OFFICE OF THE SECRETARY

Follow-up Audit on Recommendations from Audit Report No. OIG-13-031-A, *Classified Information Policies and Practices at the Department of Commerce Need Improvement*

FINAL REPORT NO. OIG-16-048-A

SEPTEMBER 30, 2016

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

FOR PUBLIC RELEASE

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

September 30, 2016

MEMORANDUM FOR: Thomas R. Predmore
Director, Office of Security
Office of the Secretary

FROM: For Mark Zabarsky
Assistant Inspector General for Acquisition
and Special Program Audits

SUBJECT: *Follow-up Audit on Recommendations from Audit Report No. OIG-13-031-A,* Classified Information Policies and Practices at the Department of Commerce Need Improvement
Final Report No. OIG-16-048-A

Attached is the final report of our audit to determine whether the Department took appropriate corrective actions on recommendations made in the OIG's September 30, 2013, report, *Classified Information Policies and Practices at the Department of Commerce Need Improvement.* The current audit assessed whether the Office of Security's (OSY's) corrective actions in response to the five recommendations have been implemented.

The report summarizes that OSY implemented corrective actions to satisfactorily address recommendations 3 and 5. However, they either did not fully implement or address recommendations 1, 2, and 4. (See table 1 in the draft report for further details on the recommendations, OSY's original action plan response, and our current audit results.)

Based on OSY's review of the draft and subsequent discussions, the agency concurs with the findings and recommendations in the report.

In accordance with Department Administrative Order 213-5, please provide us your action plan within 60 days of this memorandum. The plan should outline the actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extend to us by your staff during our audit. If you have any questions or concerns, please contact me at (202) 482-3884 or Patrice L. Berry, Supervisory Auditor, at (202) 482-2941.

Attachment

cc: MaryAnn Mausser, Audit Liaison, Office of the Secretary

Report in Brief

SEPTEMBER 30, 2016

Background

Executive Order (order) 13526, "Classified National Security Information" prescribes a uniform system effective June 27, 2010, for classifying, safeguarding, and declassifying national security information. In addition to controlling the amount and duration of classification and sharing classified information more freely, order 13526 outlines mandatory training requirements for those with classification authority. The Department of Commerce is responsible for both implementing national policies and establishing Departmental policies to ensure that such information is adequately safeguarded when necessary and appropriately shared whenever possible.

Why We Did This Review

The Reducing Over-Classification Act of 2010 (Public Law 111-258) mandates that each inspector general with an officer or employee authorized to make original classification decisions conduct two evaluations to promote the accurate classification of information. The first evaluation was completed by September 30, 2013; a second, to be completed by September 30, 2016, must review progress made after the first. Our audit objective was to determine whether the Department took appropriate corrective actions on recommendations made in OIG's 2013 report.

OFFICE OF THE SECRETARY

Follow-up Audit on Recommendations from Audit Report No. OIG-13-031-A, *Classified Information Policies and Practices at the Department of Commerce Need Improvement*

OIG-16-048-A

WHAT WE FOUND

In our September 30, 2013, report, we issued the following recommendations to the Director, OSY:

1. ensure that the document custodian take action to finalize the disposition of the three documents identified with expired declassification dates;
2. require container custodians to be responsible for the classified documents in the container(s) they control;
3. amend the Security Manual to align with the language in Executive Order 13526 regarding markings on derivatively classified documents, as well as update annual refresher training on classification markings for derivatively generated documents
4. improve the process for entering accurate data into Security Manager and develop guidance addressing the processes to be followed for annual classified information inventory reviews; and
5. incorporate any relevant changes made as a result of recommendations in this report as part of OSY's annual reviews of the Department's classified information.

We found that OSY satisfactorily implemented corrective actions for recommendations 3 and 5, but either did not fully implement or address recommendations 1, 2, and 4:

- Recommendation 1: We found that the National Telecommunications and Information Administration custodian had not disposed of the three classified documents with expired declassification dates as OSY stated in its Action Plan.
- Recommendation 2: We found that OSY partially implemented this recommendation as it related to bi-annual inspections.
- Recommendation 4: We found that the Director, OSY, partially implemented this recommendation as it related to developing guidance addressing the processes to be followed to conduct and document annual classified information inventory reviews.

WHAT WE RECOMMEND

We recommend that the Director, OSY, fully implement recommendations 2 and 4 as agreed to in OIG report number OIG-13-031-A. Specifically:

1. Promote and enforce user reviews of classified documents.
2. Ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials.
3. Establish controls to ensure that accurate data is entered into Security Manager Database system.

Contents

COVER: Detail of fisheries pediment, U.S. Department of Commerce headquarters, by sculptor James Earle Fraser, 1934

Introduction

Since 1951, executive orders have directed government-wide classification standards and procedures. Executive Order (order) 13526, "Classified National Security Information"—signed by the President on December 29, 2009, and effective June 27, 2010—prescribes a uniform system for classifying, safeguarding, and declassifying national security information. In addition to controlling the amount and duration of classification and sharing classified information more freely among the executive branch and state, local, tribal, and private sector partners, order 13526 outlines mandatory training requirements for those with original and derivative classification authority. Pursuant to order 13526, the Information Security Oversight Office (ISOO)[1] provided a directive stating that training requirements must consist of classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

The Reducing Over-Classification Act of 2010 (Public Law 111-258)[2] mandates that the inspector general of each agency of the United States with an officer or employee authorized to make original classification decisions conduct two evaluations to promote the accurate classification of information. The first evaluation was completed by September 30, 2013; a second evaluation, to be completed by September 30, 2016, must review progress made pursuant to the results of the first.

The Department of Commerce (the Department) creates, receives, handles, and stores classified information as part of its mission. As a creator and user of classified information, the Department is responsible for both implementing national policies and establishing Departmental policies to ensure that such information is adequately safeguarded when necessary and appropriately shared whenever possible. With proper classification of classified products, the Department can share more information with external stakeholders. Within the Department, the Director of the Office of Security (OSY) is responsible for overseeing all security management. The classified information derives from original classification by Department officials, documents originating from other source documents, and documents from other agencies.

According to order 13526, information determined to require protection from unauthorized disclosure in order to prevent damage to national security must be marked appropriately to indicate its classification. The expected damage to national security that the original classification authority is able to identify or describe as resulting from unauthorized disclosure determines the classification level:

- *top secret*—exceptionally grave damage,
- *secret*—serious damage, or

[1] ISOO is responsible for policy oversight of the government-wide classification system. According to ISOO policy, the receiving agency must treat the information the same way as original information.

[2] Enacted October 7, 2010.

- *confidential*—damage.

Only those authorized in writing by the President, the Vice President, agency heads, or other officials designated by the President may originally classify information. These authorities must be trained on proper classification prior to originally classifying information and at least once a year thereafter. *Derivative classification*—the incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material according to the source information—includes the classification of information based on classification guidance. Personnel who apply derivative classification markings must be trained to apply the principles of order 13526 prior to derivatively classifying information and at least once every 2 years thereafter. Information may be derivatively classified from a source document or documents, or by using a classification guide.

Objectives, Findings, and Recommendations

In October 2010, the President signed the Reducing Over-Classification Act, which requires inspectors general to conduct two evaluations of their departments' compliance with the Act by September 30, 2016. We completed the Department's first audit on September 30, 2013.[3] The Director, OSY, concurred with all 5 recommendations made to the Department in OIG's report of that audit. On April 3, 2014, OSY provided us its plan detailing the corrective actions taken in response to our prior audit (see Appendix B). To comply with this Act, we conducted this follow-up audit to review progress made pursuant to the results and recommendations of the first audit.

Our audit objective was to determine whether the Department has taken appropriate corrective actions on recommendations made in OIG's September 30, 2013 report. We found that OSY satisfactorily implemented corrective actions for recommendations 3 and 5, but either did not fully implement or address recommendations 1, 2, and 4. Table 1 details our results for recommendations 1, 2, and 4.

Table 1. Details of Findings by Recommendation

Recommendation 1	**Ensure that the document custodian takes action to finalize the disposition of the three documents identified in the audit with expired declassification dates.**
OSY Action Plan Response[4]	NTIA informed OSY that the documents had been destroyed as they were no longer required for NTIA operations.
Audit Results	We found that the NTIA custodian had not disposed of the three classified documents with expired declassification dates as OSY stated in its Action Plan. This occurred because OSY relied on NTIA's email that the three classified documents had been destroyed and did not validate whether or not the destruction had actually taken place. On June 17, 2016, OSY provided us supporting documentation showing that the document custodian destroyed all three NTIA expired classified documents on May 20, 2016. We further validated that as of July 15, 2016, the Security Manager Database system[5] appropriately reflects that the three NTIA expired classified documents have been destroyed.

[3] Department of Commerce Office of Inspector General, September 30, 2013. Classified Information Policies and Practices at the Department of Commerce Need Improvement, OIG-13-031-A. Washington, DC: DOC OIG.

[4] OSY Action Plan, dated April 3, 2014.

[5] OSY uses the Security Manager Database system to track and account for the entire Department's classified information.

Recommendation 2	**Require container custodians to be responsible for the classified documents in the container(s) they control and (a) promote and enforce user reviews of classified documents, as well as (b) ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials.**
OSY Action Plan Response	Container custodians are inspected on a bi-annual basis and OSY updated and enhanced the inspection to provide custodians a "Custodian's Container and Document Pre-Inspection Check Sheet."
Audit Results	We found that OSY partially implemented this recommendation as it related to bi-annual inspections. Although OSY inferred in its action plan that these inspections were on-going, OSY did not start its bi-annual inspections of container custodians until almost 2 years later—March 2016—because of staffing issues. OSY personnel stated that during this time frame, the Information and Personnel Security Division (IPSD) staff went down from four Information Security Specialists to one. OSY personnel explained that as of March 2016, they were in the process of conducting a 100 percent review of all containers and their associated contents. OSY also provided us a copy of the "Custodian's Container and Document Pre-Inspection Check Sheet" for our review. Furthermore, due to an oversight by OSY management, OSY did not address how to promote and enforce user reviews of classified documents or ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials.

Recommendation 4	**Improve the process for entering accurate data into Security Manager and develop guidance addressing the processes to be followed to conduct and document annual classified information inventory reviews.**
OSY Action Plan Response	OSY improved its annual custodian classified information inventory reviews by updating the checklists for the Information Security Specialists who perform the inspections. OSY also made corrections to the OSY *Security Manual*, outlining the requirement for annual inventorying of classified documents.
Audit Results	We found that the Director, OSY, partially implemented this recommendation as it related to developing guidance addressing the processes to be followed to conduct and document annual classified information inventory reviews. In March 2016, OSY made corrections to the Security Manual, Chapter 22[6] outlining the requirement for annual inventorying of classified documents. OSY also updated both the Classified NSI Inspection Check Sheet[7] and the Custodian's Container and Document Pre Inspection Sheet.[8] However, the container custodians that we interviewed from National Telecommunications & Information Administration, Bureau of Industry and Security, and the Office of the Secretary could not provide us with copies of their completed Pre-Inspection forms because they had not received them from their respective Bureau Agency Security Contact. In addition, because of OSY management oversight, OSY did not address how to improve the process for entering accurate data into the Security Manager Database system.

If employees with derivative classification authority do not receive proper guidance and training on policies and procedures, classified documents, or portions of classified documents, may be improperly released; the authors of classified documents may be unknown and employees may not have all of the information necessary for declassification. Without improvements, the weaknesses identified may limit the Department's ability to make informed risk-based decisions that support the protection of classified information and the Security Manager Database system on which it resides. As such, fully implementing the recommendations identified in report number OIG-13-031-A should help enhance the Department's management of risk of overclassified information.

[6] Chapter 22, "*Custody and Accountability of Classified National Security Information*," dated March 2016 outlines the requirement for annual inventory and disposal of classified holdings.

[7] This form is used by the Information Security Specialists who perform the inspections.

[8] This form is used by the container custodians in preparation for the inspection.

Recommendations

We recommend that the Director, OSY, fully implement recommendations 2 and 4 as agreed to in OIG report number OIG-13-031-A. Specifically:

1. Promote and enforce user reviews of classified documents.
2. Ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials.
3. Establish controls to ensure that accurate data is entered into Security Manager Database system.

Summary of Agency Response and OIG Comments

OIG received comments on the draft report from OSY, which we include as appendix C of this final report.

Based on OSY's review of the draft and subsequent discussions, the agency concurs with the recommendations in the report. In its response, OSY disagreed with some facts that are included in "Recommendation 2, Audit Results." The Director, OSY, asserted that the Security Manager database showed 154 bi-annual inspections had been conducted between 2014 and 2016. On September 23, 2016, we met with the Director, OSY, and requested that they provide documentation to support their assertion of 154 bi-annual inspections; however, OSY did not respond to our request. Furthermore, as stated in our report, in an August 5, 2016, email, the Program Manager, Information and Personnel Security Division—who is responsible for overseeing the Department's bi-annual inspection program—confirmed that no bi-annual inspections were conducted in 2014 and 2015. The Program Manager also confirmed that the bi-annual inspection program did not start until March 2016.

Appendix A: Objectives, Scope, and Methodology

The objective of our audit was to determine whether the Department has taken appropriate corrective actions on recommendations made by OIG in report number OIG-13-031-A.

To accomplish our objectives, we obtained a list from the Department's OSY to identify the population of classified documents. OSY's list was generated from the Security Manager Database system, covering classified documents as of April 16, 2016. In report number OIG-13-031-A, we identified deficiencies in three bureaus —National Telecommunications and Information Administration, Bureau of Industry and Security, and the Office of the Secretary. Therefore, we judgmentally selected 21 out of 55 classified documents, from these three bureaus, that had been input into the Security Manager Database system from October 1, 2015 through April 16, 2016 for review. Top secret documents were not included within the scope of our audit of classified documents due to the process necessary to access these records and the lack of availability of properly cleared staff.

In addition, we

- reviewed the April 3, 2014, Office of Security Action Plan to familiarize ourselves with the proposed corrective actions;
- reviewed the Status of Recommendations Report and associated supporting documentation to confirm the corrective actions taken by OSY;
- discussed management classification practices with OSY; and
- coordinated our scope and methodologies with the other agency inspectors general and the Information Security Oversight Office.

We tested the reliability of the data provided in the Security Manager Database system by analyzing it for irregularities and inconsistencies such as missing data, misstatements, and other obvious errors. However, we did not have access to the IT system. While we noted discrepancies, they were not a material representation of the entire population of information and, thus, we consider the system data sufficiently reliable for use in our audit.

We conducted the audit fieldwork between March 2016 and August 2016. We performed our fieldwork at the Department of Commerce, Office of Security. We performed our work under the authority of the Inspector General Act of 1978, as amended, and Department Organizational Order 10-13, April 26, 2013. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B: Office of Security Action Plan

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

APR 3 - 2014

MEMORANDUM FOR Andrew Katsaros
Assistant Inspector General for Audit

FROM: Thomas R. Predmore
Director for Security

SUBJECT: Classified Information Policies and Practices at the Department of Commerce Need Improvement

Enclosed you will find the Office of Security Action Plan addressing the issues highlighted in the Office of Audit and Evaluation Report, Classified Information Policies and Practices at the Department of Commerce Need Improvement.

If you should have any questions or need additional information concerning this report, please contact Eric Dorsey, Assistant Director, Information and Personnel Security Division, Office of Security, at 202-482-8115 or edorsey@doc.gov.

Sincerely,

Thomas R. Predmore
Director for Security

Enclosure

DOC OFFICE OF SECURITY ACTION PLAN AND RESPONSE

Office of the Inspector General Audit Report (September 20, 2013)

"The Department could improve certain classification policies, procedures, rules and regulations prescribed by E.O. 13526 and the Department's Security Manual"

Recommendation 1 of 5: Ensure that the document custodian take action to finalize the disposition of the three documents identified in the audit with expired declassification dates:

Action/Status: Complete.

- NTIA was notified by the OIG Auditors of the three documents identified as having expired declassification dates. NTIA informed the Office of Security (OSY) that the documents have since been destroyed as they were no longer required for NTIA operations.

- OSY updated and enhanced the information security inspection by providing a "Custodian's Container and Document Pre-Inspection Sheet" for custodians to evaluate themselves prior to the OSY inspection. Specifically, there is a question in the pre-inspection sheet that asks the custodian, "Are there any classified documents in your possession that have expired declassification dates or are older than 25-years.?" The form further asks the custodian to have those documents available for review by OSY.

- OSY has included additional training for mandatory declassification reviews in the initial and annual refresher briefings.

Recommendation 2 of 5: Require container custodians to be responsible for the classified documents in the container(s) they control and: (a) promote and enforce user reviews of classified documents, as well as (b) ensure custodians are trained and understand their responsibilities to account for, control, and purge classified materials:

Action/Status: Ongoing

- Container custodians are inspected on a bi-annual basis. OSY updated and enhanced the inspection to provide a "Custodian's Container and Document Pre-Inspection Check Sheet" for custodians. The check sheet alerts custodians to commonly overlooked safeguards such as, declassification reviews; annual inventory of classified documents; and derivative/original classification accountability in the OSY database.

- The check sheet further asks the custodian for the oldest classified document(s) in their inventory, and requests the document(s) to be available during the inspection.

Recommendation 3 of 5: Amend the Security Manual to align with the language in E.O. 13526 that requires the name and position or personal identifier to be listed on derivatively classified documents, as well as update annual refresher training to include how to apply classification markings on derivatively generated documents

Action/Status: Completed and Ongoing.

- The new ISOO Marking Guide was provided electronically to the Department's Security Contacts for distribution to all clearance holders.

- Corrections to the OSY Security Manual, outlining the updated language in the Order for proper marking of derivatively classified documents are included for the next release.

- OSY has included specific directions for applying classification markings, on derivatively classified documents, in the Annual National Security Information Refresher Training.

Recommendation 4 of 5: Improve the process for entering accurate data into Security Manager and develop guidance addressing the process to be followed to conduct and document annual classified information inventory reviews.

Action/Status: Ongoing

- OSY has improved its document inspection program to include updating checklists for the Information Security Specialists who perform the inspections. Custodians are provided a pre-inspection check sheet for preparation and awareness. The check sheet is used by the security specialist to prepare for issues of inventorying, documenting generated (original and derivative) documents in the Security Manager database, and the marking of classified documents.

- Corrections to the OSY Security Manual, outlining the requirement for annual inventorying of classified documents are included for the next release. Each June, OSY will provide an inventory of documents listed in the OSY database to each custodian for them to reconcile and update the information accordingly.

- OSY also updated the classified document and container review check sheet, used by the Information Security Specialists. The check sheet now requires the specialist to ask "if" and "how" the annual inventory is conducted.

Recommendation 5 of 5: Incorporate any relevant changes made as a result of recommendations in this report as part of the Office of Security's annual reviews of the Department's classified information.

Action/Status: Ongoing

- OSY will continue to incorporate all relevant enhancements as a result of recommendations in the OIG Audit Report as a part of the OSY's regular reviews of classified information.

- The pre-inspection checklist will provide awareness of items requiring improvement in the DOC classified information policies and practices, such as notification to outside agencies for classified documents that have reached their declassification date; and other matters outlined in the OIG Audit Report.

- OSY continues to conduct the monthly After-Hours Inspection Program, which is done to verify and validate compliance with classified information storage and safeguarding requirements. The office will also begin unannounced duty-hours inspections in areas where classified systems reside.

Office of Security
Classified NSI Inspection

Date of review:_____ Inspector's name: _____

Office address being inspected _____ Room #:_____

Container # _____ Highest level of classified stored: TS S

Primary Custodian name: _____

Interviewed: Yes No Telephone: _____

Alternate Custodian name: _____

Interviewed: Yes No Telephone: _____

1. Are you aware of the need-to-know principle in regards to your security clearance?	Yes	No	N/A
2. Are appropriate forms being used and completed as required?	Yes	No	N/A
SF 700	Yes	No	N/A
SF 701	Yes	No	N/A
SF 702	Yes	No	N/A
3. Do you know who has Original Classification Authority within your bureau? If yes who?	Yes	No	N/A
4. How is classified information received in the office? Mail _____ Hand Carried _____ Other_____			
5. Is there a log maintained for classified material stored?	Yes	No	N/A
6. Can you identify a classified document that is not correctly marked?	Yes	No	N/A
7. Do containers have an excessive amount of classified?	Yes	No	N/A
8. Is any classified information subject to automatic declassification?	Yes	No	N/A
9. Does your office perform derivative classification?	Yes	No	N/A
10. Does your office have computers to process classified information?	Yes	No	N/A
11. Do you have a need to reproduce classified material received, i.e. copy machine? If no proceed to # 14	Yes	No	N/A
12. When classified material is reproduced are additional copies accounted for?	Yes	No	N/A
13. Is your copy machine approved for classified reproduction?	Yes	No	N/A
14. Do you use the appropriate cover sheets for your classified documents?	Yes	No	N/A

Office of Security
Classified NSI Inspection

15. How is classified information destroyed in your office? ____ Shredder ___ Burn ___Pulp ____Other			
16. Is the office shredder approved for classified destruction?	Yes	No	N/A
17. Do you have the proper classified destruction procedures readily available for emergencies?	Yes	No	N/A
18. Has there ever been a security infraction/violation in your office?	Yes	No	N/A
19. Are quarterly document inventories conducted?	Yes	No	N/A
20. How are yearly document inventories recorded?			
21. Review the oldest classified document in the custodian's container. Disposition: _____ _____			

(OSY Inspector should use this section to document compliance)

Document Bar code Number	Document markings		Classified-declassified line		Bar-coded (Generated Only)	
Document Compliant	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Is the container compliant? _____ Yes _____No

Inspector's initials and date of inspection _____

Appendix C: Agency Response

SEP 2 2 2016

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington D.C. 20230

MEMORANDUM FOR: Mark H. Zabarsky
Assistant Inspector General for Acquisition and Special Programs
Office of the Inspector General

FROM: Thomas R. Predmore
Director for Security

SUBJECT: Draft Report - Follow-up Audit on Recommendations from Audit Report No. OIG-13-031-A, *Classified Information Policies and Practices at the Department of Commerce Need Improvement*

Thank you for performing your follow-up audit and helping us to identify additional areas to improve our program. I concur with your findings with the exception of facts in "Recommendation 2, Audit Results."

"Recommendation 2, Audit Results" states that, "OSY did not start bi-annual inspections of container custodians until almost 2 years later – March 2016 - because of staffing issues." In fact, OSY conducted 41 container inspections in 2014, 51 in 2015 and 62 in 2016 per records in Security Manager. In addition, in 2016, OSY personnel assigned to ITA conducted 12 container inspections and 14 container inspections relating to excessing these containers as ITA relocated from swing space to permanent renovated space. These were not documented in Security Manager, but exist in hard files.

As a result, I would suggest the following revision:

"We found that OSY partially implemented this recommendation as it related to bi-annual inspections. Although OSY completed a number of container inspections, OSY needs to improve its oversight and tracking to ensure all bi-annual inspections are completed. OSY personnel stated that reduced staffing during this time frame resulted in inspection shortfalls (one extended absence and one vacancy); however, the office is now fully manned. OSY also provided us a copy of the Custodian's Container and Document Pre-Inspection Check Sheet for our review. Furthermore, due to an oversight by OSY management, OSY did not address how to promote and enforce user reviews of classified documents or ensure custodians are trained and understand their responsibilities to account for, control and purge classified materials."

For any questions or concerns regarding this matter, please contact Mr. Michael Bryant, Program Manager, Information and Personnel Security Division, at (202) 482-6380 or mbryant@doc.gov.

011200000244