) The approximately (b) (7)(E) inspected work spaces belong to the (b) (7)(E) and (b) (7)(E) The 4-person OSP team included (b) (6), (b) (7)(C) again to develop the skill-set needed to regularly participate in self-inspections along with (b) (6), (b) (7)(C) . (b) (7)(E)

Two (2) security violations were discovered in (b) (7)(E) . (b) (7)(E) The 2 security violations were processed; no other security violations or infractions were observed.

In addition to the (b) (7)(E) , we observed another (b) (7)(E) user's documents in his work space that were inappropriately using the marking "Controlled Unclassified Information" (CUI). These appeared to be official (b) (7)(E) reports, i.e., Reporting Policy Procedure, Monthly

Report to Congress and Emergency Response and Continuity of Operations Plan and Procedure. The user was advised via email that use of the CUI marking has NOT yet been approved.

Executive branch employees and contractors supporting government agencies have all been instructed to follow their existing "Sensitive But Unclassified" (SBU) schema until otherwise directed through guidance by the CUI Executive Agency (EA). We confirmed the prohibition with the EA the next day and so notified the affected individual. He was provided the on-line CUI fact sheet link to disseminate the restriction guidance among (b) (7)(E) colleagues. Approval for the Executive Branch to use of CUI for marking such information is not anticipated until calendar year 2015.

OSP requested a sampling of 100 documents created by (b) (7)(E) on the (b) (7)(E) and examined them in electronic form. The random sampling also collected a few (b) (7)(E) generated items. The documents were made available on June 19th and reviewed on June 23rd. Out of the random 100, 37 fit OSP's criteria for review, i.e., involving mandatory classification/control markings under Executive Order 13526. A statistical breakdown and analysis follows:

> 24 were marked Secret//NOFORN; 5 were marked Secret; 2 were marked Confidential//NOFORN; 2 were marked Confidential and 4 were marked Unclassified (the latter 4 were all properly marked).
>
> 15 contained all required classification markings.
>
> 36 showed the overall classification/page markings except for one that was missing this on the top of every page (in an apparent header error).
>
> 29 had required markings on the classified and unclassified paragraphs/portions.
>
> 21 were missing required declassification instructions, i.e., Classified by, Derived from, and Declassify on markings.
>
> 3 documents were sent along to (b) (7)(E) about incomplete aspects, i.e., Classified by line indicating "Treasury" in lieu of the name or alpha-numeric identifier and missing declassification instructions. 1 was forwarded to (b) (7)(A), (b) for a determination on whether it is a Treasury or other agency document; OSP was told its Treasury's; it only contains the overall marking.

By comparison with previous reviews of classified email (and including small numbers of classified attachments), users seem to be doing a better job of paragraph/portion marking on draft/final classified documents but not attending to the required declassification instructions.

Office of Special Security Programs 3rd Quarter Self Inspections

The third quarter FY14 inspections conducted by the Office of Special Security Programs encompassed (b) (7)(E) of Main Treasury and (b) (7)(E) SSP facility

security officers inspected [redacted] workstations, [redacted] Two minor findings were noted, of which all were corrected on-site. [redacted] No security finding resulted in the disclosure of classified information. However, all findings were identified to members and will be emphasized during annual training.

September 4, 2014

MEMORANDUM FOR: **CHARLES J. CAVELLA, Jr.**
DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Acting Director, Office of Security Programs

(b) (6), (b) (7)(C)
Acting Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**

Office of Security Programs 4th Quarter FY 2014 Self Inspections

During the 4th quarter of FY14, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 July 31, 2014, OSP's non-working-hours self-inspection was conducted of the (b) (7)(E) The approximately (b) (7)(E) work spaces inspected belonged to the (b) (7)(E) and (b) (7)(E)

There were a total of (b) (7)(E) on the (b) (7)(E) No other security violations or infractions were observed.

In the fourth quarter FY 2014, OSP requested and reviewed a larger sampling of classified documents created by (b) (7)(E) on the (b) (7)(E). We looked at 120 items; 55 were derivatively classified. This represented a 67% increase in the volume of classified items reviewed the previous quarter. These fit OSP's criteria for review, i.e., mandatory classification markings under Executive Order 13526. Another 55 were marked as unclassified. For this quarter 41% of all actual classified documents reviewed were properly marked. Adding appropriately marked unclassified documents the rate increases to 60% (see below).

The classified items included 41 marked Secret//NOFORN, 12 marked Secret, and 2 marked Confidential. Another 3 were classified by either State or Defense and therefore not included as part of the OSP review process. For the classified items, 17 contained all required classification markings. Some had multiple errors as 18 were missing declassification instructions and/or did not identify the derivative classification source(s) or retain a list thereof when relying on multiple sources; one Secret document was only marked at the top of the page (rather than top and bottom); and another document did not mark the subject line. One document added an extra line in the declassification instructions indicating the actual classification date.

Out of the 120 items, 55 were marked Unclassified and/or Unclassified//FOUO and contained required overall and portion markings. Two others were respectively marked Sensitive But Unclassified and Law Enforcement Sensitive. The last 5 items among the overall 55 we examined were unmarked briefing memos and/or distinctly unclassified press release items.

Where the account holder could be identified, we reached out to him/her to provide direct training about marking irregularities and how to correct same. The feedback in that regard was distinctly positive. However, while the overall results show improvement and some positive reinforcement, at least 40% (or more) users still need to apply greater attention to properly marking their classified products to comply with the Executive Order.

Office of Special Security 4th Quarter Self Inspections

The 4th Quarter FY14 inspections encompassed Room (b) (7)(A), (b) (7)(E) of the Main Treasury. Inspections covered [redacted] workstations total, (b) (7)(E). A total of 21 findings were noted. The findings were:

1. (b) (7)(E)
2. (b) (7)(E) (Employees notified)
3. (b) (7)(E)
   (Corrected on the spot.)

4. (b) (7)(E) (Employee notified.)

5. (b) (7)(E) . (Corrected on the spot.)

No security finding resulted in the disclosure of classified information. All findings were identified to members and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 7, 2015

MEMORANDUM FOR: **MICHAEL W. MASON** [redacted]
ACTING DEPUTY ASSISTANT SECRETARY FOR SECURITY

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs
(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 1st Quarter FY 2015 Self Inspections

During the 1st quarter of FY15, the Office of Security Programs (OSP) and the Office of Special Security Programs (SSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 12, 2014, OSP's non-working-hours self-inspection was conducted of the (b) (7)(E) [redacted] The (b) (7)(E) work spaces inspected belonged to (b) (7)(E) and contained (b) (7)(E) . On December 15, 2014, (b) (7)(E) (b) (7)(E) work spaces located on the (b) (7)(E) [redacted] were inspected. These spaces contained (b) (7)(E) [redacted] On December 16, 2014, (b) (7)(E) (b) (7)(E) work spaces located on the (b) (7)(E) [redacted] were inspected. These spaces contained (b) (7)(E) [redacted] No security violations were noted.

In the First Quarter FY 2015, OSP requested and reviewed a sampling of classified documents created by (b) (7)(E) on the (b) (7)(E) . 87 classified/unclassified emails/documents were reviewed this quarter. These fit OSP's criteria for review, i.e., mandatory classification markings under Executive Order 13526. Of these, 29 were marked as unclassified.

The classified items included 57 marked Secret//NOFORN, with one (1) marked Secret. Another three (3) were classified by either State or Defense and therefore not included as part of the OSP review process. For the classified items reviewed, four (4) contained all required classification markings. All 57 (100%) contained proper overall page classification markings However, with the exception of five (5) emails and one (1) document, the majority of emails (51) did not contain paragraph portion marking to enable the reader to determine what part of the email was classified or unclassified. One (1) classified (b) (7)(E) attachment/document that was reviewed contained all the proper markings, but did not contain the classification authority block or declassification instructions.

We reached out to two (2) account holders, and attempted to contact a third, to provide direct feedback about marking irregularities and how to correct then. In addition, a message was left with (b) (7)(E) Security POC, (b) (7)(C), (b) (6), to communicate our findings and provide constructive feedback to disseminate to (b) (7)(E) personnel to assist them in applying greater attention to properly marking their classified products to comply with the Executive Order.

Office of Special Security Programs 1st Quarter FY 15 Self Inspections

The first quarter FY15 inspections encompassed rooms (b) (7)(E) of Main Treasury. On December 10, 2014, SSP FSOs conducted self-inspection of suite (b) (7)(E) and suite (b) (7)(E) of the Main Treasury building. The (b) (7)(E) offices, (b) (7)(E) workstations, and (b) (7)(E) (b) (7)(E) belonged to the (b) (7)(E) and the (b) (7)(E) offices of (b) (7)(E) and contained (b) (7)(E) terminals, and (b) (7)(E) . A total of six (6) serious infractions were noted in which (b) (7)(E) . A total of six (6) minor findings were noted, of which two (2) were corrected on the spot and four (4) were corrected after email notifications were sent. The findings were (b) (7)(E)

On December 15, and 16, 2014, SSP FSOs conducted self-inspection of suite (b) (7)(E) and suite (b) (7)(E) of the Main Treasury building. The (b) (7)(E) offices, (b) (7)(E) workstations, and (b) (7)(E) conference room belonged to the (b) (7)(E) and contained (b) (7)(E) terminals, and (b) (7)(E) . A total of two (2) serious infractions were noted in which (b) (7)(E) were returned to the Office Director of each person in violation the next business day. A total of nine (9) minor findings were noted, of which four (4) were corrected on the spot and five (5) were corrected after email notifications were sent. The findings were (b) (7)(E)

On December 17, 2014, SSP FSOs conducted self-inspection of suite (b) (7)(E) of the Main Treasury building. The (b) (7)(E) offices, (b) (7)(E) workstations, and (b) (7)(E) (b) (7)(E) belonged to the (b) (7)(E) and contained (b) (7)(E) terminals, and (b) (7)(E). A total of five (5) minor findings were noted, of which three (3) were corrected on the spot and two (2) were corrected after email notifications were sent. The findings were (b) (7)(E)

On December 18, 2014, SSP FSOs conducted self-inspection of suite (b) (7)(E) of the Main Treasury building. The (b) (7)(E) offices and (b) (6) workstations belonged to the (b) (7)(E) and contained (b) (7)(E) terminals, and (b) (7)(E). A total of two (2) serious infractions were noted in which (b) (7)(E) materials were returned to the Office Director of each person in violation the next business day. One (1) minor finding was noted which was corrected on the spot. The finding was (b) (7)(E)

No security finding resulted in the disclosure of classified information. All findings were identified to members and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 14, 2015

MEMORANDUM FOR: **Michael W. Mason** [redacted]
(Acting) Deputy Assistant Secretary for Security

FROM: [redacted]
Director, Office of Security Programs
[redacted]
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 2nd Quarter FY 2015 Self Inspections

During the 2nd quarter of FY15, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 18, 2015, OSP's non-working-hours self-inspection was conducted on the [redacted] Floor Main Treasury Building. The [redacted] workstations inspected belonged to [redacted]. The inspection team checked for [redacted] and reviewed electronic email from a sample of [redacted] account holders. A total of [redacted] were inspected. No security violations were noted.

In the 2nd Quarter FY 2015, OSP requested and reviewed a sampling of classified documents created by [redacted] or contained in their folders on the [redacted] shared-drive. Twenty-seven classified/unclassified electronic emails with and without attachments were reviewed. These fit most of OSP's criteria for review, i.e., mandatory classification markings under Executive Order 13526. Of these, four of the 27 emails were marked as unclassified. Another four were

classified by the Department of State (DOS) and therefore not included as part of the OSP review process.

The classified items included 14 emails marked Secret//NOFORN, one marked Secret, one marked Confidential//NOFORN and three marked Confidential. Of the classified items reviewed, none of them contained all the required classification markings.

Eighteen out of the 19 emails contained proper overall page classification markings, declassification authorities and sources, but did not contain the required paragraph portion classification markings, preventing the reader to determine what part of the email was classified or unclassified. Of the 19 Treasury classified documents reviewed, 16 were originated by the [redacted]; two came from [redacted] employees and one originated from the (b) (7)(E) Office. While reviewing the [redacted] folder samples, we identified a trend of classification marking errors in the emails that had originated from the [redacted].

We reviewed 16 emails originated by the [redacted]. Analysis of those documents revealed that the [redacted] was using classified source documents and not transferring the markings. For example, there would be a classified email from another agency with a classified subject. The [redacted] would create a pdf of the document using the classified subject to name it without marking the pdf document title with the appropriate classification marking. Additionally, the classified subject from the included email was transferred to the (b) (7)(E) cover sheet without marking its classification level appropriately. Lastly, the classified subject was used in the subject of the forwarding email without indicating that the subject itself is classified or unclassified. This is significant because the recipient is not made aware of the classification of all the material received which creates the potential for compromises and/or unauthorized disclosures of classified information.

Of the three remaining classified emails, the two from [redacted] employee and the one from the (b) (7)(E) office involved failures to portion mark paragraphs added to classified documents. In one of the [redacted] emails, the sender failed to mark the appropriate dissemination control marking "NOFORN" to the overall markings.

We contacted the [redacted] Director, (b) (6), (b) (7)(C), and provided direct feedback regarding our findings of the marking irregularities and provided classification marking guidance to correct them. We sent [redacted] classified document marking essentials that appears on the Green for distribution to [redacted] employees to prevent future recurrences. In addition, we contacted three account holders from [redacted] and the (b) (7)(E) Office and provided constructive feedback and the same training.

Office of Special Security Programs (SSP) 2nd Quarter FY 15 Self Inspections

The Second quarter FY15 inspections encompassed rooms (b) (7)(E) [redacted] of the Main Treasury.

On February 24, 2015, SSP FSOs conducted a self-inspection of (b) (7)(E) and (b) (7)(E) of the Main Treasury building. These offices have (b) (7)(E) and (b) (7)(E) occupied by (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). No infractions were noted.

On March 3, 2015, SSP FSOs conducted a self-inspection of (b) (7)(E) of the Main Treasury building. This office has (b) (7)(E) occupied by (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). One serious infraction was noted in which (b) (7)(E) were returned to the Office Director and the employee in violation was briefed on the requirement (b) (7)(E) A total of three minor findings were noted, of which two were corrected on the spot and one was corrected after email notification was sent. The findings were (b) (7)(E)

On March 4, 2015, SSP FSOs conducted a self-inspection of (b) (7)(E) and (b) (7)(E) of the Main Treasury building. These rooms have (b) (7)(E), (b) (7)(E), (b) (7)(E) and (b) (7)(E) occupied by the (b) (7)(E) and (b) (7)(E) with (b) (7)(E) terminals, (b) (7)(E) fax machines, (b) (7)(E) digital senders and (b) (7)(E). A total of eight minor findings were noted, of which seven were corrected on the spot and one was corrected after email notification was sent. (b) (7)(E)

On March 6, 2015, SSP FSOs conducted a self-inspection of room (b) (7)(E) of the Main Treasury building. This room has (b) (7)(E) and (b) (7)(E) occupied by (b) (7)(E) and (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). A total of five serious infractions were noted in which (b) (7)(E) were collected by the FSO and were returned the same day to each employee in violation after they were briefed on the requirement (b) (7)(E) A total of 10 minor findings were noted, of which four were corrected on the spot and six were corrected after email notification was sent. (b) (7)(E)

On March 11, 2015, SSP FSOs conducted a self-inspection of room (b) (7)(E) of the Main Treasury building. This room has (b) (7)(E) and (b) (7)(E) occupied by (b) (7)(A), (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). A total of 10 minor findings were noted, of which seven were corrected on the spot and three were corrected after email notification was sent. (b) (7)(E)

No security finding resulted in the disclosure of classified information. All findings were identified to the offenders and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 23, 2015

MEMORANDUM FOR: **Michael W. Mason** [redacted]
(Acting) Deputy Assistant Secretary for Security

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs
(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 3rd Quarter FY 2015 Self Inspections

During the 3rd quarter of FY15, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 June 18, 2015, OSP's non-working-hours self-inspection was conducted on the (b) (7)(E) Main Treasury Building. The [redacted] workstations inspected belonged to (b) (7)(E) [redacted] Of the [redacted] workstations, (b) (7)(E), and (b) (7)(E) were inspected. One security infraction was discovered and (b) (7)(E) [redacted] It was noted that access by unauthorized persons was not possible as the outer door to the hallway had been secured. (b) (7)(E) [redacted] properly secured by the OSP personnel inspection team. No other security infractions were noted.

In the 3rd Quarter FY 2015, OSP requested and reviewed samplings of classified documents created by [redacted] or were contained in their folders on the (b) (7)(E) [redacted]. Twenty-four classified/unclassified electronic emails and documents were reviewed. These fit most of OSP's criteria for review (i.e. mandatory classification markings under Executive Order 13526). Of these, one item was marked as unclassified.

The classified items reviewed included 20 electronic emails or attachments marked Secret//NOFORN and three marked Confidential. Of the classified items reviewed, two documents were compliant with all the required classification markings. However, these two documents were marked Secret and were included as attachments in emails that did not identify their classification. The documents had been sent within an email that had been classified as Confidential. (b) (6) , was contacted and advised of the error and instructed on the correct procedure. With the exception of this one email, all documents contained the correct overall page markings, classification authorities and declassification instructions. The majority of electronic emails (19) did not contain paragraph portion markings to enable the reader to determine what part of the email was classified or unclassified. Of the 23 classified documents reviewed, 15 were originated by (b) (7)(E); seven were originated from (b) (7)(E) personnel and one originated from the (b) (7)(E) .

Office of Special Security Programs 3rd Quarter FY 15 Self Inspections

The 3rd Quarter FY15 inspection encompassed rooms (b) (7)(E)

On June 10, 2015, SSP FSOs conducted a self-inspection of the (b) (7)(E) . This facility has (b) (7)(E) and (b) (7) cubicles with (b) (7)(E) terminals and (b) (7)(E). Zero security infractions were noted.

On June 22, 2015, SSP FSOs conducted a self-inspection of room (b) (7)(E) at Main Treasury. This (b) (7)(E) is primarily used by (b) (7)(E) and has (b) (7)(E) terminals. Zero security infractions were noted.

On Jun 26, 2015, SSP FSOs conducted a self-inspection of rooms (b) (7)(E) and (b) (7)(E) of Main Treasury. These offices are occupied by the (b) (7)(E) and the (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). Zero security infractions were noted.

On June 26, 2015, SSP FSOs conducted a self-inspection of the (b) (7)(E) This conference room has (b) (7)(E) kiosk positions with (b) (7)(E) terminals. A total of 10 minor security findings were noted. The findings were (b) (7)(E) . The security infractions were corrected during the inspection.

No security finding resulted in the disclosure of classified information. All findings were identified to the members and will be emphasized during annual security refresher training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 23, 2015

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

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs
(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 4th Quarter FY 2015 Self Inspections

During the 4th Quarter of FY15, the Office of Security Programs (OSP) conducted a non-working-hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 August 13, 2015, OSP's non-working-hours self-inspection was conducted on the (b) (7)(E) [redacted] The (b) (7)(E) workstations inspected belonged to (b) (7)(E). Of the (b) (7)(E) [redacted] were inspected. One security infraction was discovered and (b) (7)(E) [redacted] It was noted that access by unauthorized persons was not possible as the outer door to the hallway was secured. (b) (7)(E) [redacted] (b) (6) [redacted] security representative, was contacted regarding (b) (6) [redacted] No other security infractions were noted.

In the 4th Quarter FY 2015, OSP reviewed samplings of classified documents created by Treasury employees with (b) (6) accounts. Thirty-two (32) classified and unclassified electronic emails and documents were reviewed. These fit most of OSP's criteria for review (i.e. mandatory classification markings under Executive Order 13526). The classified items reviewed included 16 emails or attachments marked Secret and 15 marked Confidential. One document, an email attachment, contained no classification markings and it was determined to contain Secret information on the basis of related emails. Of the classified items reviewed, 13 documents were compliant with all the required classification markings. The majority of emails (19) did not contain paragraph portion markings to enable the reader to determine what part of the email was classified or unclassified. (b) (6) from (b) (7)(E) and (b) (6) (b) (7)(E) were contacted and advised of the discrepancy and was instructed of the proper marking procedures. OSP inspectors provided classification marking reference material, including an Information Security Oversight Office (ISOO) marking booklet and a (b) (7)(E) information guide sheet for classification marking, to assist them to in correctly portion mark documents on the (b) (7)(E). Of the 32 classified documents reviewed, 18 were originated by (b) (7)(E); eight were originated from (b) (7)(E) personnel, four originated from (b) (7)(E) and two were originated from the office of (b) (7)(E).

Office of Special Security Programs 4th Quarter FY15 Self Inspections

The 4th Quarter FY15 self-inspection encompassed rooms (b) (7)(E) of the Main Treasury and the (b) (7)(E) and room (b) (7)(E)

On September 19, 2015, Special Security Program Facility Security Officials (SSP FSO) conducted a self-inspection in (b) (7)(E). (b) (7)(E) has (b) (7)(E), and (b) (7)(E) cubicles occupied by (b) (7)(E) employees with (b) (7)(E). One serious security infraction was discovered in which (b) (7)(E) was returned to the Office Director the next business day and the employee in violation was briefed (b) (7)(E) Four minor security findings were identified, (b) (7)(E) These security findings were corrected after email notifications were disseminated to employees.

On September 19, 2015, SSP FSOs conducted a self-inspection in (b) (7)(E). (b) (7)(E) has two offices, and (b) (7)(E) occupied by (b) (7)(E) employees with (b) (7)(E) terminals and (b) (7)(E). One serious security infraction was discovered and consisted of (b) (7)(E) The employee in violation was briefed on the requirement (b) (7)(E) before departing the facility for the day. Four minor security findings were discovered, of which one security finding was corrected during the inspection and three were corrected after email notifications were disseminated to employees. (b) (7)(E)

(b) (7)(E)

On September 19, 2015, SSP FSOs conducted a self-inspection in (b) (7)(E). (b) (7)(E) has four offices, and (b) (7)(E) occupied by (b) (7)(E) employees with (b) (7)(E) terminals and (b) (7)(E). Two serious security infractions were discovered and consisted of (b) (7)(E) materials were returned to the Office Director the next business day and the employees in violation were briefed on the proper storage (b) (7)(E). Thirteen (13) minor security findings were discovered, of which five were corrected during the inspection and eight were corrected after email notifications were disseminated to the employees. The security findings discovered consisted of (b) (7)(E)

On September 19, 2015, SSP FSOs conducted a self-inspection in (b) (7)(E). (b) (7)(E) has (b) (7)(E) workstations with (b) (7)(E) systems. No security infractions were identified.

On September 26, 2015, SSP FSOs conducted a self-inspection of the (b) (7)(E). The (b) (7)(E) has (b) (7)(E) and (b) (7)(E) occupied by (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). Seventy-Two (72) minor security findings were discovered, of which 43 were corrected during the inspection and 29 were corrected after email notifications were disseminated to the employees. The security findings discovered consisted of (b) (7)(E) The FSOs removed the unauthorized equipment and briefed the users.

On September 26, 2015, SSP FSOs conducted a self-inspection (b) (7)(E). The (b) (7)(E) has (b) (7)(E), and (b) (7)(E) occupied by (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). Twenty-six (26) minor security findings were discovered, of which 17 were corrected during the inspection and nine were corrected after email notifications were disseminated to the employees. The security findings discovered consisted of (b) (7)(E) A work request was submitted to have the proper spacing of equipment corrected.

No security finding resulted in the disclosure of classified information. All security findings were identified to employees and will be emphasized during annual security training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 13, 2016

MEMORANDUM FOR: **Michael W. Maso** [redacted]
Deputy Assistant S r Security

FROM: [redacted]

[redacted]
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 1st Quarter FY 2016 Self Inspections

During the 1st Quarter of FY16, the Office of Security Programs (OSP) conducted a non-working hours self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 22, 2015, OSP's non-working-hours self-inspection was conducted on the [redacted] facility. The [redacted] workstations inspected belonged to [redacted] Of the [redacted] workstations, [redacted] were inspected. Eight security infractions were discovered within [redacted] The security infractions were recorded by OSP personnel inspection team. [redacted] security representative, was notified regarding the [redacted]

infractions and security guidance was provided to [redacted] to correct deficiencies. No other security infractions were noted.

In the 1st Quarter FY 2016, OSP reviewed samplings of classified documents created by Treasury employees with [redacted] accounts. Five (5) classified hard copy documents were reviewed from the [redacted] office. These fit most of OSP's criteria for review (i.e. mandatory classification markings under Executive Order 13526). The classified documents reviewed were marked Secret NOFORN (S/NF) and all documents were compliant with all the required classification markings.

Office of Special Security Programs 1st Quarter FY16 Self Inspections

The 1st Quarter FY16 self-inspection encompassed [redacted], located in Rooms [redacted], [redacted] of the Main Treasury.

On December 7 - 8, 2015, Special Security Programs Facility Security Officials (SSP FSO) conducted a self-inspection of Room [redacted]. Room [redacted] has [redacted] with [redacted] workstations consisting of [redacted] terminals, and [redacted]. A total of two serious security infractions were discovered in which [redacted] were returned the next business day to the Office Director of each employee in violation. Four minor security findings were discovered, of which two were corrected during the inspection and two were corrected after email notifications were disseminated to the employees in violation. The findings consisted of [redacted].

On December 8, 2015, SSP FSO conducted a self-inspection of Room [redacted]. Room [redacted] is one room with [redacted] workstations, [redacted], [redacted], and [redacted] in room [redacted] are neither [redacted], nor [redacted] systems and will only be identified for this room in this report as computer terminals. No security violations were identified.

On December 12, 2015 SSP FSO conducted a self-inspection of Rooms [redacted] and [redacted]. Rooms [redacted] and [redacted] has [redacted] with [redacted] workstations consisting of [redacted] terminals, and [redacted]. One serious security infraction was discovered in which [redacted] was returned the next business day to the Office Director of the employee in violation. Seven minor security findings were discovered, in which five were corrected during the inspection and two were corrected after email notifications were disseminated to the employees in violation. The findings consisted of [redacted]

(b) (7)(E)

On December 19, 2015 SSP FSO conducted a self-inspection of Room (b) (7)(E). Room (b) (7)(E) has (b) (7)(E) There are (b) (7)(E) terminals, and (b) (7)(E). One serious security infraction was discovered in which (b) (7)(E) was returned to the Office Director of the employee in violation the next business day. Three minor security findings were discovered, of which one was corrected during the inspection and two were corrected after e-mail notifications were sent to the employees in violation. The security findings consisted of (b) (7)(E)

On December 19, 2015, SSP FSO conducted a self-inspection of Room (b) (7)(E). Room (b) (7)(E) has (b) (7)(E) with (b)(7)(E) workstations consisting of (b) (7)(E) terminals, and (b) (7)(E). One serious security infraction discovered (b) (7)(E) material was returned to the Office Director of the employee in violation the next business day. Four minor security findings were discovered of which three were corrected during the inspection. The security findings consisted of (b) (7)(E)

No security finding resulted in the disclosure of classified information. All findings were identified to the employees and will be emphasized during annual training. In cases where employees did not (b) (7)(E), each person was later briefed by the FSO of their violation and reminded that (b) (7)(E) as outlined in the Facility's Standard Operating Procedures (SOP).

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

April 4, 2016

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

FROM: (b) (6), (b) (7)(C)
Director, Office of Security Programs
(b) (6), (b) (7)(C)
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 2nd Quarter FY 2016 Self Inspections

During the 2nd Quarter of FY16, the Office of Security Programs (OSP) conducted a self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 31, 2016, OSP's self-inspection was conducted on the (b) (7)(E) A total of (b) (7)(E) workstations were inspected. Of the (b) (7)(E) workstations, there were (b) (7)(E) inspected. No security discrepancies were identified.

During this 2nd Quarter FY 2016 self-inspection, OSP reviewed random samplings of classified documents created by Treasury employees from the (b) (7)(E) located in Room (b) (7)(E) of the Main Treasury. Sampling of ten classified and unclassified electronic emails and attachments generated by (b) (7)(E) employees were reviewed with the employee directly. These samplings fit most of OSP's criteria for review (i.e. mandatory classification markings under Executive Order 13526). The classified items reviewed included seven emails or attachments

marked Secret and three marked Unclassified, For Official Use Only. Of the classified items reviewed, four documents were compliant with all the required classification markings. Three email attachments, classified Secret, contained no classification markings and it was determined to contain Secret information on the basis of related emails. The majority of emails did not contain paragraph portion markings to enable the reader to determine what part of the email was classified or unclassified. (b) (6) from the (b) (7)(E) were advised of this discrepancy and were instructed of the proper marking procedures and received on the spot classification marking training. The OSP inspector provided classification marking reference material, including an Information Security Oversight Office (ISOO) marking booklet and a TSDN information guide sheet via email to each employee for future guidance on classification marking.

Office of Special Security Programs 2nd Quarter FY16 Self Inspections

The 2nd Quarter FY 2016 inspections encompassed rooms (b) (7)(E) of the Main Treasury.

On March 12, 2016, Special Security Programs Facility Security Officials (SSP FSO) conducted a self-inspection of suite (b) (7)(E) of the Main Treasury building which is occupied by (b) (7)(E) Suite (b) (7)(E) has (b) (7)(E) (b) (7)(E) and (b) (7)(E) Within the suite there are (b) (7)(E) terminals, and (b) (7)(E) . Three serious security violations were noted in which (b) (7)(E) (b) (7)(E) returned to each person in violation the next business day. They were also informed of the proper handling and protection (b) (7)(E). A total of 10 minor security findings were noted, of which seven were corrected on the spot and two were corrected after email notifications were sent to employees. The findings were that (b) (7)(E)

On March 14, 2016, SSP FSO conducted a self-inspection of (b) (7)(E) and (b) (7)(E) of the Main Treasury building which is occupied by (b) (7)(E) team. (b) (7)(E) has (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E) . (b) (7)(E) is (b) (7)(E) managed by (b) (7)(E). One minor security finding was noted in (b) (7)(E) and was corrected on the spot. The finding was (b) (7)(E) There were no security infractions in (b) (7)(E)

On March 16, 2016, SSP FSO conducted a self-inspection of suite (b) (7)(E) of the Main Treasury building, which is occupied by (b) (7)(E). Suite (b) (7)(E) has (b) (7)(E) with (b) (7)(E) terminals, and (b) (7)(E) . Three minor security findings were noted, of which two were corrected on the spot and one was corrected after an email notification was sent to the employee. The findings were (b) (7)(E)

(b) (7)(E)

On March 18, 2016, SSP FSO conducted a self-inspection of suite (b) (7)(E) of the Main Treasury building. Suite (b) (7)(E) is jointly occupied by the (b) (7)(E) and (b) (7)(E) Suite (b) (7)(E) has (b) (7)(E) offices, (b) (7)(E), (b) (7)(E) and (b) (7)(E). Within suite (b) (7)(E) there are (b) (7)(E) terminals, (b) (7)(E) fax machines, (b) (7)(E) and (b) (7)(E). A total of 11 minor security findings were noted, of which ten were fixed on the spot and one finding was corrected after email notification was sent to employee. The findings were (b) (7)(E)

On March 18, 2016, SSP FSO conducted a self-inspection of suite (b) (7)(E) of the Main Treasury building. Suite (b) (7)(E) is occupied by (b) (7)(E). Within Suite (b) (7)(E) there are (b) (7)(E) terminals, and (b) (7)(E). No security infractions were identified.

In conclusion, no security finding resulted in the disclosure of classified information. All findings were identified to the employees and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

July 18, 2016

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

FROM: [redacted]
Director, Office of Security Programs
[redacted]
Director, Office of Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 3rd Quarter FY 2016 Self Inspections

During the 3rd Quarter of FY16, the Office of Security Programs (OSP) conducted a self-inspection to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 June 17, 2016 OSP's self-inspection was conducted on the [redacted]. A total of [redacted] workstations were inspected. Of the [redacted] workstations, there were [redacted] inspected. One security infraction was identified [redacted] This finding was corrected immediately during our inspection and policy guidance was provided to [redacted] staff. All safe containers had the required security container check sheet (SF 702) posted and proper open/close records were maintained. All information systems, printers and STE phones were properly labeled with classification stickers. No other security infractions were noted.

(b) (6), (b) (7)(C), Physical Security Specialist reviewed (b) (7)(E) Standard Operating Procedures (SOP) and identified (b) (7)(E) approval is limited to information technology systems connectivity only and paper requires closed storage. (b) (7)(E) SOP needs to be re-aligned with (b) (7)(E) requirements stated in (b) (7)(E) space accreditation letter. Coordination between OSP Chief of Physical Security and (b) (7)(E) Security Official is required to revise (b) (7)(E) SOP.

During this 3rd Quarter FY 2016 self-inspection, OSP reviewed random samplings of classified documents created by (b) (7)(E) employees on the (b) (7)(E) terminals located in Suite (b) (7)(E). A sampling of 34 classified and unclassified actual electronic emails and attachments generated by (b) (7)(E) employees were reviewed with the employee present. These samplings fit most of OSP's criteria for review (i.e. mandatory classification markings under Executive Order 13526). The classified items reviewed included 23 emails or attachments marked Secret or Secret NOFORN and 11 were marked Unclassified For Official Use Only. Of the classified items reviewed, seven documents were compliant with the required classification markings. Sixteen emails had incorrect portion marking(s) related to subject line, paragraph(s) and/or attachments. The (b) (7)(E) staff selected for random classification sampling were advised of classification marking discrepancies and instructed on proper marking procedures, receiving on the spot classification marking training from OSP. The OSP inspector provided classification marking reference material, including an Information Security Oversight Office (ISOO) marking booklet and a (b) (7)(E) information guide sheet via email to each employee for future guidance on classification marking. All findings identified will be emphasized during annual security refresher training.

Office of Special Security Programs 3rd Quarter FY16 Self Inspections

The 3rd Quarter FY16 inspections encompassed rooms (b) (7)(E) of the Main Treasury, (b) (7)(E) room (b) (7)(E) and rooms (b) (7)(E)

On June 23, 2016, SSP FSO conducted a self-inspection of room (b) (7)(E) of the Main Treasury building. This (b) (7)(E) is primarily used by (b) (7)(E) and has a (b) (7)(E) (b) (7)(E) terminals. Zero security infractions were noted.

On June 23, 2016, SSP FSO conducted a self-inspection of rooms (b) (7)(E) of the Main Treasury building. This office is occupied by the (b) (7)(E) with (b) (7)(E) terminal, and (b) (7)(E) One minor infraction was noted. (b) (7)(E) and the employee briefed.

On June 23, 2016, SSP FSO conducted a self-inspection of room (b) (7)(E) of the Main Treasury building. This office is occupied by (b) (7)(E) with (b) (7)(E) terminal, and (b) (7)(E). One serious infraction was noted in which a (b) (7)(E) The occupant was briefed and the document was returned.

On June 22, 2016, SSP FSO conducted a self-inspection of the (b) (7)(E) This facility has (b) (7)(E), (b) (7)(E), (b) (7)(E) with a (b) (7)(E). It is occupied by (b) (7)(E). There are (b) (7)(E) terminals, and (b) (7)(E). A total of four minor infractions were noted and corrected on the spot. The findings were (b) (7)(E)

On June 24, 2016, SSP FSO conducted a self-inspection of the (b) (7)(E) This (b) (7)(E) has a (b) (7)(E) and (b) (7)(E) positions with (b) (7)(E) terminals. Zero security infractions were noted.

On June 22, 2016 SSP FSO conducted a self-inspection of room (b) (7)(E). Room (b) (7)(E) serves as a (b) (7)(E) with (b) (7)(E), (b) (7)(E) and (b) (7)(E) workstations. There are (b) (7)(E) terminals, along with (b) (7)(E) (b) (7)(E), (b) (7)(E), (b) (7)(E) unclassified fax, and (b) (7)(E). Zero security infractions were noted.

On June 22, 2016 SSP FSO conducted a self-inspection of room (b) (7)(E). Room (b) (7)(E) is an (b) (7)(E) with (b) (7)(E) which house all (b) (7)(E) Zero security infractions were noted.

In conclusion, no security finding resulted in the disclosure of classified information. All findings were identified to members and will be emphasized during annual training.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 28, 2016

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

FROM: [redacted]
Director, Office of Security Programs
[redacted]
Director, Office Special Security Programs

SUBJECT: **After-hours Security Inspections**
Office of Security Programs 4th Quarter FY 2016 Self Inspections

During the 4th Quarter of FY16, the Office of Security Programs (OSP) conducted self-inspections for the Departmental Offices of Public Affairs, Domestic Finance, and International Affairs to review and evaluate employee compliance with security practices and procedures. These activities support the development of corrective action plans to include tailored training initiatives. All inspections were conducted for possible security infractions and security violations of requirements for safeguarding classified information. OSP's work was conducted in compliance 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 September 19, 2016 OSP inspected [redacted] located in the Main Treasury Building. A total of [redacted] workstations were inspected. Of the [redacted] workstations, there were [redacted] and [redacted] inspected. One minor security infraction was discovered in room [redacted] relating to [redacted]. [redacted] personnel had a [redacted] on their desk with disabled accounts due to infrequent use of the system. During the inspection, [redacted] random employees were interviewed to assess their awareness of policies/procedures for safeguarding classified information. As a result of the OSP random interviews, [redacted] employees interviewed, handled classified information and [redacted] employees were Public Trust with no access to classified information.

On September 22, 2016 OSP inspected (b) (7)(E) Rooms (b) (7)(E) located in the Main Treasury Building. A total of [redacted] workstations were inspected. Of the [redacted] workstations, there were (b) (7)(E) and (b) (7)(E) inspected. Three security infractions were identified relating to (b) (7)(E)

A total of [redacted] personnel had a (b) (7)(E) located on their desk with disabled accounts due to infrequent use of the system. A random sampling of classified documents from the (b) (7)(E) could not be performed during this inspection. A total of [redacted] employees were interviewed to assess individual awareness of policies/procedures for safeguarding classified. OSP reviewed a sampling of classified documents stored in a safe container located in room [redacted]. Ten classified (Secret level) documents were reviewed, three documents belonged to (b) (7)(E) and seven classified documents were external to Treasury. Of these, the three documents did not contain the proper classification authority block. OSP instructed (b) (7)(E) to return the three documents to the (b) (7)(E) office for proper classification authority blocks.

On September 29, 2016, OSP inspected (b) (7)(E) Rooms (b) (7)(E) located in the Main Treasury Building. A total of [redacted] work stations were inspected. Of the [redacted] workstations, there were (b) (7)(E). [redacted] employees were interviewed to assess their awareness of policies/procedures for safeguarding classified information. Employees displayed a keen understanding of marking policies and procedures and are using the Information Security Oversight Office Marking Classified Information Booklet (Revision 3) provided from OSP. OSP conducted a sampling of 20 classified emails (Secret level) for proper classification markings. No classification marking discrepancies were found. No security findings were identified within (b) (7)(E).

Affected collateral Departmental Offices inspected are responsible for correcting security findings. Departmental Offices shall provide a written formal notification within 30 days of receipt of OSP's "Reporting Follow-Up and Corrective Actions Taken" correspondence.

Office of Special Security Programs 4th Quarter FY16 Self Inspections

The 4th Quarter FY16 self-inspection encompassed rooms (b) (7)(E) of the Main Treasury, the (b) (7)(E) and Suite (b) (7)(E)

On September 17, 2016 Special Security Programs (SSP) Facility Security Official (FSO) conducted a self-inspection of room [redacted] of the Main Treasury building. This facility is occupied by the (b) (7)(E) and has (b) (7)(E), and (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E) A total of two minor security findings were noted and corrected on the spot. The findings were (b) (7)(E).

On September 17, 2016 SSP FSOs conducted a self-inspection of room (b) (7)(E). This facility is occupied by (b) (7)(E) personnel and has (b) (7)(E) offices and (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E) There was one serious security infraction identified. (b) (7)(E) A total of nine minor security findings were noted. The findings consisted of (b) (7)(E) Six of the findings were corrected on the spot and three were corrected on September 19, 2016. E-mail notifications were sent at all offenders.

On September 17, 2016 SSP FSOs conducted a self-inspection of room (b) (7)(E). Room (b) (7)(E) has (b) (7)(E) workstations with (b) (7)(E) computer terminals. Zero security findings were identified.

On September 17, 2016 SSP FSOs conducted a self-inspection of the (b) (7)(E). The (b) (7)(E) is occupied by the (b) (7)(E) personnel and has (b) (7)(E) offices, and (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E). One serious security infraction was discovered. (b) (7)(E) and the employee was counseled on proper closing procedures on September 19, 2016. A total of 17 minor security findings were noted. The findings consisted of (b) (7)(E) Twelve of the findings were corrected on the spot and five were corrected on September 19, 2016. E-mail notifications were sent at all offenders.

On September 17, 2016 SSP FSOs conducted a self-inspection of Suite (b) (7)(E) Suite (b) (7)(E) is occupied by (b) (7)(E) personnel and has (b) (7)(E) (b) (7)(E) offices, and (b) (7)(E) with (b) (7)(E) terminals, and (b) (7)(E). A total of 13 minor security findings were identified. The findings consisted of (b) (7)(E). Nine of the security findings were corrected on the spot and four were corrected on September 19, 2016. E-mail notifications were sent at all offenders.

On September 19, 2016 SSP FSOs conducted a self-inspection of room (b) (7)(E). Room (b) (7)(E) is occupied by (b) (7)(E) and has (b) (7)(E), and (b) (7)(E) with (b) (7)(E) terminals and (b) (7)(E) A total of three minor security findings were discovered. The findings were

(b) (7)(E) [redacted] On September 19, 2016 e-mail notifications were disseminated to the offenders.

No security finding resulted in the disclosure of classified information. All findings were identified to members and will be emphasized during annual training.