Office of the Inspector General
U.S. Department of Justice

Follow-up Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements

Audit Division 16-26 September 2016

FOLLOW-UP AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

EXECUTIVE SUMMARY

In fiscal year (FY) 2010, Congress passed Public Law 111–258 (2010), the *Reducing Over-Classification Act*, which required the Inspectors General for all federal agencies and departments with officers and employees possessing original classification authority to conduct two evaluations – one in FY 2013 and another in FY 2016.

In September 2013, the Department of Justice (DOJ or Department) Office of the Inspector General (OIG) issued its audit report on DOJ's Implementation of and Compliance with Certain Classification Requirements.[1] For that first evaluation, Congress directed the Inspectors General to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within departments, agencies, or components; and (2) identify policies, procedures, rules, regulations, or practices that may contribute to persistent misclassification of material within such departments, agencies, or components.

The OIG found that DOJ, through the Justice Management Division's (JMD) Security and Emergency Planning Staff (SEPS), had established classification policies and procedures, but had not effectively administered them to ensure that information was classified and disseminated appropriately. Although we did not find indications of widespread misclassification, we identified deficiencies relating to the implementation of DOJ's classification program, including a persistent misunderstanding and lack of knowledge of certain classification processes by DOJ officials. We also identified weaknesses in DOJ's implementation of classification standards, the limited distribution of automated tools designed to improve DOJ's classification and marking processes, and weaknesses in the application of information security education and training programs. In our FY 2013 report, we made 14 recommendations to help improve DOJ's classification management program and its implementation of classification procedures.

Pursuant to the requirements of the *Reducing Over-Classification Act*, in this report we evaluate DOJ's progress made pursuant to the results of our FY 2013 report. We found that since our last audit SEPS has improved its administration of classification policies and procedures and enhanced the DOJ's classification management program. These improvements were evident in our review of DOJ's classification authority delegations, classification decision designations, updated

[1] U.S. Department of Justice Office of the Inspector General, *Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements,* Audit Report 13-40 (September 2013).

classification guidance, and classification reports. We believe that DOJ achieved these improvements because SEPS provided updated classification guidance, instruction, and training to DOJ components, which resulted in components having a clearer understanding of classification policies and procedures. As a result of SEPS's progress in these areas, we have closed 11 of the 14 recommendations identified in our FY 2013 audit.

The appropriate use of original classification authority (OCA) reduces the risks of misclassifying and overclassifying information. In our FY 2013 report, we found that several DOJ components improperly classified information as "original" classification decisions, when the classification of this type of information previously had been decided. The improper use of original classification authority increases the risk that individuals could classify the same piece of information differently, resulting in the misclassification of information. In our current audit, we found significant improvements in this area, as evidenced by DOJ reducing the number of officials with Original Classification Authority from 64 in FY 2013 to 46 in FY 2016 and eliminating original classification decisions, as shown in the number of reported original classification decisions decreasing from 4,455 in FY 2013 to 0 in FY 2015. In our FY 2013 audit, we found that the high number of original classification decisions was primarily due to a misunderstanding of the differences between original and derivative classification decisions within several Department components. We believe that the dramatic reductions are indicative of DOJ personnel now having a better understanding of the classification types, as well as an improved knowledge of how to classify information using security classification guides. In addition, in 2015 SEPS incorporated comprehensive classification marking instructions in the *DOJ Marking Classified National Security Information*, implemented a software application to improve classified marking procedures for electronic files processed on classified information systems, and mandated usage of these tools for all DOJ classifiers. Security Programs Managers throughout the Department told us that these changes have resulted in classifiers more appropriately marking classified work products, in particular electronic documents.

SEPS is also involved in the Fundamental Classification Guidance Review process, with a potential outcome of consolidating Departmental security classification guides, by June 30, 2017. Through this process and its establishment of a working group comprised of officials throughout the Department, SEPS plans to reduce the number of classification guides and to ensure that classification guidance is appropriate, accurate, and complete for all DOJ components.

However, we also found areas in which the Department still needs to improve its classification procedures and practices. Specifically, we determined that SEPS has not thoroughly evaluated DEA's use of the ORCON dissemination control marking to ensure that it is appropriate, as we recommended in our 2013 audit report. In fact, between the issuance of our last audit report in FY 2013 and initiation of this follow-up audit, the DEA had not changed its use of the ORCON marking. In January 2016, the DEA implemented a process to evaluate information on a case-by-case before marking it ORCON. Also, we found that the DEA may be implementing classification practices that result in the under- or over-classification

of information. For example, we found that the DEA's practices could result in it classifying the same piece of information as unclassified law enforcement sensitive information in a DEA investigative case file, but as classified information in a DEA intelligence report. SEPS must continue to coordinate with the DEA to ensure that it is appropriately implementing classification procedures and consistently and accurately marking classified information.

SEPS also has been unable to implement consistently its enhanced process for reviewing component self-inspections reports. Additionally, although SEPS issued a memorandum to all components requiring the incorporation of classification management into the performance plans and evaluations, DOJ components, including the Criminal Division, have not done so. Also, DOJ did not publish updated procedures for the Mandatory Declassification Review process, as required by Executive Order 13526, *Classified National Security Information*.

Finally, we reported in FY 2013 that deficiencies reported in DOJ's classification management program were in part due to staffing resource constraints within SEPS. In our current audit, we found that SEPS continues to report that resource constraints hinder its ability to most effectively manage its classification management program. This situation may be further complicated by the impending expansion of SEPS's responsibilities to launch and oversee the DOJ's efforts related to the new government-wide program for controlled unclassified information (CUI) – unclassified information that requires controls for safeguarding or dissemination.

As a result of our findings in this audit, we make three new recommendations to SEPS to further help improve DOJ's classification management program and implementation of classification procedures. In addition to working with SEPS to implement these recommendations, we will continue to coordinate with SEPS on the resolution and implementation of our previous recommendations related to the review of security classification guides and validation that the DEA's use of the ORCON dissemination control is appropriate.

FOLLOW-UP AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

TABLE OF CONTENTS

FOLLOW-UP AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

INTRODUCTION

The appropriate classification of information is critical to the government's efforts to ensure national security. Over-classification of information restricts accurate and actionable information sharing, increases the cost of securing information, and needlessly limits stakeholder and public access to information.[2] In 2010, Congress passed Public Law 111-258, the *Reducing Over-Classification Act* (Act), to determine whether agencies' classification procedures and practices contribute to over-classification and restrict information sharing. The Act directed the federal Inspectors General to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within the DOJ; and (2) identify policies, procedures, rules, regulations, or practices that may contribute to persistent misclassification of material within the DOJ. The Act also mandated that the Inspectors General follow up on their initial reviews 3 years later to assess DOJ's progress made pursuant to the results of the first evaluation. In fiscal year (FY) 2013, the Department of Justice (DOJ or Department) Office of the Inspector General (OIG) completed the first evaluation and issued an audit report on DOJ's Implementation of and Compliance with Certain Classification Requirements.[3] In our FY 2013 audit, we made 14 recommendations to help improve the DOJ's classification management program and implementation of classification procedures.[4] This follow-up audit assesses the Department's progress in implementing these recommendations, 11 of which are closed, and makes additional recommendations for further improvement in this important area.

Classification Management and Process Overview

Executive Order (EO) 13526, *Classified National Security Information*, prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The National Archives and Records Administration's (NARA) Information Security Oversight Office is responsible for issuing directives for implementing EO 13526 to all government agencies that handle classified information.

---

[2] Over-classification is either treating unclassified information as if it were classified, or classifying it at a higher level of classification than is appropriate.

[3] U.S. Department of Justice Office of the Inspector General, *Audit of the Department of Justice's Implementation of and Compliance with Certain Classification Requirements,* Audit Report 13-40 (September 2013).

[4] Appendix 2 provides an overview of these 14 recommendations.

Within DOJ, the Justice Management Division's (JMD) Security and Emergency Planning Staff (SEPS) is responsible for the classification management program and must ensure that DOJ complies with classified national security information laws, regulations, directives, and other guidance, as appropriate. SEPS promulgates all DOJ classification policies and procedures through the issuance of the Security Program Operating Manual (SPOM). In addition, SEPS works with DOJ components' Security Programs Managers on the implementation and oversight of the classification management program. In our FY 2013 report, we identified that DOJ had a total of 57,979 employees and contractors who had security clearances and, thus, classification responsibilities. SEPS officials identified that as of June 2016 the number of cleared personnel with classification responsibilities had increased to 63,046.

The classification process begins when information is identified as posing a risk to national security if disclosed without authorization. An official with "Original Classification Authority" (OCA) designates the information as classified, which is referred to as the "original classification decision." When making this decision, the OCA official must determine how the information meets one of the eight categories prescribed in Executive Order (EO) 13526.[5] In addition, the OCA official must explain how the disclosure of information could damage national security and for how long that information needs to be protected from disclosure. Finally, the OCA official must document these determinations on the original (source) document or in a security classification guide. Security classification guides identify predetermined original classification decisions and provide instructions for derivative classifiers to use when making derivative classification decisions, including the classification level of that information, the nature of the risk to national security, the length of time the information should remain classified, and the specific category of national security information from Section 1.4 of EO 13526.

When making a derivative classification decision, an individual possessing the appropriate security clearance must carry forward and apply to any newly created derivative document the pertinent classification markings from the source document or the security classification guide.

OIG Audit Approach

During this audit, we conducted interviews with officials from the Security and Emergency Planning Staff (SEPS), Criminal Division, Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), National Security

[5] Section 1.4 of EO 13526 prescribes the following eight categories for classified national security information: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) U.S. government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; and (h) the development, production, or use of weapons of mass destruction.

Division, and Office of the Chief Information Officer (OCIO).[6] In addition, we reviewed DOJ-wide and specific DOJ components' reports on classification decisions between FY 2013 and FY 2015. We also reviewed and analyzed updated classification guidance, instruction, and training disseminated to DOJ following our previous audit and examined DOJ's implementation of the Classification Management Tool.

The results of our audit are detailed in our Audit Findings. We organized this report in the same format as our 2013 report to better enable assessments of DOJ's progress in implementing recommendations from our previous audit. The first finding area provides the results of the OIG's evaluation of changes made to DOJ's classification policies, processes, practices, and classification management tools as a result of recommendations made during our first audit. The second finding area provides our analysis of changes in DOJ's management and oversight of the classification program, evaluation of reporting requirements, the notification process regarding component involvement in Special Access Programs, and an overview of DOJ's implementation of statutory and regulatory requirements.

[6] For more information about our audit scope and methodology, see Appendix 1.

AUDIT FINDINGS

DOJ CLASSIFICATION POLICIES, PROCESSES, AND PRACTICES

In FY 2013, we found that DOJ had established classification policies and procedures, but had not effectively administered those policies and procedures to ensure that information is classified, marked, and disseminated appropriately. We believe that DOJ has improved its classification management program through the implementation of updated classification guidance, instruction, and training. Also, DOJ has reduced both the number of officials with original classification authority and original classification decisions. This was achieved through SEPS's ongoing efforts to correct or improve DOJ components' understanding of classification requirements and procedures, to include the use of security classification guides to make classification decisions. In addition, SEPS revised DOJ's classification marking guide, and expanded and mandated the use of the Classification Management Tool (CMT), which improves classified marking procedures for electronic files processed on classified information systems. SEPS can continue to improve DOJ's classification management through the ongoing effort to consolidate Department security classification guides. Furthermore, SEPS must continue to work with the DEA to ensure that its use of the ORCON dissemination control marking is appropriate and that the DEA's implementation of classification practices do not result in under- or over-classification.

DOJ Original and Derivative Classifiers

According to EO 13526, the delegations of OCA officials shall be limited to the minimum required to ensure the consistency and integrity of classified national security information, and agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority. At the end of FY 2013, DOJ had 64 OCA officials who were located in 13 components, which was a substantial reduction from the 102 OCA officials designated in FY 2012. At that time, we noted that among all DOJ components, the FBI executed the largest reduction of OCA officials from 55 to 17. During our last audit, we found that the frequency in which information is classified in the first instance, an "original classification," should be extremely rare. As a result, we found that DOJ could further reduce the number of OCA officials, particularly at the DEA, which in FY 2013 had the highest number of OCA officials. We recommended that SEPS, in conjunction with the components, re-evaluate the number and types of positions that require original classification authority to ensure compliance with EO 13526.

In response to our recommendation, JMD SEPS issued a memorandum in October 2013 that informed DOJ components of the OIG's recommendation and instructed them to reexamine the number of OCA officials in order to ensure that all

delegations of OCA are limited to designated officials who have a demonstrable and continuing need to exercise this authority. In addition, SEPS officials worked with DOJ components to ensure that OCA delegations are limited to the minimum necessary to administer EO 13526. As a result, DOJ reduced its OCA official delegations to 59, and we closed our recommendation in September 2014. Since, the Department reduced the number of OCA officials by an additional 15, and as of May 2016 had 46 OCA officials, as shown in Table 1.

Table 1

DOJ Officials with Original Classification Authority as of May 2016

DOJ Component	FY 2013	FY 2014	FY 2015	FY 2016
Office of the Attorney General	2	2	2	2
Office of the Deputy Attorney General	3	3	3	3
Office of the Associate Attorney General	1	1	1	1
Office of the Inspector General	1	1	1	1
Antitrust Division	1	1	1	1
Bureau of Alcohol, Tobacco, Firearms and Explosives	1	1	1	1
Criminal Division	7	4	3	2
Drug Enforcement Administration	20	20	20	8
Federal Bureau of Investigation	17	17	17	17
Federal Bureau of Prisons	1	1	1	1
Justice Management Division	2	2	2	2
National Security Division	7	6	6	6
U.S. Marshals Service	1	1	1	1
TOTAL	**64**	**60**	**59**	**46**

Source: SEPS

In our examination of information that DEA provided SEPS for justifying its need for its OCA officials, we found that dissimilar to the other components' responses, the DEA's original response to SEPS's request was brief and provided no explanation for its conclusion that all DEA OCA officials had a continuing need to exercise this authority. Thus, the DEA continued to have the highest number of OCA officials in the Department through FY 2015. During this follow-up audit, SEPS officials stated that recent reporting indicated that the DEA had reduced the number of original classification decisions from 950 in FY 2013 to none in FY 2015, which according to SEPS was a strong indication that the DEA did not need 20 OCA officials.

In FY 2015, the DEA's Office of Security Programs experienced personnel changes and identified a new individual as the Security Programs Manager. During the course of our audit, we revisited this topic several times with the DEA's new security officials, who concurred with SEPS's determination that the DEA could not justify maintaining 20 OCA officials. Consequently, in May 2016 the DEA reduced its number of OCA officials from 20 to 8.

We believe that the DEA's progress in this area is significant and supports our assessment that the Department's classification management program is

improving. To continue to build on these improvements, SEPS should routinely evaluate and ensure that DOJ components limit requests for OCA officials to those positions that have a demonstrable and continuing need to exercise this authority.

DOJ Security Classification Guides

As mentioned previously, security classification guides contain original classification decisions and provide derivative classifiers with a set of instructions to use when making derivative classification decisions. At the time we issued our initial report in FY 2013, DOJ had 10 approved security classification guides: one comprehensive guide established by SEPS for Department-wide use, and nine additional guides created by the Criminal Division, DEA, FBI, and U.S. Marshals Service (USMS). The OIG previously found that the Criminal Division, DEA, and USMS, which all had issued program or component-specific classification guides, had not adequately coordinated with SEPS on the issuance on their guides. We also found that SEPS did not coordinate with the National Security Division to ensure that the DOJ-wide classification guide incorporated all necessary information related to the National Security Division's operations and programs. As a result, National Security Division officials responsible for Foreign Intelligence Surveillance Act (FISA) processes were unaware of the existence of the *DOJ National Security Information Security Classification Guide*. Moreover, although the DEA and Criminal Division worked on a joint classified program, the Criminal Division did not consult the DEA when it developed a security classification guide for this specific program, and the DEA, therefore, did not use this classification guide in determining the classification of information derived from the joint DEA-Criminal Division classified program.

Our FY 2013 report also identified that poor coordination on security classification guides was due to a general unfamiliarity with the purpose and importance of consistent, comprehensive, and accurate security classification guides. As a result, we recommended that SEPS ensure that DOJ components are aware of and understand how to use security classification guides. Moreover, to increase efficiency and classification accuracy, we recommended that SEPS also review all DOJ security classification guides to ensure that instructions were clear, precise, consistent, and provided derivative classifiers with sufficient information to make accurate classification decisions.

In response to our recommendation, SEPS updated DOJ's classification security and education training module to incorporate information on all available classification resources. In addition, SEPS established a Security Classification Guide Working Group to review all DOJ security classification guides to identify and resolve redundancies, inaccuracies, and inconsistencies throughout the Department. SEPS officials also coordinated with the National Security Division and USMS to incorporate necessary changes into the overall DOJ security classification guide. Following this coordination, the USMS rescinded its security classification guide and along with the National Security Division began using the *DOJ National Security Information Security Classification Guide*.

Although SEPS planned for the Security Classification Guide Working Group to accomplish the holistic review of all DOJ classification guides by June 2015 that did not occur and SEPS assigned one of its staff members the task of managing the classification guide review. However, in January 2016, SEPS suspended all activities related to the classification guide review in order to refocus its efforts to address similar review requirements promulgated for a Fundamental Classification Guidance Review. In accordance with EO 13526, the DOJ, along with all Federal agencies with significant classification programs, must conduct a Fundamental Classification Guidance Review on a periodic basis to ensure that classification guidance is current, limits classification decisions to the minimum necessary to protect security information, and supports the declassification of information that no longer requires protection. Therefore, by June 30, 2017, DOJ must examine recent classification decisions to determine if these decisions reflect the intent of the guidance as to what is classified and if the decisions contain the appropriate markings and declassification dates. SEPS officials stated that they will, again, utilize the Security Classification Management Working Group to complete the Fundamental Classification Guide Review and implement our recommendation. We will continue to monitor SEPS's efforts in this area.

In addition, SEPS officials stated that they intend to update the current *DOJ National Security Information Security Classification Guide* and use the FBI's *National Security Information Classification Guide* as a template to develop a new DOJ-wide guide. According to these officials, the FBI's guide better aligns with the requirements of the Fundamental Classification Guidance Review. In conjunction with development of a new DOJ-wide classification guide, SEPS officials stated that they plan to work with the DEA to incorporate any DEA-specific information into the DOJ-wide guide and retire the DEA's classification guide. SEPS also coordinated with the Criminal Division to determine the current and future status of its security classification guide. SEPS officials and the Criminal Division Security Programs Manager thought this guide was retired in 2014 when the Criminal Division and DEA terminated the classified program associated with the guide. However, according to Criminal Division officials who were responsible for handling outstanding issues related to the classified program, the Criminal Division classification guide was still in use for residual information and for declassification purposes. In June 2016, the Criminal Division's Security Programs Manager met with officials associated with the classified program and informed them that the classification guide should not be used and that any newly created documents should be derivatively classified based on the previously classified source documents.

We understand that the review and consolidation of all DOJ security classification guides is a significant undertaking and believe that SEPS has made progress in this area since the issuance of our first audit report. SEPS should continue to coordinate with all components through the Security Classification Management Working Group in order to ensure that classification guidance throughout the Department is relevant, comprehensive, and consistent. The OIG will coordinate with SEPS to monitor its implementation of the Fundamental Classification Guidance Review and subsequent progress associated with our

original open recommendation for SEPS to review all DOJ security classification guides.

DOJ's Classification Decisions

In our previous report, we identified that DOJ components reported a total of 4,689 original classification decisions and approximately 8.4 million derivative decisions in FY 2012.[7] Since that time, DOJ has reduced the annual number of original classification decisions to zero; the number of derivative classification decisions decreased to 7.8 million, a 7 percent reduction. SEPS officials attributed these reductions, in part, to the issuance of the OIG's 2013 audit report and SEPS's efforts to enhance its classification training program. These officials stated that DOJ classifiers are now more knowledgeable about the appropriate processes for making original and derivative classification decisions and they have increased their use of security classification guides. The following table shows the changes in classification decisions between FY 2012 and FY 2015.

[7] Classification decisions include all actions in which an OCA official initially determines that information should be classified and each time derivative classifiers incorporate, paraphrase, restate, or generate in a new form, information that is already classified.

Table 2

FY 2012 – FY 2015
DOJ Classification Divisions

Original Classification Decisions				
DOJ Component	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**
Bureau of Alcohol, Tobacco, Firearms and Explosives	0	0	0	0
Criminal Division	603	0	0	0
Drug Enforcement Administration	849	950	630	0
Federal Bureau of Investigation[8]	4	11	1	0
Justice Management Division	0	0	0	0
National Security Division	3,232	3,494	3,010	0
Office of the Inspector General[9]	0	0	0	0
U.S. Marshals Service	1	0	1	0
Total DOJ	**4,689**	**4,455**	**3,642**	**0**
Derivative Classification Decisions				
DOJ Component	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**
Bureau of Alcohol, Tobacco, Firearms and Explosives	105	39	35	21
Criminal Division	231	1,001	941	496
Drug Enforcement Administration	80,953	77,365	68,593	62,801
Federal Bureau of Investigation	8,355,880	8,694,400	8,937,150	7,683,400
Justice Management Division	54	172	743	370
National Security Division	280	1,722	3,852	5,784
Office of the Inspector General	185	3	186	6
U.S. Marshals Service	0	0	2	0
Total DOJ	**8,437,688**	**8,774,702**	**9,011,502**	**7,752,878**

Source: SEPS

The appropriate use of OCA reduces the risks of misclassifying and overclassifying information. In our FY 2013 audit, we identified DOJ components improperly classified information as "original" classification decisions, when the classification of this type of information previously had been decided. The improper use of original classification authority increases the risk that individuals could classify the same piece of information differently, resulting in the misclassification of information. We determined that the incorrect designations were made because at least some Criminal Division, DEA, and National Security Division officials were unaware of the difference between an original and derivative classification decision. We recommended that SEPS emphasize to OCA officials the importance of the standardized classification process, ensure that OCA officials understand the difference between original and derivative classification decisions, and ensure OCA

[8] The FBI had a minimal number of original classification decisions between FY 2012 and FY 2015, which is consistent with what we found during our previous audit. In addition, we noted that the FBI reduced its number of derivative classification decisions in FY 2015; however, FBI officials from the Security Division could not identify a specific reason for this reduction.

[9] Although the OIG reported derivative classification decisions during our audit period, we excluded the OIG from our review to avoid a conflict of interest.

officials properly mark classified information according to the proper requirements of the classification decisions.

In October 2013, SEPS issued a formal memorandum to DOJ components that explained the importance of understanding the differences between original and derivative classification decisions. Specifically, SEPS reinforced that an original classification decision occurs when information is first identified as posing a risk to national security if disclosed without authorization. SEPS also updated DOJ's training materials to provide clarity on the differences between original and derivative classification decisions. In addition, SEPS began an annual process of collecting acknowledgement statements from all OCA officials attesting that they understand the difference between original and derivative classification decisions and how to properly mark classified information. As a result of the revised training materials as well as the implementation of the annual collection of acknowledgement statements, we closed this recommendation in February 2015.

As shown in Figure 2 above, the Department's dramatic reduction in original classification decisions (4,455 in FY 2013 to 0 in FY 2015) demonstrates a marked shift in classification behavior throughout DOJ. SEPS officials acknowledged that DOJ OCA officials have come a long way since the OIG's FY 2013 audit. Through the annual training requirements and OCA officials' attestations, SEPS will have the ability to continue to reinforce the requirements of original and derivative classification decisions to help ensure that classified information is appropriately categorized and marked.

Dissemination Controls – Use of ORCON

Another area for improvement identified during the initial audit was the Department's inappropriate use of dissemination markings, in particular the use and understanding of the Originator Controlled (ORCON) marking. ORCON is an Office of the Director of National Intelligence (ODNI) dissemination control marking that allows originators of classified information to maintain knowledge, supervision, and control of the distribution of the information beyond its original dissemination. Further dissemination of ORCON information requires advanced permission from the originating agency, or "originator." ODNI stipulates that originators should apply ORCON to classified intelligence that clearly identifies or reasonably permits ready identification of intelligence sources and methods that are particularly susceptible to countermeasures capable of nullifying or measurably reducing their effectiveness.[10]

During our FY 2013 audit, we found that DEA offices within and outside of the Intelligence Community used the ORCON dissemination control on classified documents that did not meet the ORCON definition in the Controlled Access

[10] To supplement the Information Security Oversight Office's Marking Classified National Security Information booklet, ODNI established the Intelligence Community Authorized Classification and Control Marking Manual (Manual) through its Controlled Access Program Coordination Office (CAPCO).

Program Coordination Office Intelligence Community Authorized Classification and Control Marking Manual (CAPCO Manual).[11] In FY 2013, DEA officials explained that adding ORCON and additional warning caveats to classified work products was done to protect ongoing investigations and confidential source information. These officials justified the use of the ORCON markings and warning caveats as a way to ensure that other government agencies did not act on DEA-related information without first "deconflicting" or coordinating their operations with the DEA. However, officials noted that even with the addition of the ORCON control markings, other government agencies have misused DEA information and in some cases, this resulted in the compromise of an ongoing operation or damage to relations with a foreign nation. Therefore, including the ORCON marking and warning caveat was the DEA's attempt to better protect its information by instructing recipients to consult with the DEA before taking any action based on DEA information.

During our FY 2013 audit, a DOJ official stated that it is difficult for an agency to deal with ORCON-marked documents because it inhibits sharing of information. Moreover, this official explained that individuals may also be unaware of what the ORCON marking actually entails and people may not be following the instruction for getting authorization from the originating agency to further share the information. Accordingly, our FY 2013 report conveyed this information and acknowledged that the broad use of the ORCON dissemination marking may impede the timeliness for sharing classified information among agencies.

As a result of our findings related to the DEA's use of ORCON, we recommended that SEPS ensure that the ODNI's ORCON-specific training is promulgated to DOJ components. We also recommended that SEPS coordinate with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure the DEA's appropriate use of dissemination control markings.

In response to this recommendation, SEPS coordinated with ODNI to obtain ORCON training for DOJ components. SEPS disseminated this training to DOJ components in December 2014. On May 6, 2015, SEPS required that the DEA Security Programs Manager confirm that the DEA's use of the ORCON dissemination control marking is appropriate. On July 1, 2015, the DEA's Security Programs Manager responded to SEPS and confirmed that all DEA employees in DEA offices that handle a "significant amount" of Intelligence Community information understand the proper use and application of the ORCON dissemination control

[11] The DEA's Office of National Security Intelligence is a member of the Intelligence Community and bound by requirements of the Office of the Director of National Intelligence; no other DEA offices are part of the Intelligence Community.

marking.[12] We did not close this recommendation because SEPS did not provide evidence that it had coordinated with the DEA to verify that the DEA's use of ORCON was appropriate.

In December 2015, officials from the DEA's Office of Security Programs acknowledged that the DEA was continuing to use ORCON in the same inappropriate manner that we noted in our prior report. As a result, we met with DEA officials from the Office of National Security Intelligence who asserted to the OIG that the DEA continued to use the ORCON dissemination control despite the findings in our FY 2013 report because DEA officials believed it was the only way the DEA could protect its information. Further, DEA officials told us that between February 2015 and November 2015, the DEA attempted to work with ODNI to develop a new dissemination control marking titled "DEA Restricted." Upon its review, ODNI denied the DEA's request to create a new marking because the definition of the "DEA Restricted" marking was synonymous with the ORCON definition. Further, effectively echoing our finding in our FY 2013 report, ODNI questioned the DEA's use of the ORCON marking. Through their coordination with ODNI, DEA officials from the Office of National Security Intelligence determined that the "DEA Sensitive" marking – already an officially recognized control marking – was the most appropriate dissemination control for the information DEA was marking as ORCON.[13] Consequently, as of January 2016, the DEA's Office of National Security Intelligence ended its broad application of the ORCON marking on its classified products and implemented a process to evaluate information on a case-by-case before marking it ORCON. The DEA initially promulgated this process change through an e-mail and then, in April 2016, incorporated the policy into the DEA's Reports Officer Handbook.

DEA officials believe that the revised approach for using ORCON and the promulgation of procedures that specifically define what types of DEA-originated information shall be marked ORCON significantly reduce the likelihood for misusing the ORCON marking. Although we believe this revised approach is an improvement, the DEA must ensure that the procedures are successfully implemented to mitigate the possibility of misuse of the ORCON marking.

Further, as previously mentioned, in our FY 2013 audit we found that DEA offices outside the Intelligence Community also improperly applied ORCON to classified work products. Officials from both SEPS and the DEA's Office of Security Programs did not evaluate these DEA offices' work products. In fact, current

[12] The DEA Security Programs Manager's memorandum to SEPS specifically stated that the following DEA entities received ORCON training: the Office of National Security Intelligence, the Office of Special Intelligence, the Organized Crime Enforcement Task Force Fusion Center, the El Paso Intelligence Center, the Office of Global Enforcement, the Office of Special Projects, and the Special Operations Division.

[13] According to the DEA's National Security Information Security Classification Guide, "DEA Sensitive" is the designation applied by DEA to sensitive information or material that does not meet the criteria of causing at least "identifiable" damage to the national security as defined in EO 13526, but must nonetheless receive restricted distribution.

officials in the DEA's Office of Security Programs were not aware that DEA offices that were not members of the Intelligence Community were applying the ORCON control marking to work products. Therefore, we will continue to work with SEPS to verify complete implementation of the original recommendation related to the DEA's proper use of the ORCON dissemination control marking.

Previous Factors Contributing to Classification Deficiencies

In our previous audit, we found that the classification deficiencies we identified were often attributable to various factors associated with DOJ's implementation of its classification management program. As described below, these factors included deficiencies in DOJ's implementation of classification and control marking guidance, inadequate and inconsistent use of security classification guides, a lack of automated tools capable of improving classification processes, deficiencies in the systems infrastructure used to process and store classified information, and weaknesses in DOJ's security education and training programs.

Classification and Control Marking Guidance

During our first audit, we found that officials throughout DOJ were unaware of classification guidance and procedures. Although the *DOJ Marking Classified National Security Information* guide was available to all DOJ personnel, it did not incorporate all Intelligence Community marking requirements. In particular, officials from DOJ components that were not part of, but worked with, the Intelligence Community and received classified work products were generally unaware of ODNI's policies and procedures regarding dissemination control markings. As such, these officials did not understand the instruction or requirements for how to carry forward dissemination markings on classified products. In particular, we noted that some National Security Division officials who were responsible for administering and managing Foreign Intelligence Surveillance Act (FISA) activities lacked knowledge of the requirement for FISA markings in classified documents, as defined by the CAPCO Manual. As a result, National Security Division officials were not carrying forward those FISA-specific markings from the Intelligence Community's original source documents.

This finding led to a recommendation that SEPS ensure that all DOJ components are aware of and understand how to apply classification resources and markings, in particular, security classification guides, the CAPCO manual, and required FISA-specific dissemination controls, as appropriate. SEPS's efforts to address this recommendation DOJ-wide began with the evaluation and improvement of training materials to include the application of classification resources.[14] This recommendation remained open prior to initiating the follow-up audit because the National Security Division had not implemented a process to ensure the proper use of dissemination control markings.

[14] The Security Education and Training section below covers this area more specifically.

During our audit, we spoke to the National Security Division officials responsible for addressing FISA-specific marking requirements. In December 2015, the National Security Division coordinated with ODNI regarding this issue. ODNI opined that even though the National Security Division is not a member of the Intelligence Community, the National Security Division processes a significant amount of Intelligence Community information and should therefore, as a best practice, follow the standards laid out in the CAPCO Manual. The National Security Division has concurred with ODNI's opinion and stated that they will carry forward all FISA-specific portion markings to newly created documents. In addition, the National Security Division will have the right to use the FISA portion marking on derivative information based upon FISA material. According to National Security Division officials, this ability to add markings where necessary will ensure more clean and consistent court filings. The National Security Division has already taken several steps to facilitate the standardized use of FISA-specific portion markings, including conducting training sessions and updating templates for FISA-related documents. National Security Division officials estimated that all necessary standardization would be fully integrated by the end of the year.

Based upon the information we obtained during this follow-up audit, we found that the Department has taken and planned sufficient action to ensure that all DOJ components are aware of and understand how to apply classification resources and markings. As a result, we plan to close this recommendation.

Comprehensive Marking Instructions

Our previous audit identified that the *DOJ Marking Classified National Security Information* guide did not adequately address the various ways to properly mark and classify e-mail correspondence. In addition, there was not an overview of how to classify notes from in-person meetings or secure phone calls related to national security information. To that end, we recommended that SEPS review the *DOJ Marking Classified National Security Information* guide and incorporate comprehensive instructions for marking all types of classified products, including e-mail correspondence and meeting notes.

In June 2014, SEPS reviewed and submitted an updated classification marking guide to NARA'S Information Security Oversight Office that included instructions on how to properly classify and mark e-mails and notes taken during classified meetings and phone calls. SEPS then posted the revised guide to its DOJ Intranet site. As a result of JMD's actions, this recommendation was closed in September 2014.

During our current audit, Security Programs staff from the Criminal Division, DEA, FBI, and National Security Division stated that the changes to the marking guide provided clearer guidance on how to mark classified products. As a result of this and the implementation of the Classified Management Tool (CMT) that is discussed later in this report, these Security Programs personnel stated that they receive fewer inquiries regarding how to mark classified e-mail products and meeting notes and stated that classified e-mails are generally classified

appropriately. As a result of JMD's actions, this recommendation was closed in September 2014.

Security Classification Guide Use

As previously stated, security classification guides are instructions from OCA officials on how to properly classify information. During our FY 2013 audit, we reviewed National Security Division and Criminal Division classified documents and found that a security classification guide was not used to classify those documents. We reported that officials who created classified documents were unaware of how to use a security classification guide and did not know that DOJ had established the *DOJ National Security Information Security Classification Guide* for use by all DOJ components.

In addition, our initial audit revealed that certain requirements in the *DOJ National Security Information Security Classification Guide* were not being consistently followed by DOJ components. At the time of our first audit, the guidance indicated that classifiers were required to specifically identify the elements in the classification guide that formed the basis for the classification decision. During our reviews of classified documents, we found it difficult to determine if classification decisions were appropriate when the classification block did not identify the specific element number(s) within a security classification guide used to classify the information. These documents used a "general citation" to an entire security classification guide without specifically identifying the element, which requires a review of the entire security classification guide to determine the reason for the classification decisions. According to information we received from SEPS officials at that time, a "general cite" to the entire security classification guide should be used only when there are four or more classification guide elements that apply to the classified information.

As a result of the findings of our initial audit, the OIG concluded that JMD should ensure that all DOJ components understand how to properly use security classification guides to derivatively classify documents.[15] We recommended that SEPS reinforce to DOJ components its requirement to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four classification guide elements when multiple elements are used.

In response to this recommendation, SEPS reevaluated DOJ's requirement for citing specific item numbers when using security classification guides as the classification source. SEPS determined that DOJ would follow NARA's Information Security Oversight Office's national policy guidance, which states that the citation of a classification guide is sufficient as a source of derivative classification and the specific item number is not required. As such, in May 2015, SEPS revised the *DOJ*

[15] We discuss SEPS's actions related to increasing awareness and enhancing instructions for using security classification guides below in the section entitled Security Education and Training.

Handbook for Writing Security Classification Guides and identified the inclusion of the specific item number in the citation process as a best practice, but no longer as a requirement. Additionally, SEPS issued a memorandum to all DOJ components recommending that all derivative classifiers begin incorporating this best practice of identifying individual classification guide elements when citing a classification guide. We closed this recommendation in June 2015 as a result of SEPS's rescission of the requirement based on national policy and designation of citing security classification guide item number(s) during the classification process as a best practice. We maintain, however, that including the specific classification guide element used to classify information increases accountability for classifying information and facilitates a quicker and more effective review of classified information during the declassification process.

During our follow up audit, we learned that since the issuance of the updated *DOJ Handbook for Writing Security Classification Guides* and memorandum, SEPS had not coordinated with components to determine if any required citing the specific classification guide elements when classifying material. SEPS officials stated that they did not see a benefit in determining whether DOJ components adopted this best practice because it is not a requirement. Moreover, SEPS officials stated that they believed most components would not implement the "best practice" because citing the security classification guide, alone, is an easier process than identifying a specific item number.

Automated Classification Marking Tools

During our FY 2013 audit, we found that one of the factors contributing to classification deficiencies was a lack of an automated application that classifiers use to generate and apply classification markings to documents and e-mails. At the time of our last audit, the automated CMT was only available to the FBI and DEA for use on their classified networks because these components are the only DOJ components within the Intelligence Community. We believed that all DOJ components working with classified information could benefit from using automated classification tools to ensure that classified documents, in particular classified e-mail communications, are marked appropriately. We found that these automated tools could assist DOJ components in streamlining the process for creating standardized classified documents and, therefore, we recommended that SEPS evaluate the possibility of using automated classification tools throughout DOJ.

The Department conducted an evaluation on the feasibility of using automated classification tools in December 2013. Specifically, SEPS and members of JMD's Office of the Chief Information Officer (OCIO) developed a CMT Working Group to discuss the requirements needed to launch a pilot test of the CMT, develop guidance on its usage, and identify requirements to implement on classified computer terminals Department-wide. Throughout a 2-year period, JMD completed testing phases and gradually rolled out the CMT. The OCIO assumed responsibility for the Department-wide implementation and mandatory usage, while SEPS's involvement was limited to providing classification subject matter expertise. The

CMT became operational for all DOJ components in August 2015 and this recommendation was closed.

To follow up on this recommendation, we focused our inquiry on the initial user response and ongoing feedback of DOJ users of the CMT. We also sought to identify any issues and problems with the CMT reported by components. We found that, initially, users had trouble understanding how to use the CMT, which in part, was due to their lack of knowledge on how to mark classified information. As this initial transition period ended, DOJ Security Programs Managers provided positive feedback about the CMT. However, these officials noted that some of the continued negative feedback centered around users who were unaware of proper classification practices, inadvertently tried to bypass the CMT classification marking controls based on their preconceived and incorrect classification processes, and therefore were unable to create documents without proper classification markings. To combat these issues, SEPS designated a classification management official to conduct classification marking training sessions and to resolve any classification questions related to the use of the CMT. In addition, SEPS deployed additional CMT-specific training seminars and coordinated with the OCIO to develop a helpdesk to assist end users in troubleshooting any CMT software problems.

Because the Department has mandated the usage of the CMT, it has been widely deployed and supported by the OCIO. Officials at each of the components we spoke with said that the CMT has improved classification markings for their classified electronic products and we believe the implementation of the CMT has enhanced the DOJ's classification management program. Moreover, we believe that the CMT has increased awareness of classification procedures and provides DOJ employees with additional support in marking classified documents in an appropriate manner.

Classification Protocols and Classified Infrastructure

Previously we found that DOJ components did not always have adequate infrastructure for accessing and sharing classified national security information, as personnel had no access to a comprehensive classified systems infrastructure capable of quickly and securely communicating classified or sensitive compartmented information to all personnel who may need it. We therefore recommended that SEPS evaluate the current classified infrastructure to determine what improvements were needed for DOJ components to successfully and appropriately classify, use, and share national security information.

To that end, SEPS evaluated the Department's classified infrastructure and determined that the DOJ's classified systems provide a comprehensive classified system infrastructure capable of quickly and securely communicating classified information. However, SEPS found that some DOJ component personnel, particularly those in field offices who work with Intelligence Community agencies, might not be aware of how to communicate their classified information system needs within the Department. Moreover, SEPS identified budget limitations and

resources as the main impediments to expanding the Department's classified system infrastructure.

In December 2014, we closed this recommendation after the Department Security Officer issued a memorandum to all component Security Programs Managers to communicate the evaluation findings and request that component staff be made aware of all procedures and requirements that are needed to properly process classified information. The Department Security Officer also suggested that all components evaluate any future classified infrastructure and technology concerns and forward them to the component Chief Information Officer.

During our follow-up audit, we asked the Criminal Division, DEA, FBI, and National Security Division Security Programs Managers if they utilized their respective Chief Information Officers to voice any concerns or needs pertaining to classified infrastructure. Staff from the Criminal Division, DEA, and FBI all stated they did not identify any classified infrastructure and technology concerns. However, the National Security Division identified a concern with the implementation of the CMT and a need to improve secure information sharing among headquarters-based offices and attorneys in the field. During our audit, National Security Division officials noted that these concerns were appropriately addressed by the OCIO and SEPS and these issues were in the process of being resolved.

We believe that SEPS' evaluation of the Department's classified infrastructure and technology and the subsequent communication of the evaluation's results sufficiently addressed our prior recommendation. Additionally, by identifying component Chief Information Officers as the main point of contact for infrastructure concerns, components became more proactive in addressing individual classified infrastructure concerns.

Security Education and Training

In our FY 2013 audit, the OIG reported that many DOJ officials and personnel expressed confusion and a general lack of understanding on how to identify and properly mark classified information. Additionally, we reported that DOJ personnel indicated that when they were uncertain about how to classify and mark information, they were more likely to err on the side of caution and mark the information as classified. These issues were attributed to inadequate classification training programs that were not ensuring all personnel were aware of policies, procedures, and requirements. As a result, we recommended that SEPS work with DOJ component Security Programs Managers to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.

To address this recommendation, SEPS coordinated with the Security Classification Management Working Group to assess training requirements and find ways to enhance DOJ's classification training programs. Subsequently, SEPS revamped its training platform with updated material to provide updated guidance

on how to apply classification markings in accordance with security classification guides and information on how to access additional classification resources. On December 9, 2014, SEPS deployed the updated training to DOJ components' personnel who are authorized access to classified information, including original classification authorities, declassification authorities, security managers, security specialists, and all other personnel whose duties involved the creation or handling of classified information. We reviewed the updated training materials and found that it provides guidance on how to apply classification markings, including security classification guides, and information on where to access additional classification resources. As a result, we closed this recommendation in February 2015.

During our follow-up audit, SEPS personnel informed us that the changes in the training materials have resulted in numerous positive effects. SEPS officials stated the components have responded positively to the new training and feel that the effect of revised training is most visible in the overall transition away from original classification decisions towards more appropriately applying derivative classification decisions. Crediting in-person training sessions, SEPS officials believe relationships between SEPS and the component Security Programs Managers have improved and this development has fostered more collaboration with components on appropriate classification standards. Further, Security Programs Managers from the Criminal Division and the National Security Division concurred with SEPS's assessment that DOJ-wide training has improved and increased Departmental awareness of classification procedures.

Classification of Otherwise Unclassified Information

During our last audit, we did not find widespread over-classification in the Department. However, we found that the DEA's Office of National Security Intelligence instituted a process that we questioned as contributing to over-classification. Specifically, when disseminating intelligence reports to the Intelligence Community, DEA officials took unclassified law enforcement sensitive information, sanitized the information to exclude operational information and conceal sources and methods, and upgraded the classification of that information to Secret. A DEA official justified this practice by explaining that any compromise of this type of information may affect the DEA's operations, sources, and relations with foreign services, and would be damaging to U.S. interests. In addition, this DEA official explained that the DEA's classification practice is also based on the "mosaic theory" of classification, where individual unclassified facts can add up to classified facts when considered in the aggregate.

We questioned this process as a cause for possible over-classification because this practice allows for the same piece of information to exist as unclassified law enforcement sensitive information in a DEA case file and as classified information in a DEA intelligence report. However, in response to our inquiries, SEPS officials and DOJ's Department Review Committee, which functions as DOJ's oversight entity in resolving issues related to the implementation of EO 13526, upheld the classification status of the intelligence reports. The entities upheld the DEA's classification justification, which was based on the mosaic theory

of classification, where individual unclassified facts can add up to classified facts when looked at in the aggregate.

During our current audit, we did not find any indication of widespread over-classification, but we revisited the DEA's process for classifying intelligence reports. We determined that the DEA has recently discontinued its process of classifying all information in intelligence reports that it disseminates to the Intelligence Community. Officials from the DEA's Office of National Security Intelligence stated that they have employed a new process that requires classifiers to review all information and appropriately mark law enforcement information as unclassified in reports for the Intelligence Community. We believe that this demonstrates that the DEA has taken steps to implement more appropriate classification processes; however, in reviewing this process we continue to have some concerns.

Specifically, DEA officials from the Office of National Security Intelligence stated that if during a review of law enforcement-related information, classifiers identify information that they deem to meet the standards for classification, then they classify and mark the information in the intelligence report. However, these classifiers do not inform the originators of the information of this classification decision. Therefore, the potential for the same piece of information to exist as unclassified law enforcement sensitive information in a DEA case file and as classified information in a DEA intelligence report continues. In addition, not classifying national security information appropriately elevates the risk that the information is not adequately protected. During follow-up discussions with DEA officials, they stated that the Office of National Security Intelligence leadership will review the potential for implementing a process to notify originators when the classification level of their information is elevated. We recommend that SEPS coordinate with the DEA's Office of National Security Intelligence to ensure that its classification practices do not result in over- or under-classification.

DOJ CLASSIFICATION OVERSIGHT AND MANAGEMENT

During our FY 2013 audit, we found that DOJ had developed classification program oversight and review processes but had not successfully implemented those processes because of insufficient resources, deficient oversight, and inadequate assistance from DOJ components. In response to our recommendations, SEPS incorporated required classification policies and procedures in the DOJ Security Program Operating Manual (SPOM). SEPS also coordinated with the OCIO to improve the process for reporting and reviewing incidents of compromised classified information. In addition, SEPS revised processes for evaluating DOJ components' self-inspection reports to improve the validity of the information reported to NARA's Information Security Oversight Office. However, we found that SEPS did not implement this enhanced process consistently between FYs 2013 and 2015, which resulted in self-inspection reporting deficiencies and inaccuracies. In general, SEPS officials stated that resource constraints continue to hinder their ability to manage DOJ's classification program effectively and efficiently.

SEPS Classification Management and Oversight

During our FY 2013 audit, SEPS officials expressed concern that while Executive Order (EO) 13526, the *Reducing Over-Classification Act*, and other mandates related to classification have substantially increased SEPS's responsibilities over the past few years, SEPS has not received any additional resources to fulfill those obligations. At that time, these officials stated that the resource constraints limited the effectiveness and breadth of their oversight and management of DOJ's security and classification management program.

In July 2016, SEPS employed over 90 personnel with various oversight and operational responsibilities for DOJ's workforce of more than 120,000 employees. Within SEPS, the Office of Information Safeguards and Security Oversight oversees the Compliance Review Team and Classification Management Unit, which have primary responsibilities related to oversight of DOJ's classification management program, continue to be staffed at levels that hinder their oversight and management capabilities. Since 2013, several SEPS staff members transferred to other DOJ components and left vacancies within SEPS's Compliance Review Team and Classification Management Unit. In fact, in November 2015 the Compliance Review Team was staffed by only one person. In addition, we found that between FYs 2013 and 2015, SEPS's staffing of the Classification Management Unit fluctuated from three to five individuals. As of July 2016, the Classification Management Unit was comprised of four employees and one contractor, and the Compliance Review Team was comprised of four employees. Of those personnel, SEPS officials stated that there is only one experienced classification subject matter expert responsible for training employees in classification management, reviewing and updating all DOJ security classification guides and declassification guides, and

conducting mandatory annual declassification reviews. This official is also responsible for developing information security policy and coordinating with all DOJ Security Programs Managers on questions related to annual classification reports required by NARA's Information Security Oversight Office.

According to SEPS officials, the loss of personnel with subject matter expertise combined with the need to timely train new personnel have affected SEPS's ability to manage its classification management programs effectively. SEPS officials explained that they often have to rearrange staffing levels within operational sections and units on a reactionary basis in order to fulfill new and ongoing responsibilities. In addition, SEPS officials believe that the level of resources available to fulfill all of its classification requirements is insufficient. SEPS officials stated that all of these resource issues have led to several problems including invalidated self-inspections reports, which we discuss in further detail below; limitations on policy developments and updates; and lack of availability to coordinate with DOJ components and participate in working groups on classification practices and procedures.

We believe that the topic of SEPS's resources is relevant to future requirements related to the impending implementation of the Controlled Unclassified Information (CUI) program, which falls under SEPS's areas of responsibility. The CUI program, established in 2010 under EO 13556, is similar to the classification management program, as it requires a standardized approach to the way the Executive Branch handles unclassified information that still requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies. As the Department's CUI program manager, SEPS will be responsible for developing, managing, and providing department-wide oversight and training for appropriately handling and marking CUI material. SEPS requested additional resources to establish a CUI Office that would develop and administer the CUI policy and program within the Department. According to SEPS officials, if SEPS does not receive additional resource for the CUI program, as requested, it will have to rely on the Classification Management Unit to implement and oversee this program, as well as perform its duties for the classification management program.

Special Access Programs

A Special Access Program (SAP) is a program established for a specific class of classified information and designed to impose safeguarding requirements that exceed those normally required for information at the same classification level. During our previous audit, we identified that SEPS was unaware of the FBI and DEA participating in Intelligence Community SAPs dating back to the 1990's. As a result, we recommended that SEPS establish a policy for DOJ components to alert SEPS of their participation in SAPs that are overseen by the Intelligence Community.

To address this recommendation, SEPS revised Chapter 11 of the SPOM, entitled "Special Access Programs," to require all DOJ components to alert SEPS of

participation in any SAPs that are overseen by the Intelligence Community. The Department Security Officer then drafted a notice of this revision in a December 2014 memorandum that was distributed to all Security Programs Managers to ensure they were aware of this new requirement. We believe that by implementing and disseminating this requirement, SEPS took the appropriate actions to address this finding area and we closed this recommendation in February 2015. Additionally, according to SEPS officials, and we did not find evidence to the contrary, since our last audit DOJ components have not implemented any new SAPs, and have not begun participating in new SAPS overseen by the Intelligence Community.

Classification Program Reporting Requirements

SEPS is required to submit to NARA's Information Security Oversight Office annual reports – self-inspections and SF-311 reports – that contain metrics on the number of DOJ original and derivative classification decisions, number of challenges to DOJ classification decisions, number of DOJ employees who received classification training, and the associated costs of maintaining DOJ classified information. During our previous audit, we found that SEPS relies on DOJ components to self-report the above information, but did not always verify the accuracy of the information reported. Consequently, if components submit inaccurate information to SEPS that is then incorporated into the annual reports for NARA's Information Security Oversight Office, the resulting DOJ annual reports do not provide a complete and accurate picture of the classification program.

Of particular concern was components' incorrect execution of the self-inspection process to include methodological errors, which resulted in inaccurate and incomplete information related to classification management. Although SEPS officials were aware of these discrepancies, SEPS officials told us that resource constraints inhibited its ability to follow-up with DOJ components to obtain appropriate, accurate, and complete information. During our previous audit, SEPS began hosting monthly focus meetings for Security Programs Managers on the self-inspection process and requirements. To complement this initial improvement, the OIG recommended that SEPS evaluate its oversight of the self-inspections process to ensure that DOJ improves the reliability of information submitted to NARA's Information Security Oversight Office.

Following our audit, SEPS continued its training efforts and implemented a process to coordinate with DOJ components to verify the validity and completeness of the information contained in the self-inspection reports. In addition, in April 2014, the Department Security Officer issued a memorandum to all DOJ Security Programs Managers that provided an overview of the top trending issues identified in the self-inspections reports. As a result of SEPS's updated process and evaluation efforts, we closed this recommendation in September 2014.

During our follow-up audit, however, we reviewed annual self-inspection reports compiled by SEPS and identified that between FYs 2013 and 2015 SEPS continuously changed its process for reviewing and analyzing these reports. As a result, the methodology used to review the reports was inconsistent, which reduces

the value of continuity in identifying both new and ongoing problems. We also found discrepancies in components' FYs 2014 and 2015 inspections reports. For example, the Criminal Division identified in both FYs 2014 and 2015 that it did not perform a classification document review, as required. Therefore, the Criminal Division reports did not include information related to the appropriateness, accuracy, and completeness of classification decisions and markings.

In addition, our review of self-inspection reports during our current audit also revealed that prior to its FY 2015 report, the DEA's submissions included inaccurate information related to classification training. According to the individual who performed the DEA's FY 2015 self-inspection, the DEA's FY 2015 report contained more complete and accurate information than previous reports. In its FY 2014 report, the DEA reported that it provided initial security training to 100 percent of its employees with security clearances. In FY 2015, the DEA reported that it provided this training to 42 percent of employees with security clearances. This individual stated that the FY 2015 submission was based on a thorough assessment of the DEA's dissemination of classification training. Further, although he could not directly speak to the accuracy of the FY 2014 report, he stated that the DEA has never developed or implemented initial security training for new employees who are non-core personnel and, therefore, the DEA cannot have a 100 percent completion rate, which was the rate reported in FY 2014.[16]

We believe that the inconsistencies found in the DEA's FY 2014 and 2015 reports are an indication that SEPS has not continued its thorough review of components' self-inspections reports to ensure their accuracy and completeness. Similar to its response in our previous audit, SEPS officials explained that each component has the responsibility to report accurate information and Security Programs Managers are expected to ensure that they have a proper understanding of the self-inspections requirements. Moreover, SEPS officials stated that responsibility for the review of self-inspections reports has shifted to different SEPS staff members due to resource fluctuations and staff turnover. Thus, the review process that SEPS implemented in FY 2013 has not remained consistent and has resulted in varying levels of review of DOJ components' submissions.

SEPS officials noted that ideally they would like to proactively manage the self-inspections program by conducting one-on-one training sessions with Security Programs Managers, assisting components with certain aspects of the self-inspections process, and performing trend and multi-year comparison analysis. These officials believe that this proactive approach would improve the DOJ's classification management program, but stated that they would need more resources to assign to the review. We understand SEPS's concerns regarding their limited resources and appreciate their ideas on how to improve the self-inspections process, if given more resources. However, with any level of resources, we believe that SEPS must remain vigilant and consistent in its oversight of the self-

[16] The DEA's non-core personnel consist of attorneys, professional/administrative staff, technical/clerical staff, and investigative technology staff.

inspections process in order to continuously ensure that DOJ provides NARA's Information Security Oversight Office with an accurate, reliable, and complete overview of DOJ's classification management program.

Oversight of Compromised Classified Information

The DOJ SPOM sets the policies and procedures for components to conduct and report to SEPS any inquiries into reported loss, possible compromise, or unauthorized disclosure of classified information. During our FY 2013 audit, we reported that the FBI had experienced a compromise of Top Secret information and that the FBI did not report the event to SEPS. The FBI attributed this situation to limited resources and lack of an enhanced, automated, and standardized reporting system at the time of the incident. We noted that the discrepancy was also due, in part, to the FBI's Security Programs Manager not following specific requirements and recommended that SEPS review the DOJ components' procedures for and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS.

To address this recommendation, SEPS conducted a review of the security incident reporting policies and drafted new DOJ-wide instructions mandating more expansive incident-reporting requirements and in-depth coordination between Security Programs Managers and the DOJ OCIO. In addition, in December 2014 the Department Security Officer disseminated a memorandum to all Security Programs Managers to reinforce the importance of reporting classified information compromises. SEPS also held training sessions to educate the DOJ Security Programs Managers on the updated security incident reporting requirements. As a result of these actions, we closed this recommendation in February 2015.

During our current audit, we spoke with component Security Programs officials and SEPS personnel about changes to the incident reporting process. SEPS officials reported seeing a consistent number of incidents and noted they typically look for overarching trends in the reported data that may indicate a need for additional or expanded training in specific areas. For instance, in reviewing multiple incident reports, SEPS identified that a DOJ component had an insufficient process for destroying classified computer hard drives and worked with the component to rectify this issue. We believe that SEPS has taken appropriate action to increase awareness of security reporting requirements and to improve component reporting of classified information compromises.

DOJ Implementation of Regulatory Requirements

During our previous audit, we identified that SEPS is responsible for ensuring that policies and procedures comply with all regulations and federal requirements. However, we noted that SEPS did not adequately address the following requirements of EO 13526: (1) prohibition of retribution for challenging the classification of information; (2) a process of transferring ownership of classified information with a transfer of functions; (3) incorporation of classification management into performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials; and (4) publication of the updated

Mandatory Declassification Review process in the Federal Register. We also recommended that SEPS incorporate in the SPOM a reference to the procedures DOJ components are required to follow when transferring ownership of classified information.

In January 2014, SEPS updated the SPOM to include language for the prohibition of retribution for challenging the classification of information and a discussion on the process of transferring classified information from one agency to another when a transfer of functions occurs. As a result, we closed this recommendation in February 2015. However, during our follow-up audit, we found two areas that still require attention: integrating classification management into employee performance plans and publishing declassification procedures.

In FY 2013, SEPS officials stated that they instructed component Security Program Managers to incorporate classification management into the performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials. However, through our reviews of self-inspections reports, we found that not all DOJ components have incorporated classification management into their performance evaluations, as instructed. Of particular concern, the Criminal Division, which was included in our last audit because of the significant amount of classified documents it creates, has not included classification management in performance work plans for all OCA officials and derivative classifiers. When we addressed this with SEPS officials, they stated that proper incorporation of classification management in performance plans and evaluations is a DOJ-wide issue, not just a Criminal Division deficiency. We recommend that SEPS develop a process to ensure that DOJ components incorporate classification management elements in such performance plans and evaluations.

Our first audit report identified that EO 13526 requires the heads of agencies that originate or handle classified material publish regulations in the Federal Register. We reported that DOJ did not publish updated procedures for the Mandatory Declassification Review process. When we previously spoke with SEPS officials about this deficiency in May 2013, these officials stated they were working to publish the updated version of DOJ's Mandatory Declassification Review process in the Federal Register by September 2013. However, as of June 2016, SEPS had not fulfilled this requirement. SEPS told us that it has drafted the updated Mandatory Declassification Review process and, according to officials, once the draft language is approved by JMD's Office of General Counsel and the Office of Records Management Policy, SEPS will publish it in the Federal Register. Due to the delay in implementing this requirement and to ensure compliance with EO 13526, we recommend that SEPS publish the updated Mandatory Declassification Review process in the Federal Register before the end of FY 2016.

CONCLUSIONS AND RECOMMENDATIONS

As we have identified throughout this report, DOJ has made several improvements to its classification management program. In general, we found that DOJ, through SEPS, is more effectively administering classification policies and procedures, and has improved its oversight and management of the classification management program. This is exemplified in DOJ reducing the number of officials with OCA from 63 in FY 2013 to 45 in FY 2016 and eliminating the number of original classification decisions from 4,455 in FY 2013 to 0 in FY 2015. Additionally, SEPS has updated classification training, guidance, and improved communication; implemented the CMT; promulgated procedures for challenging classification decisions; and enhanced the process for reporting incidents of compromised classified information. With these improvements, we believe DOJ personnel now have a better understanding of classification policies and procedures, are applying appropriate procedures to their classification decisions and are more accurately marking classified work products.

However, we also found areas in which DOJ still needs to improve its classification procedures and practices. For example, SEPS has not completed its review of classification guides in use in throughout DOJ as we recommended in our FY 2013 report. In addition, SEPS has not thoroughly evaluated the DEA's use of the ORCON dissemination control marking to ensure appropriateness, and we found that the DEA may be implementing classification practices that result in the under- or over-classification of information. SEPS also has been unable to implement consistently its enhanced process for reviewing component self-inspection reports. Additionally, although SEPS stated that it issued a memorandum to all components requiring the incorporation of classification management into the performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials, we found that not all DOJ components have done so. Finally, DOJ did not publish updated procedures for the Mandatory Declassification Review process, as required by EO 13526.

We reported in FY 2013 that deficiencies reported in DOJ's classification management program were in part due to staffing resource constraints within SEPS. In our current audit, SEPS officials have continued to identify resource constraints as a hindrance to effectively managing DOJ's classification management program. We believe that this situation may be further complicated by the impending expansion of SEPS's responsibilities to launch and oversee DOJ's efforts related to the new government-wide CUI program.

As a result of SEPS's actions, we closed, or plan to close, 12 of the 14 recommendations identified in our previous audit and will coordinate with SEPS on the two recommendations that remain open. Based on our current audit findings, we make three additional recommendations to SEPS to further help it improve DOJ's classification management program and implementation of classification procedures. Specifically, we recommend that SEPS:

1. Coordinate with the DEA's Office of National Security Intelligence to ensure its classification practices do not result in over- or under-classification.

2. Develop a process to ensure that all DOJ components include classification management elements in the performance plans and evaluations for OCA officials, derivative classifiers, and security program officials.

3. Publish the updated Mandatory Declassification Review process in the Federal Register to ensure compliance with EO 13526.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of internal controls related to classification management within the Justice Management Division, FBI, DEA, Criminal Division, and National Security Division was *not* made for the purpose of providing assurance on the component's internal control structures as a whole. The management of these DOJ components is responsible for the establishment and maintenance of internal controls.

During our previous audit, we identified internal controls deficiencies within SEPS's oversight of DOJ's classification management program. We found that SEPS lacked the controls necessary to effectively oversee DOJ components' compliance with certain classification reporting requirements and their implementation of security classification procedures. As noted in the Audit Findings section of this report, we identified that SEPS has improved its oversight of DOJ's classification management program to include enhanced internal control procedures related to security training and education and implementation of classification requirements and processes. SEPS reported that, due to resource constraints, it continues to experience difficulties in executing internal control procedures over self-inspections and classification reporting requirements. As a result, SEPS is not consistently ensuring that all reportable classification information is complete and accurate.

Because we are not expressing an opinion on internal control structures as a whole for the Justice Management Division, FBI, DEA, National Security Division, or Criminal Division this statement is intended solely for the information and use of the DOJ components involved in this audit. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards* we tested, as appropriate given our audit scope and objectives, records, procedures, and practices, to obtain reasonable assurance that the management of the Justice Management Division, FBI, DEA, Criminal Division, and National Security Division complied with federal laws and regulations for which noncompliance, in our judgment, could have a material effect on the results of our audit. The management of these components is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that concerned the operations of the auditee and that were significant within the context of the audit objectives:

- Public Law 111-258 (2010), *The Reducing Over-Classification Act*
- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- 32 C.F.R. Part 2001 and 2003, Part V Classified National Security Information; Final Rule (2010)

Our audit included examining, on a test basis, the auditees' compliance with the aforementioned laws and regulations that could have a material effect on these DOJ components' operations. We accomplished this task by reviewing classification policies, procedures, and practices; identifying and analyzing documentation related to classification management, including training programs and self-inspection reports; interviewing personnel who oversee classification programs and who are responsible for classifying information. Nothing came to our attention that caused us to believe that the Criminal Division, DEA, FBI, JMD, and National Security Division were not in compliance with the aforementioned laws and regulations.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

In FY 2013, the OIG conducted an audit, as mandated by Congress to evaluate DOJ's policies and procedures implemented for its classification management program. Specifically, Public Law 111–258 (2010), the *Reducing Over-Classification Act* required that:

> The Inspector General of each department or agency of the United States, with an officer or employee who is authorized to make original classifications, shall carry out no less than two evaluations of that department or agency or a component of the department or agency to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within such department, agency, or component; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

Through this act, Congress also mandated that the DOJ OIG conduct a second evaluation to assess DOJ's progress made pursuant to the results of the first evaluation. To accomplish this task, we evaluated DOJ's progress in implementing the 14 recommendations we issued in our first audit report and assessed the impact and overall effectiveness of DOJ's progress on its classification management program.

In addition, during the FY 2013 audit, we participated in an Inspectors General Working Group to ensure that we fulfilled the Act's mandate to coordinate with other Inspectors General in order to follow a consistent methodology in performing the initial audit. During this follow-up audit, we continued to participate in the Working Group, but generally concentrated our review on DOJ's execution of changes made as a result of our recommendations.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our objectives, we conducted interviews with headquarters-based officials from the Criminal Division, DEA, FBI, Justice Management Division, and National Security Division. For our FY 2013 report, our testing included a review of classified documents created by these DOJ components because their classification decisions comprised a substantial proportion of all

classification decisions made by DOJ components with an OCA official. For this second audit, our testing included analyzing classification reports from these same components to identify any macro-level changes between FYs 2013 and 2015 that occurred since our first audit. In addition, we reviewed and analyzed updated classification guidance, instruction, and training introduced to DOJ following our previous audit and examined DOJ's implementation of the Classification Management Tool.

Finally, as described in our first audit report, the OIG has an OCA official and, at the time, reported derivative classification decisions; however, we excluded the OIG from our audit to avoid a conflict of interest. The exclusion of the OIG from our audit work did not affect the results of our first audit because the OIG was not one of the top four DOJ components to make classification decisions. Because we excluded the OIG from our initial audit, we did not have any follow-up work to accomplish in this audit.

APPENDIX 2

PRIOR AUDIT RECOMMENDATIONS

Recommendations	Status	Page
1. Explain to DOJ components the importance of reducing the number of OCA officials and have DOJ components re-examine their number of OCA officials.	Closed	4-5
2. Review all DOJ security classification guides and work with Security Programs Managers and OCA officials to identify and reduce redundancies and to ensure that instructions are clear, precise, consistent, and provide derivative classifiers with sufficient information to make accurate classification decisions.	Open	6-7
3. Work with DOJ component Security Programs Managers to ensure that OCA officials understand the difference between original and derivative classification decisions and properly mark classified information according to the proper requirements of the classification decisions.	Closed	9-10
4. Ensure that ODNI's ORCON-specific training is promulgated to DOJ components once it is issued and coordinate with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure that DEA's use of dissemination control markings is appropriate.	Open	10-12
5. Ensure that all DOJ components are aware of and understand how to apply classification resources and markings, in particular, security classification guides, the CAPCO manual, and required FISA-specific dissemination controls, as appropriate.	Open	12-13
6. Review the DOJ Marking Classified National Security Information guide and incorporate comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes.	Closed	14
7. Reinforce to DOJ components its requirement to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four line items when multiple line items are used.	Closed	15-16
8. Evaluate the possibility of using automated classification tools throughout DOJ.	Closed	16-17
9. Determine what classified infrastructure enhancements are needed for DOJ components, in particular those DOJ components with field offices that work with Intelligence Community agencies, to successfully use and share appropriate types of classified information.	Closed	17-18

10.	Work with DOJ components to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.	Closed	18-19
11.	Establish a policy for DOJ components to alert SEPS to participation in SAPs that are overseen by the Intelligence Community.	Closed	22-23
12.	Evaluate its oversight of the self-inspections process to ensure that DOJ improves the reliability of information in its reports to NARA's Information Security Oversight Office.	Closed	23
13.	Review DOJ component's procedures for reporting compromises of classified information and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS.	Closed	25
14.	Incorporate in the SPOM a reference to the procedures DOJ components are required to follow when transferring ownership of classified information.	Closed	25-26

JUSTICE MANAGEMENT DIVISION'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Washington, D.C. 20530

AUG 2 2 2016

MEMORANDUM FOR JASON R. MALSTROM
ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL

FROM: Lee J. Lofthus
Assistant Attorney General
for Administration

SUBJECT: Follow-up Audit of the Department of Justice's Implementation of National Security Information Classification Requirements

This responds to your July 27, 2016 memorandum requesting the agency's official response to the subject report. The sensitivity review and management representation letters will be provided under separate cover by the Department Security Officer. Below are specific comments and proposed corrective actions to the recommendations.

1. **Coordinate with the Drug Enforcement Administration (DEA) Office of National Security Intelligence to ensure its classification practices do not result in over or under classification.**

   Agree. The Security and Emergency Planning Staff (SEPS) continues to work with the DEA Office of National Security Intelligence (ONSI) to address classification management requirements. Additionally, as required by the National Archives and Records Administration, Information Security Oversight Office, every Department of Justice (DOJ) component with an Original Classification Authority (OCA) will undergo a Fundamental Classification Guidance Review (FCGR) during Fiscal Year 2017. This review will include the DEA ONSI. The objective of the FCGR is to ensure classification guidance is up-to-date and reflects current circumstances. The FCGR will ensure agency guidance keeps classification to the minimum necessary and supports the declassification of information that no longer requires protection. The results of the completed FCGR will be reported to ISOO by June 30, 2017.

2. **Develop a process to ensure that all DOJ components include classification management elements in the performance plans and evaluations for OCA officials, derivative classifiers, and security program officials.**

   Agree. I will issue a memorandum to heads of department components reminding them of the Executive Order 13526 requirement to ensure that performance contracts or other systems used to rate personnel include the designation and management of classified information as a critical element or item to be evaluated in the rating of: original classification authorities; security managers or security specialists; and all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

3. **Publish the updated Mandatory Declassification Review process in the Federal Register to ensure compliance with Executive Order 13526.**

   Agree. On June 2, 2016, SEPS submitted a draft DOJ Mandatory Declassification Review Instruction to the Office of Records Management Policy (ORMP). SEPS will continue to coordinate the draft instruction through the ORMP Directives Management Program. Upon successful DOJ coordination and publication, SEPS will submit a draft Federal Register update to the Justice Management Division, Office of General Counsel for publication by December 30, 2016.

I appreciate the opportunity to comment on the report and convey the steps being taken to implement your recommendations. Should you have any questions or require additional information, please contact James L. Dunlap, Department Security Officer, at (202) 514-2094.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The Office of the Inspector General (OIG) provided a draft of this audit report to the Justice Management Division (JMD). JMD's response is incorporated in Appendix 3 of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendations:

1. **Coordinate with the Drug Enforcement Administration (DEA) Office of National Security Intelligence to ensure its classification practices do not result in over or under classification.**

   Resolved. JMD concurred with our recommendation. JMD stated in its response that the Security and Emergency Planning Staff (SEPS) would continue to work with the DEA Office of National Security Intelligence to address classification management requirements. JMD also stated that as required by the National Archives and Records Administration, Information Security Oversight Office, every Department of Justice (DOJ) component with an Original Classification Authority (OCA), to include the DEA Office of National Security Intelligence, would undergo a Fundamental Classification Guidance Review (FCGR) during fiscal year 2017. The objective of the FCGR is to ensure classification guidance is up-to-date and reflects current circumstances. JMD's response further stated that the FCGR would ensure agency guidance keeps classification to the minimum necessary and supports the declassification of information that no longer requires protection.

   This recommendation can be closed when we receive evidence that SEPS coordinated with the DEA Office of National Security Intelligence to ensure its classification practices do not result in over or under classification. In particular, SEPS should coordinate with DEA leadership to review the potential for implementing a process to notify originators when the classification level of their information is elevated.

2. **Develop a process to ensure that all DOJ components include classification management elements in the performance plans and evaluations for OCA officials, derivative classifiers, and security program officials.**

   Resolved. JMD concurred with our recommendation. JMD stated in its response that they would issue a memorandum to DOJ components reminding them of the Executive Order 13526 requirement to ensure that systems used to rate personnel include the designation and management of classified information as a critical element or item to be evaluated. These critical elements should be included when rating original classification authorities, security managers or security specialists, and all other personnel

whose duties significantly involve the creation or handling of classified information or who regularly apply derivative classification markings.

This recommendation can be closed when we receive evidence that a process was developed to ensure all DOJ components include classification management elements in performance plans and evaluations for OCA officials, security program officials, and derivative classifiers.

3. **Publish the updated Mandatory Declassification Review process in the Federal Register to ensure compliance with Executive Order 13526.**

Resolved. JMD concurred with our recommendation. JMD stated in its response that SEPS submitted a draft DOJ Mandatory Declassification Review Instruction to DOJ's Office of Records Management Policy on June 2, 2016. Upon successful DOJ coordination and publication, SEPS will submit a draft Federal Register update to JMD's Office of General Counsel for publication by December 30, 2016.

This recommendation can be closed when we receive evidence that the updated Mandatory Declassification Review process is published in the Federal Register.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig