OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-SI-16-43 | Office of Audits | September 2016

Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information

SECURITY AND INTELLIGENCE DIVISION

OIG HIGHLIGHTS

AUD-SI-16-43

What OIG Evaluated

In March 2013, the Office of Inspector General (OIG) reported[a] that the Department of State (Department) had generally adopted classification policies, procedures, rules, and regulations prescribed by Executive Order 13526.[b] However, in that report, OIG identified instances where the Department did not effectively follow and administer certain requirements.

The objective of this compliance follow-up review was to determine whether the actions taken by the Bureau of Administration and other responsible bureaus fully addressed the deficiencies identified in the March 2013 report. OIG conducted this review pursuant to the Reducing Over-Classification Act of 2010.[c]

What OIG Recommends

OIG is modifying and reissuing one recommendation from its March 2013 report and, to advance the Department's compliance with Executive Order 13526, is making seven new recommendations. OIG received responses to the draft report from the Bureau of Administration and the Bureau of Information Resource Management (see Appendices C and D, respectively). Based on the responses, OIG considers one recommendation closed; six recommendations resolved, pending further action; and one recommendation unresolved. Management responses and OIG replies are presented after each recommendation. The Foreign Service Institute also provided general comments (see Appendix E), which OIG incorporated into the report as appropriate.

[a] OIG, *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information* (March 2013, AUD-SI-13-22).

[b] Classified National Security Information, December 29, 2009.

[c] Pub. L. No. 111-258, 124 Stat. 2648 (2010).

OFFICE OF AUDITS
Security and Intelligence Division

Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information

What OIG Found

OIG found that most of the Department's security-cleared employees had not taken the training required by Executive Order 13526. Based on training records obtained from the Foreign Service Institute, OIG found that less than 14 percent of security-cleared employees had completed the required training within the timeframe considered in this review. Moreover, only 20 percent had completed the training even one time since the outset of the training program. In addition, the Department had not implemented the sanction provision in the Executive Order that suspends an individual's classification authority until training is completed. These conditions occurred in part because the Bureau of Administration had not provided adequate guidance to the Department's bureaus specifying how the process for suspending classification authority should work. When Department employees and contractors are unaware of classification standards and no mechanism is in place to enforce training requirements, there is an increased risk that information could be incorrectly marked, misclassified, and/or improperly restricted or disseminated.

OIG also found that although the Department updated the version of the Classified State Messaging Archive and Retrieval Toolset (SMART-C), as recommended in OIG's March 2013 report, the current version allows a user to classify information as an original classifier when the user does not have that authority. Further, technical difficulties have afflicted SMART-C, which have impacted its availability on the classified email system. Both of these situations can lead to over-classification or misclassification of information. OIG confirmed that the Bureau of Administration had established a process to self-inspect its classification program, as required by Executive Order 13526. However, in a self-inspection completed in December 2014, the Bureau of Administration did not include a representative sample of all classified documents because it had not captured all classified documents during its annual count of classification decisions and had not fully determined which bureaus had collections of classified documents. In addition, Bureau of Administration officials acknowledged that they lacked the resources necessary to fully comply with the requirements of Executive Order 13526.

CONTENTS

OBJECTIVE

The Office of Inspector General (OIG) conducted this compliance follow-up review to determine whether the actions taken by the Bureau of Administration and other responsible bureaus within the Department of State (Department) fully addressed the deficiencies identified in OIG's March 2013 evaluation report.[1]

BACKGROUND

OIG undertook this second evaluation to fulfill requirements in the Reducing Over-Classification Act of 2010.[2,3] The Act requires the Inspector General of each Federal department or agency "with an officer or employee who is authorized to make original classifications" to perform evaluations "of that department or agency . . . to assess whether" the department or agency had applied and complied with classification policies, procedures, rules, and regulations. The Act was designed to address the issues highlighted by the National Commission on the Terrorist Acts upon the United States[4] about over-classification of information and to promote information sharing across the Federal Government and with state, local, tribal, and private sector entities.

Department's Shared Responsibility for Implementation of Executive Order 13526

Within the Department, the Bureau of Administration and the Bureau of Diplomatic Security (DS) share the responsibility for ensuring that the Department's classification program meets Executive Order 13526 requirements for agencies to identify and safeguard classified information. Other Department bureaus also share in the responsibilities for implementation of the Executive Order to achieve overall compliance, as shown in Figure 1.

The Bureau of Administration has the following responsibilities:

- Developing and promulgating training and guidance regarding classification and declassification of national security information.
- Maintaining the Department's self-inspection program in accordance with the Executive Order.

[1] OIG, *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information* (AUD-SI-13-22, March 2013).

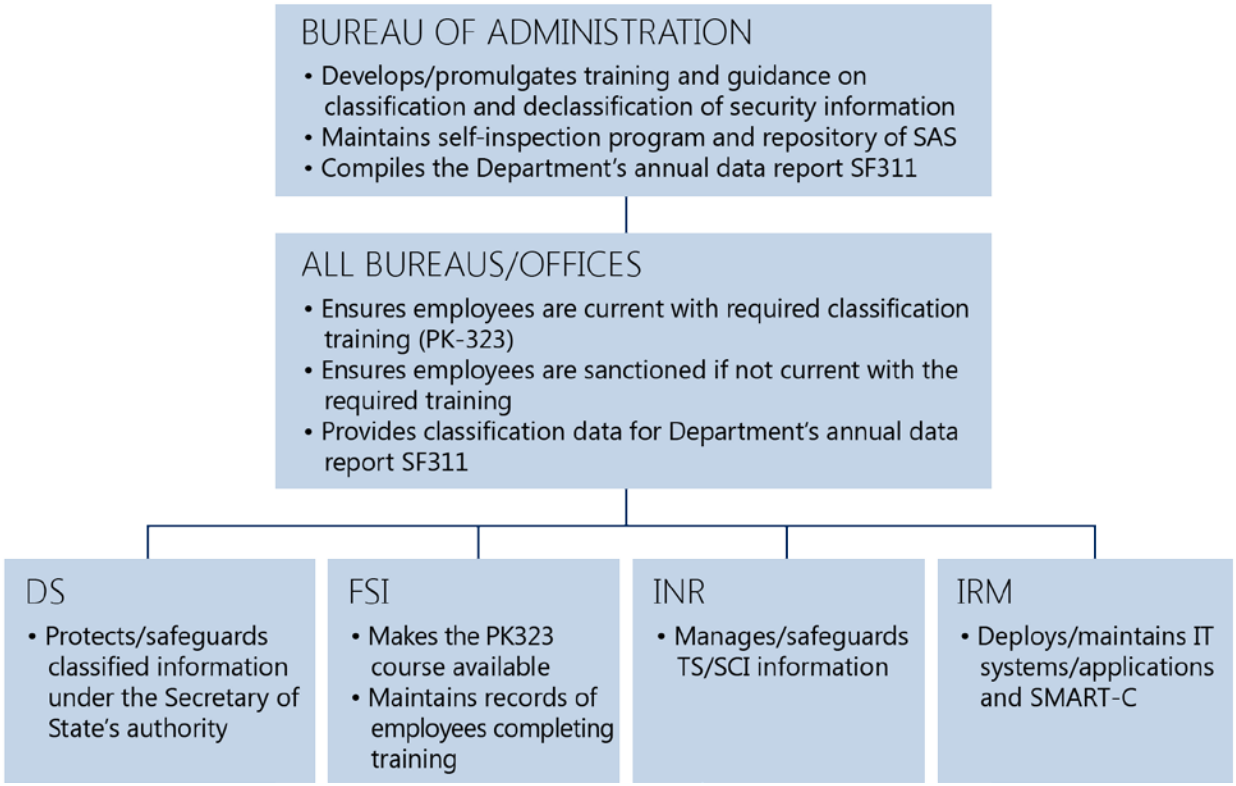
[2] Although the term "evaluation" is used, this report was scoped as a "follow-up review" and therefore is referred to as such throughout the report.

[3] Pub. L. No. 111-258, 124 Stat. 2648 (2010).

[4] The Commission is commonly referred to as the "9/11 Commission."

- Maintaining a repository of Secret and Confidential collateral[5] documents, known as the State Archiving System (SAS).
- Compiling the Department's annual Standard Form (SF) 311[6] and submitting it to the National Archives and Records Administration, Information Security Oversight Office (ISOO).

Figure 1: Department's Shared Responsibility of Implementation of Executive Order 13526



Source: OIG derived from the *Foreign Affairs Manual*.

All bureaus and offices of executive branch agencies that create and/or handle national security information are responsible for reporting annually, via SF 311, the classification management data they provided. These bureaus and offices are also responsible for ensuring that their covered employees[7] complete the prescribed training on proper classification marking (PK 323) and that, when they do not, the classification authority of those employees will be suspended.

[5] The term "collateral," as used in this context, refers to documents that do not contain sensitive compartmented information.

[6] The Agency Security Classification Management Program Data report, SF 311, is a required annual data collection report due to ISOO by November 15 of each year to provide pertinent counts regarding the Department's classification management data. Among the counts to be included in this report are the number of classification decisions made during the year and the number of Department officials with original classification authority.

[7] The term "covered employees" refers to Department of State employees with original and derivative classification authority.

DS is responsible for all aspects of protecting and safeguarding classified information created under the purview of the Secretary of State.

Three other bureaus have important supporting roles in implementing the Department's program for identifying and safeguarding classified information: the Foreign Service Institute (FSI), the Bureau of Intelligence and Research (INR), and the Bureau of Information Resource Management (IRM).

In coordination with the Bureau of Administration, FSI makes classification training available to Department employees who require it and maintains records of employees who have completed the training.

INR is responsible for the Department's program for managing, using, and safeguarding Top Secret and sensitive compartmented information. Among other related activities, INR is responsible for compiling data on classification decisions made each year within the Department by INR Information Support System (INRISS) users and providing this data to the Bureau of Administration for inclusion in the Department's annual SF 311 submission to ISOO.

IRM is responsible for deploying and maintaining information technology systems and applications throughout the Department. One application available on ClassNet[8]—known as the Classified State Messaging Archive and Retrieval Toolset (SMART-C)—enables ClassNet users to mark the classifications of Secret and Confidential emails and telegrams. ClassNet is not accredited for the storage or processing of Top Secret information or sensitive compartmented information; therefore, SMART-C is not used to process Top Secret or compartmented information.

Laws, Regulations, and Relevant Criteria

Reducing Over-Classification Act of 2010

Section 6(b) of the Act requires that the Inspector General of each Federal department or agency with an officer or employee who is authorized to make original classifications (a) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component and (b) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component. The Act established specific reporting deadlines for the Inspectors General: the first evaluation was to be completed by September 30, 2013,[9] and the second report is to be

[8] ClassNet is the Department's worldwide national security information computer network and may carry information classified at or below the Secret level.

[9] AUD-SI-13-22.

completed by September 30, 2016. The Inspectors General are also required to collaborate and coordinate with ISOO to ensure that evaluations follow a consistent methodology, as appropriate, to allow for cross-agency comparisons.

Executive Order 13526

President Barack Obama issued Executive Order 13526, Classified National Security Information, on December 29, 2009.[10] The Executive Order prescribed a uniform system for classifying, safeguarding, and declassifying national security information. It also established a monitoring system to ensure compliance with original and derivative classification policy, declassification of classified material, and safeguarding of national security information. In addition, the Executive Order outlines specific mandatory training requirements for individuals with original and derivative classification authority. The Executive Order states that the training must include instruction on the proper safeguarding of classified information.

The Implementing Directive: Code of Federal Regulations, Title 32, Section 2001, Classified National Security Information

As part of its responsibility for policy oversight of the Government-wide security classification system, ISOO published the implementing directive for Executive Order 13526 in the Code of Federal Regulations at Title 32, Part 2001, effective June 25, 2010. To fulfill its oversight responsibility, ISOO conducts on-site reviews of agency programs for classifying, safeguarding, and declassifying national security information. In addition, the implementing directive requires each designated Senior Agency Official[11] to report annually to ISOO on the agency's self-inspection program. More specifically, subpart 2001.60 of the implementing directive makes the Senior Agency Official for each department responsible for "establishing and maintaining an ongoing agency self-inspection program, which shall include regular reviews of representative[12] samples of the agency's original and derivative classification actions." The implementing directive also requires departments and agencies to report annually to ISOO data on that agency's classification activities during the year. This reporting is accomplished via SF 311. This data includes the number of original classifiers within each agency as well as the number of Confidential, Secret, and Top Secret classification decisions made within that agency during the year. ISOO combines each agency's data into Government-wide data published in an annual report to the President.

Department Guidance – The Foreign Affairs Manual

The Bureau of Administration has implemented the relevant portions of the Government-wide classification program within the Department in the *Foreign Affairs Manual* (FAM), 5 FAM 480,

[10] The Executive Order, while issued in December 2009, did not take full effect until June 2010.

[11] The Department's Senior Agency Official for classification management is the Under Secretary for Management.

[12] A representative sample is a subset of a statistical population that accurately reflects the members of the entire population.

"Classifying and Declassifying National Security Information – Executive Order 13526."[13] In addition, FSI implemented 13 FAM 370, "Mandatory Training for Classifiers of National Security Information."[14]

The FAM, 5 FAM 480, contains the policy and purpose of the Department's classification program and summarizes the scope and applicability of the Executive Order. It delineates the requirements and rationales available for use when considering whether to classify information, the responsibilities of original and derivative classifiers when creating documents that contain classified information, the levels of classification, and the marking requirements that apply to documents that contain classified information. The FAM, 5 FAM 489.1, also notes that the system used to rate personnel performance of individuals granted original classification authority and other employees whose duties significantly involve the creation of classified information include the designation and management of classified information as a critical element or item to be evaluated. Finally, it states that each Department employee and contractor is responsible for knowing and following the requirements of Executive Order 13526.

The FAM implements the Executive Order's training requirements within the Department. The FAM, 13 FAM 371a, states that Department employees with original or derivative classification authority must take training and periodic re-training regarding the proper use of their authority to identify and mark classified information: All employees who have original classification authority must take the training at least once a year, and all employees who have derivative classification authority must complete the training at least once every two years. This FAM section also gives a high-level overview of the process through which FSI, the Bureau of Administration, and each bureau's Executive Office are instructed to cooperate to ensure that each Department employee with a security clearance completes the required training.

Results of OIG's Initial Evaluation in March 2013

OIG conducted an evaluation[15] of the Department's implementation of Executive Order 13526 in response to the requirements of the Reducing Over-Classification Act and issued its report in March 2013. In that report, OIG found that the Department generally adopted the classification policies, procedures, rules, and regulations prescribed by the Executive Order but did not effectively follow and administer proper classification policies and procedures. Also, SMART-C, which enables Department employees to apply classification markings to emails and cables, required updating because the application did not have fields for derivative classifiers or drafters to enter their names and positions, as required, because the fields were accessible only to classifiers with Original Classification Authority. An outdated classification guide was also being referenced in the application. Further, the Department's self-inspection report did not fully follow requirements prescribed by the Executive Order, and the Department significantly

[13] 5 FAM 480, revised on December 11, 2015.

[14] 13 FAM 371a, revised on September 25, 2014.

[15] AUD-SI-13-22.

overstated, by as many as 2.4 million decisions, the classification decisions reported in its annual submission to ISOO. OIG made six recommendations to the Department that were intended to help the Department comply with the requirements of the Executive Order. These recommendations pertained to revising applicable regulations to enforce training requirements, updating tools that facilitate compliance with classification standards, implementing a methodology to select a representative sample of classified documents for the annual self-inspection, and establishing a process to validate[16] required submissions of data by Department bureaus. Of the six recommendations contained in the report, five were closed and one was considered resolved but remained open when this compliance follow-up review began.

OIG considers a recommendation "unresolved," "resolved," or "closed" based on the actions that management has taken or plans to take with respect to a recommendation. An unresolved recommendation is one in which management does not indicate agreement or disagreement or does not respond to the recommendation or offers an acceptable (to OIG) (1) alternative action or (2) reason for not addressing the intent of the recommendation. A resolved recommendation is one in which management has agreed to implement the recommendation or has begun to take actions but has not yet completed the actions to fully implement the recommendation. Open recommendations include both unresolved and resolved recommendations. A closed recommendation is one in which management has completed actions necessary to implement the recommendation and OIG has determined that no additional action is required.

RESULTS OF FOLLOW-UP REVIEW

Finding A: The Bureau of Administration Needs To Take Further Action To Implement the Executive Order's Suspension Provision Related to Training

Executive Order 13526[17] states that original and derivative classifiers must have training in proper classification. Specifically, all original classification authorities must receive the training in proper classification (including the avoidance of over-classification) and declassification at least once a year. The Executive Order requires that all derivative classifiers (that is, all security-cleared individuals other than those designated as original classifiers) take the security classification training at least once every two years. In addition, the Executive Order[18] states that the classification authority for all classifiers, whether original classifiers or derivative classifiers, who do not fulfill the mandatory training requirements will have their classification authority suspended until such training has been taken.

[16] To validate means to support or corroborate on a sound or authoritative basis. In this case, the authoritative basis would be ISOO's guidance: the SF 311 Agency Security Classification Management Program Data booklet.

[17] Sections 1.3(d) and 2.1(d).

[18] Requirements for suspension are covered in Section 1.3(d) for original classifiers and Section 2.1(d) for derivative classifiers.

In its March 2013 report, OIG found that although the Department had created the training course titled Classified and Sensitive But Unclassified Information: Identifying and Marking, PK 323, for security-cleared individuals within the Department to meet the Executive Order's training requirement, the Department had not identified PK 323 or any other course as a mandatory training course in the FAM. OIG also found that the Department had not fully adopted the enforcement language prescribed in the Executive Order to suspend classification authority when employees had not taken the prescribed training. Finally, OIG found that the Department had not created a method to monitor whether all security-cleared individuals within the Department had completed the required training. Based on these observations, OIG made three recommendations in its March 2013 report:

> *AUD-SI-13-22 Recommendations 1-3*
>
> ***Recommendation 1****: OIG recommends that the Bureau of Administration add the course Classified and Sensitive But Unclassified Information: Identifying and Marking (PK 323) to the mandatory training list in Volume 13 of the Foreign Affairs Manual to promote awareness of the training requirement.*
>
> ***Recommendation 2****: OIG recommends that the Bureau of Administration amend the Foreign Affairs Manual to align with the language in Executive Order 13526 that states that those individuals who fail to receive classification training "shall" have their classification authority suspended.*
>
> ***Recommendation 3:*** *OIG recommends that the Bureau of Administration, in coordination with the Foreign Service Institute, immediately establish and implement a process to identify Department of State classifiers who have not complied with the classification training requirement and to take the actions required by the amended Foreign Affairs Manual.*

In February 2015, OIG closed Recommendation 1 in response to a Bureau of Administration memorandum dated December 2014 that confirmed the publication of a revised FAM section in September 2014. Specifically, the Bureau of Administration provided a copy of the relevant FAM section[19] that added PK 323 to the list of required training courses.

In October 2014, OIG closed Recommendation 2 in response to a Bureau of Administration memorandum dated May 2014 that confirmed the publication of a revised FAM section in April 2014. Specifically, the Bureau of Administration provided a copy of the relevant FAM section[20] stating that individuals will have their classification authority suspended for noncompliance with the training requirement.

[19] 13 FAM 370.

[20] 5 FAM 488.1, "Training for Original Classification Authorities and Derivative Classifiers."

In February 2015, OIG closed Recommendation 3 in response to a Bureau of Administration memorandum dated December 2014 that described the process that the Bureau of Administration, FSI, and each of the Department's bureaus would use to identify individuals who had not completed the prescribed training in accordance with the Executive Order and to sanction noncompliant individuals accordingly. The Bureau of Administration noted that this process had been included in the FAM.[21] In its analysis of the response from the Bureau of Administration, OIG stated that the process as described in the FAM appeared to be sufficient to identify and sanction individuals who did not take the prescribed training as often as required.

Compliance Follow-Up Review Results

As described in the preceding paragraphs, the Department took action to make classification training mandatory. The Department updated the FAM and developed a process to identify Department of State classifiers who had not complied with the classification training requirement. OIG found, in this compliance follow-up review, that the Department had not emphasized the importance of the required classification training for all Department security-cleared employees until October 14, 2014, when the Under Secretary for Management sent out a Department Notice regarding the mandatory training, which was more than 3 years after the required training course was made available. OIG found that most of the Department's security-cleared employees had not taken the classification training as required by Executive Order 13526. Specifically, less than 14 percent of security-cleared employees had completed the required training within the timeframe of this evaluation.

With respect to PK323, the FAM, 13 FAM 371b,[22] states:

> The training is mandatory:
>
> (1) On an annual basis for all employees who have original classification authority; and
>
> (2) On a biennial basis for all employees who classify information by using information already classified by another source or who classify based on a classification guide (derivative classification). Any employee with a security clearance may make a derivative classification decision.

OIG obtained a list of the Department's security-cleared employees as of September 30, 2015[23], from the Bureau of Human Resources and compared that list with the lists of positions that the Department had designated as original classification authority (OCA). According to OIG's

[21] 13 FAM 370.

[22] 13 FAM 371b, "Training Mandatory for Department of State Employees," revised on September 25, 2014 (OGC).

[23] OIG selected that date as the cutoff because it corresponded closest with the FYE data reporting, with respect to the time the OIG data request was made.

analysis, 239 individuals on the Bureau of Human Resources list of security-cleared employees occupied positions that had been designated as Top Secret-level OCAs, and 671 individuals occupied positions that had been designated as Secret-level OCAs, for a total of 910 original classifiers. The Executive Order requires that OCAs take the classification training at least once per calendar year (see 13 FAM 371). OIG further identified the remaining 27,633 security-cleared individuals on the Bureau of Human Resources list as derivative classifiers, for which the Executive Order requires classification training at least once every 2 years.

To determine the degree of compliance with this requirement, OIG compared the list of security-cleared employees with a list of all PK 323 training completions maintained by FSI as of September 30, 2015. In the FAM, PK 323 is the only course identified as available for security-cleared individuals to meet the classification training requirement contained in the Executive Order.[24] For the purposes of this analysis, OIG considered an employee who occupied a position identified as OCA to be compliant with the training requirement if he or she had completed PK 323 within the 12 months up to and including September 30, 2015. For individuals who occupied positions that OIG had not identified as OCA (that is, a derivative classifier), OIG considered that employee to be compliant with the training requirement if he or she had completed PK 323 within the 24 months up to and including September 30, 2015.[25]

Of the 239 individuals who occupied positions that OIG had identified as Top Secret-level OCAs, 41 (17 percent) had completed PK 323 during the 12 months up to and including September 30, 2015. Of the 671 individuals who occupied positions that OIG identified as Secret-level OCAs, 172 (26 percent) had completed PK 323 during the 12 months up to and including September 30, 2015. Considered together, of the 910 individuals who occupied positions that OIG identified as OCAs, 213 (23 percent) had completed PK 323 in the 12 months up to and including September 30, 2015. With respect to the 27,633 individuals who occupied positions that OIG identified as derivative classifier, 3,699 (13 percent) had completed PK 323 within the 24 months up to and including September 30, 2015. Moreover, OIG's analysis determined that since the creation of PK 323 in 2011, only 20 percent of the Department's security-cleared employees had completed the course even one time.

While conducting this analysis, OIG also reviewed the list of individuals who had taken PK 323 to determine whether the Department's current[26] most senior-level officials had taken the course. OIG found that none of the individuals who occupied those senior-level positions as of September 30, 2015, had taken PK 323 at any point since the course was created in 2011.

---

[24] 13 FAM 371.

[25] As described in this report, OIG determined whether security-cleared employees had taken the required course in the 12 or 24 months, as appropriate, up to and including September 30, 2015. It is possible that, depending on the time at which they took PK323, some employees training would not be captured in this approach. A hypothetical instance would be an employee who took the course, for example, in January 2014 and again in December 2015. However, as also noted in this report, OIG found that only 20 percent of all employees required to take the PK 323 course had taken the course even one time since PK 323 was created in 2011.

[26] Current as of September 30, 2015.

According to a DS official, some or all of these officials may have received in-person security briefings or other training on protection of classified information. Nevertheless, Department guidance prescribes the completion of the PK 323 training course to fulfill the Executive Order's training requirement for all Department employees.

OIG found that the Department had revised the FAM to include PK 323 as a required course and established a process to identify classifiers who had not taken the required training for sanctioning. However, the Department had not implemented the sanction provision from the Executive Order that requires the suspension of classification authority for those individuals who do not take the required training until they have completed that training. This occurred, in part, because the Bureau of Administration had not provided adequate guidance to the Department's bureaus to specify how the process for suspending classification authority should work. Without sanctioning security-cleared individuals for failing to take the required classification training, the Department has not fully implemented the Executive Order. More importantly, when Department employees and contractors have not been trained in classification standards, the risk is increased that these employees and contractors might create and disseminate information that is incorrectly marked, misclassified, and/or improperly restricted or disseminated.

OIG found that the Department had taken steps to improve upon some of the training-related deficiencies noted in OIG's March 2013 report, but other deficiencies remained. The Bureau of Administration added initial guidance regarding training and enforcement of sanctions to 13 FAM 371. The revised FAM now requires the Department bureaus to take the following actions: (1) identify which of their employees[27] are required to take PK 323 and provide that information to the Bureau of Administration, (2) suspend the classification authority of those employees who fail to complete the prescribed training, and (3) report to the Bureau of Administration annually the names of those sanctioned employees along with a description of how the classification authority was suspended.[28]

Although as noted previously, the Department outlined in the FAM general requirements each Department bureau must follow. OIG identified shortcomings in the process outlined in the FAM. In particular, OIG noted that the FAM does not specify the following:

- Which of each bureaus' staff members should or should not be included on the list of individuals expected to take the training.
- When each bureau was expected to provide its initial list of covered individuals to the Bureau of Administration.

[27] The term "employee," as used with regard to classification training requirements in this report, encompasses all Department employees and contractors. Both Executive Order 13526 and the statutory provision that echoes and codifies the training requirement (50 U.S.C. § 435d) make the training broadly applicable. Specifically, 50 U.S.C § 438 defines "employee" as "any person who receives a salary or compensation of any kind from the United States Government, is a contractor of the United States Government or an employee thereof[.]"

[28] 13 FAM 371.

- How often each bureau was expected to provide updated lists of covered individuals to the Bureau of Administration.
- What procedures each bureau should follow to appropriately suspend the classification authority for those individuals who fail to take the required classification training as frequently as required.

Bureau of Administration officials acknowledged that they were unaware of any security-cleared employees within the Department who had been sanctioned for failing to complete the training within the appropriate timeframe.

Training for Security-Cleared Contractors

Department contractors with security clearances have the authority to classify documents derivatively and therefore are required to take the mandatory PK 323 training in accordance with Executive Order 13526 and Department policy. Bureau of Administration officials acknowledged that all security-cleared individuals working within the Department, including contractors, must receive classification training to fulfill the Executive Order's training requirement.

OIG attempted to obtain information on the number of security-cleared contractors working within the Department to determine what proportion of those contractors had received the required training. However, OIG was unable to do so because DS, which is responsible for validating security clearances for all Department personnel, including contractors, could not provide a complete list of all current Department security-cleared contractors.

According to FSI officials, contractors may enroll in FSI courses if they have a job-related need. In addition, FSI officials stated that for courses which have not been designated as "State specific," contractors may enroll only on a cost-reimbursable basis.[29] If a course is designated as State specific, FSI waives the enrollment fee for contractors. PK 323 is not designated as State specific. FSI officials stated that Bureau of Administration officials who worked with FSI to develop PK 323 did not request that the course be designated State specific. The *Foreign Affairs Handbook* states that one factor for identifying State-specific courses is that the content of the course is not available through another source. PK323 is such a course: while the general concepts related to marking classified documents may be available through another source, PK 323 demonstrates the manner through which individuals working within the Department are expected to apply these concepts through the Department's SMART system. The Bureau of Administration may want to consider working with FSI to designate PK 323 as State specific so that contractors with a job-related need can enroll at no cost. Further, to ensure that all security-cleared contractors working within the Department have a verifiable job-related need, the Bureau of Administration might request Department contracting officers to include a clause within each contract regarding the need for relevant training.

[29] FSI's tuition rate for PK 323 is $55 per enrollment.

Risk That Documents Could Be Marked Incorrectly

Without suspending the classification authority of security-cleared individuals for failing to take appropriate classification training, as required by the Executive Order, the Department has not fully complied with the Executive Order. In addition, if security-cleared Department employees and contractors have not received training in the proper marking and safeguarding of classified information, the risk that these individuals could create and disseminate classified documents that are incorrectly marked or misclassified increases.

Status

With this report, OIG is making two recommendations to address the deficiencies identified.

Recommendation 1: OIG recommends that the Bureau of Administration develop and disseminate guidance to all Department of State (Department) bureaus and offices regarding how the bureaus should meet their responsibilities outlined in the *Foreign Affairs Manual* for monitoring and enforcing the mandatory classification training requirements for all Department employees. The guidance should specify, at a minimum, how the bureaus should identify their staff members who require classification training to comply with Executive Order 13526, when each bureau's initial list of individuals who must take the required training is due to the Bureau of Administration, and how often the lists need to be updated. The guidance should also specify the procedures that each bureau must follow to sanction security-cleared individuals who do not take the required training.

Bureau of Administration Response: The Bureau of Administration concurred with this recommendation, stating that it "will update the FAM to specify that employees and contractors with a security clearance must complete classification training. The Bureau of Administration further stated, "The FAM update will include schedules for bureaus to provide initial and updated lists of covered employees to A Bureau and include language explaining that bureaus should suspend ClassNet access when employees and contractors do not complete the required training." (The Bureau of Administration's response is in Appendix C.)

OIG Reply: OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the revisions to the FAM that the Bureau of Administration identified have been completed.

Recommendation 2: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Security, develop and disseminate guidance to Department of State bureaus and offices that describes when a security-cleared contractor must take classification training required by Executive Order 13526, who will pay for the training, and how the suspension of classification authority will apply to security-cleared contractors who do not complete the required training.

Bureau of Administration Response: The Bureau of Administration concurred with this recommendation and stated: "Any contractor at the Department with a security clearance has the authority to make a derivative classification decision using either an underlying classified source document or a classification guide. Therefore, all security cleared contractors must take the classification training required by E.O. [Executive Order] 13526. A Bureau will work with Department training officials to solicit ideas on making the course available to contractors and options for covering associate costs. Procedures for suspension of classification authority for contractors will require discussion with the Office of Acquisitions and the Procurement Executive."

OIG Reply: OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Bureau of Administration has finalized the arrangements for making classification training available to security-cleared contractors, covering costs associated with contractor enrollment in the training, and sanctioning security-cleared contractors who do not take the training as often as required.

Finding B: The Bureau of Information Resource Management Needs To Take Further Corrective Action To Address SMART-C Challenges

Executive Order 13526 prescribes a uniform system for classifying national security information. The Executive Order sets forth the standard to determine the level of classification, the markings required on classified items, and the authorities used to mark classified items. The Executive Order also sets forth the framework for the ISOO implementing directive. That implementing directive states that a uniform security classification system requires that standard markings be applied to classified information. The Department chose SMART-C as a tool for facilitating the marking of classified emails on ClassNet. SMART-C was adopted by the Department in 2009 to assist classifiers in the proper marking of classified emails and telegrams.

In its March 2013 report, OIG explained that the version of SMART-C then in use (version 4.2) contributed to document-marking discrepancies that it found with respect to Confidential and Secret emails and telegrams. The discrepancies included not marking classified emails and telegrams in accordance with the document-marking standards prescribed by Executive Order 13526. The discrepancies occurred because SMART-C did not have fields for derivative classifiers or drafters to enter their names and positions. Based on this finding, OIG made the following recommendation in the March 2013 report:

AUD-SI-13-22 Recommendation 4

Recommendation 4: *OIG recommends that the Bureau of Administration, in coordination with the Bureau of Information Resource Management, replace the Classified State Messaging Archive and Retrieval Toolset (SMART-C) 4.2 application with SMART-C 5.5*

for all users of the classified email network to promote compliance with Executive Order 13526.

In March 2014, OIG closed Recommendation 4 because the Bureau of Administration coordinated with IRM and provided documentation demonstrating that IRM had fully deployed SMART-C version 5.5 to ClassNet users, which met the intent of the recommendation.

Compliance Follow-Up Results

Although IRM upgraded SMART-C to a newer version and deployed that upgrade to ClassNet users,[30] the current version of SMART-C inappropriately allows a ClassNet user to identify himself or herself as an original classifier, even when the Under Secretary for Management has not delegated such authority to that person. The FAM[31] states that information may be originally classified under Executive Order 13526 only if all conditions specified in 5 FAM 482.1b are met, including if an original classification authority is classifying the information. The situation pertaining to possible misidentification occurred because there is no mechanism within SMART-C to prevent derivative classifiers from identifying themselves as making an original classification decision. There are various methods that IRM could use to improve SMART-C to remediate the risk of an employee incorrectly identifying himself or herself as an OCA. For example, using the Joint Worldwide Intelligence Communications System email as a model, a control could be established within the application to alert the creator that OCA authority is limited to people who are designated by the President or by the agency to have OCA authority. In addition, according to Department guidance, OCA usage should be necessary only in rare instances, and when it is, only people within those positions designated with such authority can use it. The alert could also provide a link to a list of OCA personnel. Inappropriate identification as an OCA when creating and disseminating emails could lead to over-classification, incorrect declassification time limits, or misclassification of information. All of these factors could restrict public access to such information for time periods that are longer than necessary, which could result in potential violations of Executive Order 13526.

Another issue pertaining to SMART-C is that SMART-C does not remain installed within the ClassNet Outlook application. IRM has known about this problem as early as September 2012. An IRM official stated that SMART-C uninstalls because software updates conflict with different versions of the operating systems and software used within the Department. A 2015 OIG report[32] indicated that the SMART client application was still afflicted with problems and cited the uninstalling of the SMART client application as one example of the technical problems encountered by users. The report further indicated that SMART development staff had not fully understood the impact of application errors on the productivity of SMART users. IRM officials

[30] IRM officials stated that all Department bureaus have SMART-C installed except the Office of the Secretary of State, which uses a different system.

[31] 5 FAM 482.1, "Requirements for Classification."

[32] *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015).

stated that they were not able to centrally detect when SMART-C uninstalled or to notify a user when there was a loss of service. Therefore, IRM officials had to rely on each affected user to notify them of the loss of SMART-C on a case-by-case basis. This issue increases the risk that a ClassNet email user could create and send emails containing classified information that is marked improperly.

Status

With this report, OIG is issuing two recommendations to address the deficiencies related to SMART-C:

> Recommendation 3: OIG recommends that the Bureau of Information Resource Management develop and implement a control within the Classified State Messaging Archive and Retrieval Toolset that allows only individuals who occupy positions that have been designated as original classification authority to identify themselves as such when making original classification decisions.
>
> **IRM Response:** IRM concurred "that it is possible to remediate the risk of an employee incorrectly identifying himself or herself as a holder of original classification authority (OCA)." IRM further stated that in the next 7 months it would "develop, test, and implement informational alerts which will be added to the Classification Authority fields to alert the creator that OCA is limited to people who are designated by the President or by the agency and is reserved primarily for senior officers." (IRM's response is in Appendix D.)
>
> **OIG Reply:** Based on IRM's concurrence and planned corrective actions, OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that implementation of a Classified State Messaging Archive and Retrieval Toolset alert has been established that informs the user that original classification authority is limited to people who are designated by the President or by the agency and is reserved primarily for senior officers.
>
> Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement corrective actions to prevent the Classified State Messaging Archive and Retrieval Toolset from being uninstalled or, if the software becomes uninstalled, that the Bureau of Information Resource Management be notified that the software needs to be reinstalled.
>
> **IRM Response:** IRM concurred with the OIG recommendation, stating that it has "already implemented" the Classified State Messaging Archive and Retrieval Toolset Messaging Manager, which checks for the presence of the Classified State Messaging Archive and Retrieval Toolset client and automatically reinstalls it if the client is removed for any reason. IRM further stated, "This process alleviates the onus on users notifying IRM support and also eliminates the need to build in an alert mechanism."

OIG Reply: Based on IRM's concurrence with the recommendation and its implementation of corrective actions taken, as verified by OIG, OIG considers this recommendation closed.

Finding C: The Bureau of Administration Did Not Include All Classified Documents in the Samples Selected for Self-Inspections or in the Count of Classification Decisions Reported on Standard Form 311

Executive Order 13526 and the ISOO implementing directive[33] require that each department or agency conduct at least annually a self-inspection of that department's or agency's implementation of the Executive Order. Per the Executive Order, each self-inspection must include a review of a *representative* sample of the classified documents created within the department or agency. The Executive Order requires that the ISOO director compile an annual Report to the President regarding the implementation of the Executive Order throughout the executive branch. To enable this reporting, the implementing directive requires each department or agency that creates or safeguards classified information to report statistical data to ISOO each year. Among those statistical reports is an annual count of the number of classification decisions made within that department or agency each year.

In its March 2013 report, OIG stated that the Bureau of Administration had established a process and performed a self-inspection of its classification program, as required by Executive Order 13526. That report noted, however, that the self-inspection did not include a representative sample of all classified documents within the Department. This occurred because the Bureau of Administration did not have direct or timely access to the Top Secret documents held by other Department bureaus, such as INR and DS.

OIG also found in its March 2013 report that the Bureau of Administration had not accurately reported derivative classification decisions on its SF 311 report for 2011. The report noted that inaccuracies on the SF 311 report occurred because information provided to the Bureau of Administration by INR about classification decisions involving emails was overstated by as much as four times because of counting and oversight errors. In addition, the Bureau of Administration reported the data provided by INR without reviewing the submission and validating its accuracy. Based on this finding, OIG made two recommendations in its March 2013 report:

AUD-SI-13-22 Recommendations 5-6

Recommendation 5*: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Intelligence and Research and the Bureau of Diplomatic Security, develop and implement a sampling methodology that attains a representative sample of*

[33] Title 32, Code of Federal Regulations, §§ 2001.60 and 2001.90(d).

all classified documents maintained within the Department of State for its annual self-inspection of the classification program.

***Recommendation 6**: OIG recommends that the Bureau of Administration ensure that all Department of State bureaus that contribute data reported on Standard Form 311 receive and comply with guidance from the National Archives and Records Administration, Information Security Oversight Office, that pertains to validating the data submitted to the National Archives and Record[s] Administration is accurate.*

In March 2014, OIG closed Recommendation 5 in response to a Bureau of Administration memorandum dated November 2013 that confirmed that the Bureau of Administration had requested, through the Under Secretary for Management, that DS, INR, and IRM supply all information needed to complete the annual self-inspection report. The Bureau of Administration noted additionally that it later sent a memorandum to INR and DS detailing the information that INR and DS should provide. With its November 2013 response, the Bureau of Administration provided a copy of the memorandum from the Under Secretary for Management to DS, INR, and IRM and a copy of its own memorandum to DS and INR. The memorandum from the Bureau of Administration to DS and INR included a copy of ISOO's guidelines for self-inspections, as well as a copy of OIG's March 2013 report.

With respect to Recommendation 6, the Bureau of Administration agreed to implement the recommendation. Therefore, OIG considered the recommendation resolved, pending further action, when this current compliance follow-up review began.

Compliance Follow-Up Review Results

During this current compliance follow-up review, OIG affirmed that the Bureau of Administration had established a process to self-inspect the Department's classification program, as required by Executive Order 13526. However, the Bureau of Administration's sample of classified documents for the self-inspection for 2014—the most recent self-inspection that the Bureau of Administration had completed at the time OIG began its compliance follow-up review—did not include a representative sample of all classified documents within the Department. Further, OIG found that the Bureau of Administration was not capturing all of the collections of classified documents created within the Department as a part of the annual count of classification decisions and had not fully determined which bureaus had collections of classified documents for the SF 311 data submission to ISOO.

To fully comply with the Executive Order, the Bureau of Administration must determine which bureaus and offices within the Department have collections of classified documents and assist those bureaus and offices, when necessary, to develop a count of the classified documents that each pertinent bureau and office creates each year. After making the determination regarding which bureaus and offices have responsive records, the Bureau of Administration should request a report of all classification decisions made by each Department bureau each year. Further, to enable the Bureau of Administration's review of a representative sample of classified documents

for each self-inspection, all bureaus and offices that the Bureau of Administration determines have pertinent collections of classified documents should maintain repositories of the classified documents they create each year.

Bureau of Administration officials stated that they had not reached out to all bureaus within the Department to identify a complete universe of the classification decisions made because they do not have sufficient resources to allow them to take on such an initiative. For instance, given their current ongoing responsibilities with Freedom of Information Act (FOIA) request processing and other assigned duties, the officials stated that there is limited opportunity to coordinate with other bureaus to identify the universe of classification decisions.

Bureau of Administration's 2014 Self-Inspection Document Sampling Procedures

During this compliance follow-up review, OIG continued to find that the self-inspection performed by the Bureau of Administration did not include a representative sample of all classified documents within the Department. For the document-review portion of the 2014 self-inspection, the Bureau of Administration selected and reviewed 251 classified documents for proper classification and marking. The Bureau of Administration official responsible for the self-inspection document review selected a sample of 245 documents from SAS.

Although the universe of classified documents that the Bureau of Administration used for its self-inspections was incomplete, OIG selected and reviewed a judgmental sample[34] of 28 documents from among those that the Bureau of Administration had reviewed to validate the conclusions that the Bureau of Administration had reached regarding proper classification and marking during the document-review portion of the 2014 self-inspection. OIG found no reportable deficiencies related to those classified documents selected and reviewed.

Unlike the classified documents contained in SAS, the Bureau of Administration obtained a count of classified emails from INR but did not select a sample from those emails for the self-inspection. INR officials told OIG that INR did not maintain a repository of the classified emails created and sent by INRISS[35] users. As a result, the Bureau of Administration was not able to select a sample of these classified emails for the Department's self-inspection. As an alternative to selecting a sample from emails sent by INRISS users, the Bureau of Administration selected, for the 2014 self-inspection, 6 documents from among 172 classified INR documents posted on ClassNet during 2014. Two of the six INR documents selected for the self-inspection were classified as Secret, and four were classified as Confidential. None of those documents were classified as Top Secret. When asked why no Top Secret documents were selected for the self-inspection, the Bureau of Administration official responsible for the document-review portion of

[34] Judgmental sampling is a non-probability sampling technique in which documents are sampled based on the audit team's knowledge and professional judgment.

[35] INRISS is the information technology system through which authorized Department users process and store Top Secret information.

the self-inspection provided two primary reasons. He stated that DS no longer maintains a listing of the storage locations for collateral[36] Top Secret documents that are created within the Department, although such a list existed at the time of OIG's prior review. He also stated that he does not have access to INRISS, the system on which such documents can be processed electronically.

However, excluding Top Secret documents from the self-inspection does not meet the Executive Order's requirement to select and review a *representative* sample of classified documents for each self-inspection.

Collections of Information Included in 2014 SF 311 Count of Classification Decisions

OIG found shortcomings with the count of classification decisions the Bureau of Administration reported in its SF 311 report to ISOO for 2014. Specifically, the information provided by INR, which represented a count of classified emails, was an estimate that the Bureau of Administration did not validate. While ISOO's guidelines for generating the SF 311 data allow the use of estimates when counting emails, the guidelines state that it is "essential that agencies conduct a quality control check before submitting their" information to ISOO. The Bureau of Administration accepted and reported the data provided by INR without reviewing the submission and validating its accuracy. Also, the Bureau of Administration obtained data from only two Department sources without reaching out to the other bureaus and offices within the Department to determine whether they also had created classified documents during the reporting period that the Bureau of Administration should have included in the SF 311 report for 2014. For example, classified documents created within the Office of the Secretary were not included in the self-inspection or the SF 311 report.

As previously stated, for the 2014 SF 311 submission, the Bureau of Administration obtained and combined data from two sources: a count of cables and record emails contained in the SAS database and an estimate of the number of emails created in INRISS. The Department's SF 311 submission to ISOO stated that the Department made 210,846 classification decisions during the year. According to the Bureau of Administration's subsidiary information, as shown in Table 1, the overall count consisted of 56,526 classified documents (cables and record emails) contained in SAS and INR's estimate of 154,320 classified emails sent by its INRISS users.

Table 1: Department of State Classification Decisions Reported to the Information Security Oversight Office for 2014

Source and Type of Classification Decision	Top Secret	Secret	Confidential	Total
SAS Count				
Original classifications	not applicable*	9,105	8,427	17,532

[36] In this context, the term "collateral" is defined as information that is not sensitive compartmented information.

Source and Type of Classification Decision	Top Secret	Secret	Confidential	Total
Derivative classifications	not applicable*	25,237	13,757	38,994
SAS Count Total	not applicable*	34,342	22,184	56,526
INR Email Estimate				
Original classifications	48	480	192	720
Derivative classifications	76,800	68,400	8,400	153,600
INR Email Estimate Total	76,848	68,880	8,592	154,320
Overall Total	**76,848**	**103,222**	**30,776**	**210,846**

*SAS is not accredited for storage of Top Secret information.
Source: OIG-prepared based on the Department's 2014 SF 311 submission to ISOO and subsidiary information provided by the Bureau of Administration.

The first set of data that the Bureau of Administration included in the SF 311 report was a count of the classified cables and record emails contained in SAS for 2014. The Bureau of Administration official responsible for compiling the data requested and received this data from the SAS program office in the Bureau of Administration.

The second set of data that the Bureau of Administration included in the SF 311 report was an estimate from INR regarding the number of classified emails that was created and sent during the year using INRISS. The INR information technology director and a former employee of that office who developed the estimated count of emails for 2014 both stated that the estimate was derived from a live count of classified emails that were created during a 2-week period in December 2014. The former INR information technology employee stated in an email that he "believe[d] … [that INR] randomly selected someone from the [INR] [F]ront [O]ffice … [t]hen a random selection was made from the pool of division chiefs and the remaining 5 users were selected randomly from the pool of remaining users." He further wrote that he believed these users "were selected from an available pool of approximately 600 users." The INR information technology director stated that after he and the former employee obtained the raw count of classified emails, they extrapolated the raw count to make an estimate of the total number of classified emails created during the year for all INRISS users. They calculated the estimate by expanding, through multiplication, the number of users selected for the raw count to the total number of users and by expanding, again through multiplication, the 2-week total by 26 to get data covering 52 weeks. However, if INR does not maintain a repository of the emails sent by INRISS users during the year, the Bureau of Administration's ability to validate INR's estimate of the number of emails is significantly diminished.

Insufficient Guidance and Resources

Although the Bureau of Administration has made improvements with respect to the self-inspection sampling procedures and SF 311 reporting since OIG's prior report, more needs to be done to fully comply with the Executive Order's requirements. For example, the Bureau of

Administration needs to reach out to all the Department's bureaus and offices each year to determine which bureaus and offices have collections of classified documents and assist those bureaus and offices, when necessary, to develop their counts of classified documents. The starting point for this annual information-gathering process is for the Bureau of Administration to send out a formal request to all Department bureaus and overseas missions to report all classification decisions made over the past year. Further, responsible bureaus that report classification decisions must develop and maintain repositories of the classified documents they count so that the Bureau of Administration can subsequently validate the information provided. To assist with that effort, the Bureau of Administration needs to develop and disseminate guidance to all Department bureaus regarding how to create and maintain repositories of classified documents.

Officials in the Bureau of Administration office responsible for developing the SF 311 report and performing the self-inspection stated that the Bureau of Administration does not have the resources needed to fully comply with Executive Order 13526 requirements because it is also responsible for the Department's activities related to processing and responding to FOIA requests.[37] For example, the responsible Office Director within the Bureau of Administration noted that his office (Global Information Services, Office of Information Programs and Services [IPS]) was busy processing FOIA requests. Given that the individuals responsible for completing the SF 311 submission and self-inspection each year have other demanding responsibilities, the Bureau of Administration may need additional resources to fully comply with the requirements of the Executive Order. According to an internal website published by the Bureau of Human Resources, an office within that bureau has the experience and expertise to provide assistance to bureaus in determining the proper level of resources an office may need in order to complete all of its assigned responsibilities fully and effectively.

Inability To Comply With Executive Order

As a result of the deficiencies identified in this follow-up report, the Bureau of Administration will remain unable to identify a complete universe of classified documents within the Department for the annual self-inspection until additional capabilities are instituted. In addition, the SF 311 report submitted annually to ISOO will not accurately represent all of the Department's classification decisions because not all decisions are being identified or sampled as part of the Department's self-inspection program.

[37] The OIG report *Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary* (ESP-16-01, January 2016) stated that the Bureau of Administration needed additional resources to be able to complete its FOIA processing responsibilities in a timely manner.

Status

With this report, OIG is making two new recommendations and modifying Recommendation 6 from the March 2013 report to address the issues identified during this follow-up review:

> Recommendation 5: OIG recommends that the Bureau of Administration develop and implement a process to formally request and obtain, from all bureaus and offices within the Department of State, annual reports of all classification decisions made to facilitate compliance with Executive Order 13526 and with the inspection and reporting requirements contained in Title 32, Code of Federal Regulations, Sections 2001.60 and 2001.90.
>
> **Bureau of Administration Response:** The Bureau of Administration concurred with this recommendation and stated that since it "currently counts electronic classification decisions via the SMART system, counting hard copy documents will significantly increase the risk of double counting." It further stated: "Checking hard copy documents against the email archive to avoid duplication would require resources (both employees and systems) that are not currently available to the bureau. Please note that the Top Secret Control Officer Program referenced by OIG in this report, ceased to exist on October 1, 2013 (see Department Notice 2013_09_168)."
>
> **OIG Reply:** OIG considers this recommendation unresolved. Although the Bureau of Administration concurred with the recommendation, it did not state the manner in which it would develop and implement a process to formally request and obtain annual reports of classification decisions made from all bureaus and offices within the Department. Bureau of Administration officials did note in their response their concern about the adequacy of their resources that would be needed to ensure the completeness and/or accuracy of the annual data reported by Department bureaus and offices under this recommendation.
>
> This recommendation will be considered resolved when OIG receives and accepts documentation demonstrating that the Bureau of Administration plans to develop a process to implement the recommendation. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Bureau of Administration has developed and implemented such a process.
>
> Recommendation 6: OIG recommends that the Bureau of Administration develop and disseminate guidance to all bureaus and offices regarding the creation and maintenance of repositories of classified documents to facilitate the count of classification decisions reported annually in the Agency Security Classification Management Program Data form and to facilitate the review of a representative sample of classified documents during each self-inspection.

Bureau of Administration Response: The Bureau of Administration concurred with this recommendation, stating that it "will work with the Bureau of Diplomatic Security to develop guidance regarding the creation and maintenance of repositories of classified information."

OIG Reply: OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Bureau of Administration and DS have developed and disseminated the guidance noted.

Recommendation 7: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Human Resources, (a) conduct a staffing workload assessment of the Bureau of Administration, Office of Information Programs and Services, and (b) ensure that the office has, or will obtain, the adequate level of resources as determined by the assessment. The purpose of the assessment is to determine whether the Bureau of Administration has the appropriate level of resources necessary to establish and maintain an effective sustainable process for the development of the annual Agency Security Classification Management Program Data report and for sampling and reviewing classified documents required as part of a self-inspection under Executive Order 13526.

Bureau of Administration Response: The Bureau of Administration concurred with this recommendation, stating that it "will coordinate with our Executive Office for the recommended staffing workload study."

OIG Reply: OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the staffing workload assessment has been completed and that the Bureau of Administration has requested the level of resources determined by the assessment.

OTHER MATTERS

Lists of Positions Authorized To Make Original Classification Decisions Not Up To Date

The Bureau of Administration has published two lists of Department positions in which individuals are authorized to make original classification decisions. One list is for Secret-level OCAs, and the other list is for Top Secret-level OCAs. The list of Secret-level OCAs has not been updated since 2009, and the list of Top Secret-level OCAs has not been updated since 2010.

According to the OCA lists published by the Bureau of Administration, the individuals who are authorized to make Top Secret original classification decisions are generally the most senior officials within the Department. The list of Top Secret-level OCAs includes such positions as the Secretary, the Deputy Secretaries, the Under Secretaries, Assistant Secretaries or equivalent

positions, and Ambassadors. According to the OCA lists published by the Bureau of Administration, the individuals who are authorized to make Secret-level original classification decisions have less seniority within the Department than do Top Secret OCAs. Such positions include Deputy Assistant Secretaries and equivalent positions, Deputy Chiefs of Mission, and Principal Officers at consulates and consulates general.

OIG compared the lists of positions authorized as Top Secret OCAs and Secret OCAs published by the Bureau of Administration with lists of all of the security-cleared Department employees as of September 30, 2015, which OIG obtained from the Bureau of Human Resources. OIG identified 239 individuals who occupy positions in which these individuals appear to be authorized to make original classification decisions at levels up to Top Secret; OIG identified another 671 individuals who occupy positions in which these officials appear to be authorized to make original classification decisions up to the Secret level. Combined, OIG identified 910 positions that provide individuals with OCA. Conversely, the Department's SF 311 submission for 2014 identified the number of positions for individuals authorized as OCAs as 262 Top Secret OCA positions and 737 Secret OCA positions, for an overall total of 999 OCA positions. This is the same count of OCA authorized positions that has been reported by the Department over the past 4 years, since 2011. The difference between the Department's count and OIG's count of OCA positions (89 [999 minus 910]) is attributable, in part, to the changes in the organizational structure and staffing of the Department's bureaus over that same time period.

Several of the Department's bureaus have been restructured since the lists of Secret-level OCA and Top Secret-level OCA positions were last updated in 2009 and 2010, respectively. For example, the Department created the Bureau of Counterterrorism and Countering Violent Extremism, which was previously the Office of the Coordinator for Counterterrorism. Another bureau identified on the OCA lists was split into two distinct organizations within the Department: the former Bureau of Resource Management was split into the Bureau of Budget and Planning and the Bureau of the Comptroller and Global Financial Services. Other changes occurred within bureaus. For example, DS officials advised OIG that four Assistant Director positions were elevated to the Deputy Assistant Secretary level. All of these modifications would change the number of OCA positions within the Department. Since the OCA lists have not been updated, these changes, among others, were not reflected on the OCA lists maintained by the Bureau of Administration.

Through Executive Order 13526, the President granted the Secretary of State the authority to make the determination regarding which employees and/or positions within the Department would be authorized to have original classification authority. Further, the Executive Order[38] states:

[38] Executive Order 13526, Section 1.3(c)(1), "Delegation of Original Classification Authority."

> Delegations of original classification authority shall be limited to the minimum [number of individuals] required to administer this [Executive] order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this [original classification] authority.

The need to periodically review and update policy-related documents, including OCA lists, is emphasized in the Government Accountability Office's *Standards for Internal Control in the Federal Government,*[39] which states that good management controls call for the periodic updating of information to keep it current and accurate.

The Bureau of Administration's standard operating procedures related to implementing the Executive Order do not address keeping the lists of OCA positions up to date. Establishing a process to periodically review and update (as necessary) the OCA lists appears warranted considering the number of changes in the structure of bureaus and offices that occur over time. Outdated OCA lists fail to inform Department personnel of the positions within the Department in which personnel are authorized to make original classification decisions. In addition, the existing, out-of-date OCA lists may identify positions in which personnel are being authorized to make original classification decisions when those positions no longer exist. Since the Under Secretary for Management is the Department's designated Senior Agency Official for classification management and has the authority to delegate OCAs, his office would need to be aware of and involved in any periodic process to review and, as necessary, update OCA designations.

> **Recommendation 8:** OIG recommends that the Bureau of Administration, in coordination with the Under Secretary for Management, develop and implement a standard operating procedure for periodically reviewing and updating the lists of positions in which personnel are authorized to make original classification decisions to ensure that these lists are current and accurate.
>
> **Bureau of Administration Response:** The Bureau of Administration concurred with this recommendation, stating that it "will develop a process to review the lists of positions designated as Original Classification Authorities on an annual basis and will seek the approval of the Under Secretary for Management when the Secret level OCA list requires updating and the Secretary of State when the Top Secret level OCA list requires updating."
>
> **OIG Reply:** OIG considers this recommendation resolved. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Bureau of Administration has developed and implemented the standard operating procedures.

[39] GAO-14-704G, September 2014, Principle 9, "Identify, Analyze, and Respond to Change."

RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Administration develop and disseminate guidance to all Department of State (Department) bureaus and offices regarding how the bureaus should meet their responsibilities outlined in the *Foreign Affairs Manual* for monitoring and enforcing the mandatory classification training requirements for all Department employees. The guidance should specify, at a minimum, how the bureaus should identify their staff members who require classification training to comply with Executive Order 13526, when each bureau's initial list of individuals who must take the required training is due to the Bureau of Administration, and how often the lists need to be updated. The guidance should also specify the procedures that each bureau must follow to sanction security-cleared individuals who do not take the required training.

Recommendation 2: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Security, develop and disseminate guidance to Department of State bureaus and offices that describes when a security-cleared contractor must take classification training required by Executive Order 13526, who will pay for the training, and how the suspension of classification authority will apply to security-cleared contractors who do not complete the required training.

Recommendation 3: OIG recommends that the Bureau of Information Resource Management develop and implement a control within the Classified State Messaging Archive and Retrieval Toolset that allows only individuals who occupy positions that have been designated as original classification authority to identify themselves as such when making original classification decisions.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement corrective actions to prevent the Classified State Messaging Archive and Retrieval Toolset from being uninstalled or, if the software becomes uninstalled, that the Bureau of Information Resource Management be notified that the software needs to be reinstalled.

Recommendation 5: OIG recommends that the Bureau of Administration develop and implement a process to formally request and obtain, from all bureaus and offices within the Department of State, annual reports of all classification decisions made to facilitate compliance with Executive Order 13526 and with the inspection and reporting requirements contained in Title 32, Code of Federal Regulations, Sections 2001.60 and 2001.90.

Recommendation 6: OIG recommends that the Bureau of Administration develop and disseminate guidance to all bureaus and offices regarding the creation and maintenance of repositories of classified documents to facilitate the count of classification decisions reported annually in the Agency Security Classification Management Program Data form and to facilitate the review of a representative sample of classified documents during each self-inspection.

Recommendation 7: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Human Resources, (a) conduct a staffing workload assessment of the Bureau of Administration, Office of Information Programs and Services, and (b) ensure that the office has, or will obtain, the adequate level of resources as determined by the assessment. The purpose of the assessment is to determine whether the Bureau of Administration has the appropriate level of resources necessary to establish and maintain an effective sustainable process for the development of the annual Agency Security Classification Management Program Data report and for sampling and reviewing classified documents required as part of a self-inspection under Executive Order 13526.

Recommendation 8: OIG recommends that the Bureau of Administration, in coordination with the Under Secretary for Management, develop and implement a standard operating procedure for periodically reviewing and updating the lists of positions in which personnel are authorized to make original classification decisions to ensure that these lists are current and accurate.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Office of Inspector General (OIG) conducted this compliance follow-up review to determine whether the actions taken by the Bureau of Administration and other responsible bureaus fully addressed the deficiencies identified in OIG's March 2013 evaluation report.[1] OIG conducted this review pursuant to the Reducing Over-Classification Act of 2010,[2] which requires that OIG conduct no fewer than two reviews of the Department of State's (Department) implementation of Executive Order 13526.[3]

OIG performed fieldwork from September 2015 to March 2016 at the Bureau of Administration, the Bureau of Diplomatic Security (DS), the Foreign Service Institute (FSI), the Bureau of Intelligence and Research (INR), the Bureau of Information Resource Management (IRM), the Bureau of Human Resources, and the Office of the Secretary. This compliance follow-up review was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. These standards require that OIG plan and perform the compliance follow-up review to obtain evidence supporting findings, conclusions, and recommendations that are sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions presented.

To gather information for this compliance review, OIG interviewed officials from DS's Office of Information Security; IRM's Messaging Systems Office; INR's Executive Office and Publications Office; FSI's Executive Office; the Bureau of Administration's Global Information Services, Office of Information Programs and Services; and the Department's Executive Secretariat, located within the Office of the Secretary. OIG obtained and reviewed records from the Bureau of Administration, DS, FSI, INR, IRM, and the Bureau of Human Resources.

OIG researched and reviewed regulations and guidance related to Executive Order 13526. These regulations and guidance included policies and procedures contained in the *Foreign Affairs Manual* and the *Foreign Affairs Handbook*; guidance from the National Archives and Records Administration, Information Security Oversight Office (ISOO); and prior OIG reports, as described. OIG obtained and reviewed samples of classified documents created by Department officials. Additionally, OIG had correspondence with classifiers of various classified documents.

[1] OIG, *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information* (March 2013, AUD-SI-13-22).

[2] Pub. L. No. 111-258, 124 Stat. 2648 (2010).

[3] Classified National Security Information, issued on December 29, 2009.

Prior Reports

- *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information* (AUD-SI-13-22, March 2013). The Background section of this report summarized the results of the March 2013 evaluation.

- *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015). In this review, OIG reported that system designers in IRM needed more understanding and knowledge of the needs of their customers to make the State Messaging and Archive Retrieval Toolset system more useful. The report stated that a new procedure for monitoring the needs of customers would facilitate making those adjustments.

Work Related to Internal Controls

OIG performed steps to assess the adequacy of internal controls related to the areas evaluated. OIG gained an understanding of the internal controls by meeting with Department officials and reviewing documents evidencing processes and control activities. Specifically, OIG evaluated the adequacy of the design of processes and controls implemented to address the recommendations issued by OIG in Report AUD-SI-13-22. Work performed on internal controls during the compliance follow-up review is detailed in the Results of Follow-up Review section of this report.

Use of Computer-Processed Data

OIG conducted two tests during the compliance follow-up review that required the use of computer generated data: (1) to test the Bureau of Administration's self-inspection, OIG reviewed classified documents from two of the Department's electronic archive systems, and (2) to test the training requirements set forth in Executive Order 13526, OIG compared data, as of September 30, 2015, on security-cleared Department employees (from the Bureau of Human Resources) with information in the employees' training records (from FSI) for the classification and marking course (PK 323).

OIG assessed the reliability of the computer-generated data by interviewing cognizant officials and assessing classified documents provided by the Department and employees and training records from the Bureau of Human Resources and FSI. OIG obtained, from the Bureau of Administration, a list of the classified documents that it reviewed during the 2014 self-inspection. The Bureau of Administration selected these documents from among those contained in the State Archiving System (SAS) and INR's ClassNet webpage. OIG found no reportable deficiencies related to those classified documents selected and reviewed. In addition, OIG obtained, from the Bureau of Human Resources, a listing of all of the Department's security-cleared employees and compared that list with the employees' training records from FSI for the classification and marking course (PK 323) to determine the level of employee compliance with the requirements with Executive Order 13526. OIG could determine only the compliance level of

the Department's security-cleared contractors because the Department could not provide a reliable accounting of security-cleared contractors who work for the Department. OIG determined that the data used in this report was sufficiently reliable to reach the conclusions presented.

APPENDIX B: ORIGINAL RECOMMENDATIONS FROM THE MARCH 2013 EVALUATION REPORT (AUD-SI-13-22) AND THEIR STATUS

The original recommendations from the Office of Inspector General's (OIG) report *Evaluation of Department of State Implementation of Executive Order 13526, Classified National Security Information* (AUD-SI-13-22, March 2013) are presented, along with their status.

Recommendation 1: OIG recommends that the Bureau of Administration add the course Classified and Sensitive But Unclassified Information: Identifying and Marking (PK 323) to the mandatory training list in Volume 13 of the *Foreign Affairs Manual* to promote awareness of the training requirement.

> Status: Closed. In February 2015, OIG closed this recommendation in response to a Bureau of Administration memorandum dated December 2014 that confirmed that a revised *Foreign Affairs Manual* section was published in September 2014.

Recommendation 2: OIG recommends that the Bureau of Administration amend the *Foreign Affairs Manual* to align with the language in Executive Order 13526 that states that those who fail to receive classification training "shall" have their classification authority suspended.

> Status: Closed. In October 2014, OIG closed this recommendation in response to a Bureau of Administration memorandum dated May 2014 that confirmed that a revised *Foreign Affairs Manual* section was published in April 2014.

Recommendation 3: OIG recommends that the Bureau of Administration, in coordination with the Foreign Service Institute, immediately establish and implement a process to identify Department of State classifiers who have not complied with the classification training requirement and to take the actions required by the amended *Foreign Affairs Manual*.

> Status: Closed. In February 2015, OIG closed this recommendation in response to a Bureau of Administration memorandum dated December 2014 in which the Bureau of Administration described the process that each of the Department's bureau would use to identify individuals who had not completed the prescribed training and to sanction noncompliant individuals accordingly.

Recommendation 4: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Information Resource Management, replace the Classified State Messaging Archive and Retrieval Toolset (SMART-C) 4.2 application with SMART-C 5.5 for all users of the classified email network to promote compliance with Executive Order 13526.

> Status: Closed. In March 2014, OIG closed this recommendation because the Bureau of Administration coordinated with the Bureau of Information Resources Management

regarding this matter and provided documentation demonstrating that the Bureau of Information Resources Management had fully deployed SMART-C 5.5 to all ClassNet users.

Recommendation 5: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Intelligence and Research and the Bureau of Diplomatic Security, develop and implement a sampling methodology that attains a representative sample of all classified documents maintained within the Department of State for its annual self-inspection of the classification program.

Status: In March 2014, OIG closed this recommendation in response to a Bureau of Administration memorandum dated November 2013 in which the Bureau of Administration confirmed that it had requested, through the Under Secretary for Management, that the Bureau of Diplomatic Security, the Bureau of Intelligence and Research, and the Bureau of Information Resources Management supply all information needed to complete the annual self-inspection report. The Bureau of Administration's memorandum to these bureaus detailed the information that these bureaus should provide and contained a copy of the Under Secretary's memorandum. The Bureau of Administration's memorandum to these bureaus also included a copy of guidelines for self-inspections from the National Archives and Records Administration, Information Security Oversight Office, and a copy of OIG's March 2013 report.

Recommendation 6: OIG recommends that the Bureau of Administration ensure that all Department of State bureaus that contribute data reported on Standard Form 311 receive and comply with guidance from the National Archives and Records Administration, Information Security Oversight Office, which pertains to validating that the data submitted to the National Archives and Record Administration is accurate[1].

Status: Resolved, pending further action. As of February 2015, the Bureau of Administration had agreed to implement this recommendation but had not yet completed its actions to do so.

[1] This recommendation was modified and reissued in this Compliance Follow-Up Review report (page 23) based upon the findings identified during the conduct of the Review.

APPENDIX C: BUREAU OF ADMINISTRATION RESPONSE

United States Department of State

Washington, D.C. 20520

www.state.gov

August 5, 2016

UNCLASSIFIED

MEMORANDUM FOR NORMAN P. BROWN – OIG/AUD

From: A – Joyce A. Barr

SUBJECT: Bureau of Administration response to the Draft Report on *Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information* dated July 19, 2016.

The Bureau of Administration (A) appreciates the opportunity to review the subject draft report and provide our written response. The Bureau of Administration notes that the recommendations in this report will significantly increase the workload of the E.O. 13526 Program.

Recommendation 1: OIG recommends that the Bureau of Administration develop and disseminate guidance to all Department of State (Department) bureaus and offices regarding how the bureaus should meet their responsibilities outlined in the Foreign Affairs Manual for monitoring and enforcing the mandatory classification training requirements for all Department employees. The guidance should specify, at a minimum, how the bureaus should identify their staff members who require classification training to comply with Executive Order 13526, when each bureau's initial list of individuals who must take the required training is due to the Bureau of Administration, and how often the lists need to be updated. The guidance should also specify the procedures that each bureau must follow to sanction security-cleared individuals who do not take the required training.

UNCLASSIFIED

A Bureau Response : The Bureau of Administration concurs with this recommendation and will update the FAM to specify that employees and contractors with a security clearance must complete classification training. The FAM update will include schedules for bureaus to provide initial and updated lists of covered employees to A Bureau and include language explaining that bureaus should suspend ClassNett access when employees and contractors do not complete the required training.

Recommendation 2: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Security, develop and disseminate guidance to Department of State bureaus and offices that describes when a security-cleared contractor must take classification training required by Executive Order 13526, who will pay for the training, and how the suspension of classification authority will apply to security-cleared contractors who do not complete the required training.

A Bureau Response: The Bureau of Administration concurs with this recommendation. Any contractor at the Department with a security clearance has the authority to make a derivative classification decision using either an underlying classified source document or a classification guide. Therefore, all security cleared contractors must take the classification training required by E.O. 13526. A Bureau will work with Department training officials to solicit ideas on making the course available to contractors and options for covering associate costs. Procedures for suspension of classification authority for contractors will require discussion with the Office of Acquisitions and the Procurement Executive.

Recommendation 5: OIG recommends that the Bureau of Administration develop and implement a process to formally request and obtain, from all bureaus and offices within the Department of State, annual reports of all classification decisions made to facilitate compliance with Executive Order 13526 and with the inspection and reporting requirements contained in Title 32 of the Code of Federal Regulations Sections 2001.60 and 2001.90.

A Bureau Response: The Bureau of Administration concurs with this recommendation. Since the A Bureau currently counts electronic classification decisions via the SMART system, counting hard copy documents will significantly increase the risk of double counting. Checking hard copy documents against the email archive to avoid duplication would require resources (both employees and systems) that are not currently available to the bureau. Please note that the Top Secret Control Officer Program referenced by OIG in this report, ceased to exist on October 1, 2013 (see Department Notice 2013_09_168).

Recommendation 6: OIG recommends that the Bureau of Administration develop and disseminate guidance to all bureaus and offices regarding the creation and maintenance of repositories of classified documents to facilitate the count of classification decisions reported annually in the Agency Security Classification Management Program Data form and to facilitate the review of a representative sample of classified documents during each self-inspection.

A Bureau Response: The Bureau of Administration concurs with this recommendation and will work with the Bureau of Diplomatic Security to develop guidance regarding the creation and maintenance of repositories of classified information.

Recommendation 7: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Human Resources, (a) conduct a staffing workload assessment of the Bureau of Administration, Office of Information Programs and Services, and (b) ensure that the office has, or will obtain, the adequate level of resources as determined by the assessment. The purpose of the assessment is to determine whether the Bureau of Administration has the appropriate level of resources necessary to establish and maintain an effective sustainable process for the development of the annual Agency Security Classification Management Program Data report and for sampling and reviewing classified documents required as part of a self-inspection under Executive Order 13526.

A Bureau Response: The Bureau of Administration concurs and will coordinate with our Executive Office for the recommended staffing workload study.

Recommendation 8: **OIG recommends that the Bureau of Administration, in coordination with the Under Secretary for Management, develop and implement a standard operating procedure for periodically reviewing and updating the lists of positions in which personnel are authorized to make original classification decisions to ensure that these lists are current and accurate.**

A Bureau Response: The Bureau of Administration concurs and will develop a process to review the lists of positions designated as Original Classification Authorities on an annual basis and will seek the approval of the Under Secretary for Management when the Secret level OCA list requires updating and the Secretary of State when the Top Secret level OCA list requires updating.

APPENDIX D: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE

United States Department of State

Washington, D.C. 20520

August 3, 2016

TO: OIG/ISP – Patricia Stewart

FROM: PDCIO – Robert L. Adams, Acting

SUBJECT: IRM Response to OIG CFR of E.O. 13526: Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information

IRM's response to the following recommendation is provided below:

Recommendation 3: OIG recommends that the Bureau of Information Resource Management develop and implement a control within the Classified State Messaging Archive and Retrieval Toolset that allows only individuals who occupy positions that have been designated as original classification authority to identify themselves as such when making original classification decisions.

IRM Response (August 2016): As noted by OIG in the cited examples, IRM concurs that it is possible to remediate the risk of an employee incorrectly identifying himself or herself as an Original Classification Authority (OCA). In the next seven months IRM will develop, test, and implement informational alerts which will be added to the Classification Authority fields to alert the creator that OCA authority is limited to people who are designated by the President or by the agency and is reserved primarily for senior officers.

Recommendation 4: OIG recommends that the Bureau of Information Resource Management develop and implement corrective actions to prevent the Classified State Messaging Archive and Retrieval Toolset from being uninstalled or, if the software becomes uninstalled, that IRM be notified that the software needs to be reinstalled.

IRM Response (August 2016): IRM concurs with the OIG recommendation and already implemented the SMART-C Messaging Manager which checks for the

presence of the SMART client and automatically reinstalls it if the client is removed for any reason. This process alleviates the onus on users notifying IRM support and also eliminates the need to build in an alert mechanism.

APPENDIX E: FOREIGN SERVICE INSTITUTE COMMENTS

United States Department of State

Foreign Service Institute

George P. Shultz National Foreign Affairs Training Center
Washington, D.C. 20522-4201

UNCLASSIFIED

August 2, 2016

INFORMATION MEMO FOR NORMAN P. BROWN, ASSISTANT INSPECTOR GENERAL (OIG/AUD)

FROM: FSI/EX – Elizabeth G. Hamly, Management Analyst

SUBJECT: Draft Report - Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information

Thank you for providing FSI the opportunity to review the abovementioned draft report. Below are our suggested edits:

- Page 10/last paragraph/last sentence, "Nevertheless, Department policy states that only completion of the PK323 training fulfills the Executive Order's training requirement for Department employees." This statement is inaccurate in that 13 FAM 371 does not state that only completion of PK323 fulfills the Executive Order's training requirement for Department employees.
- Page 11/second paragraph/third sentence, "The revised FAM now requires bureau executive directors to take the following actions: (1) identify which of their employees[28][…]"
    - This statement is inaccurate in that 13 FAM 371 stipulates that bureaus are responsible for identifying employees not "executive directors" specifically.
- Footnote 28 states, "The term employee as used with regard to classification training requirements, encompasses all Department employees and all contractors and other personnel." This statement is confusing in that 13 FAM 371 mentions "employees," however, it does not mention "contractors and other personnel."
    - Page 11/third paragraph/first sentence, "Although, as noted previously, the Department outlined in the FAM general requirements each bureau executive director [….]" This statement is inaccurate in that 13 FAM 371 in that it is bureaus that are responsible for identifying employees not "executive directors" specifically.

Please let me know if you have any further questions or comments. I can be reached at 703-302-6731/hamlyeg@state.gov.

ABBREVIATIONS

DS	Bureau of Diplomatic Security
FAM	Foreign Affairs Manual
FOIA	Freedom of Information Act
FSI	Foreign Service Institute
INR	Bureau of Intelligence and Research
INRISS	INR Information Support System
IRM	Bureau of Information Resource Management
ISOO	Information Security Oversight Office
SAS	State Archiving System
SF	Standard Form
SMART-C	Classified State Messaging Archive and Retrieval Toolset

OIG REVIEW TEAM

Regina Meade, Director
Security and Intelligence Division
Office of Audits

William Irving, Audit Manager
Security and Intelligence Division
Office of Audits

Judith Balent Morsy, Management Analyst
Security and Intelligence Division
Office of Audits

Phillip Ropella, Senior Auditor
Security and Intelligence Division
Office of Audits

Patrick Sampson, Senior Auditor
Security and Intelligence Division
Office of Audits

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
HOTLINE@stateoig.gov
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
WPEAOmbuds@stateoig.gov