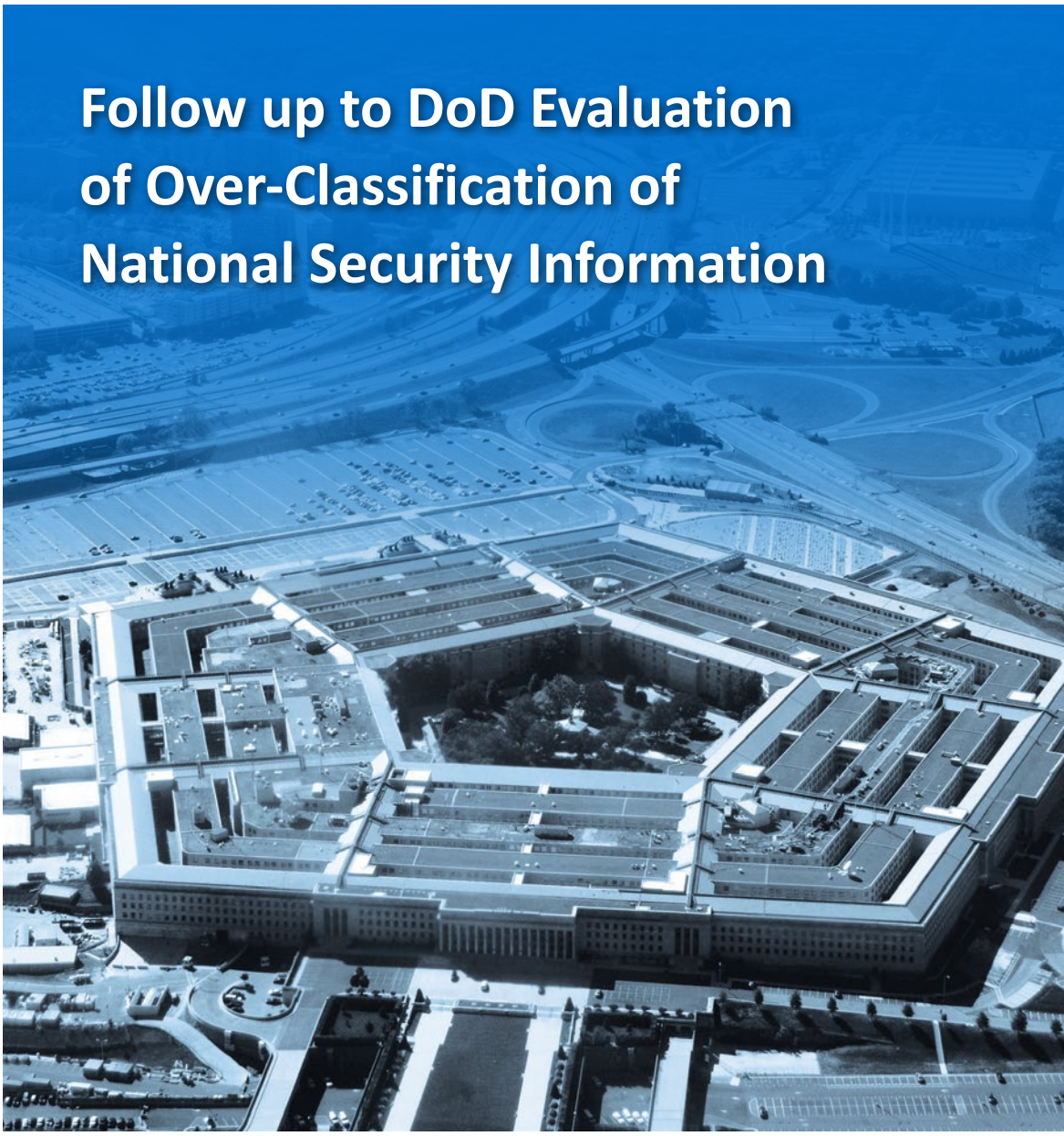
Report No. DODIG-2017-028

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 1, 2016

Follow up to DoD Evaluation of Over-Classification of National Security Information



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Follow up to DoD Evaluation of Over-Classification of National Security Information

December 1, 2016

Objective

We determined the implementation status of 13 recommendations concerning Department of Defense classification policies and procedures contained in Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," which we issued on September 30, 2013.

Background

We conducted this follow-up review in response to Public Law (PL) 111-258, "Reducing Over-Classification Act," which requires that the Inspector General (IG) of each department or agency of the U.S. with an officer or employee who is authorized to make original classifications, in consultation with the Information Security Oversight Office (ISOO) shall carry out evaluations of that department or agency or a component of the department or agency:

- to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and
- to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

Visit us at www.dodig.mil

Findings

We determined that the Under Secretary of Defense for Intelligence (USD(I)) fully implemented two and partially implemented 11 of the 13 recommendations we previously made. Of the 11 that were partially implemented, four were in the process of being implemented in conjunction with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)).

The following recommendations were implemented.

- We recommended that the USD(I) enhance its outreach to the security community to expand awareness of the Defense Security Service Center for Development of Security Excellence (DSS CDSE). DSS CDSE has increased delivery methods for security training courses and broadened its outreach efforts, with the goal of improving timeliness of training provided to original and derivative classifiers.
- We recommended that the USD(I) ensure all original and derivative classifiers receive relevant and timely training. DSS CDSE has implemented additional course offerings that are tailored to original and derivative classifiers.

However, the following recommendations are still in the process of being implemented.

- We recommended that the USD(I) provide the implementation status of DoD Component actions to include a critical element on security in original and derivative classifier's performance evaluations. On May 7, 2016, the requirement to include a critical element on security was incorporated into DoD Instruction 1400.25, Volume 2011, "DoD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Performance Management." However, of the 1,988 derivative classifiers we surveyed, 82 percent stated that security was a critical element in their performance evaluations, while 18 percent stated security was not a critical element in their performance evaluations.

Results in Brief

Follow up to DoD Evaluation of Over-Classification of National Security Information

Findings (cont'd)

- We recommended that the USD(I) revise policy to incorporate template language for security classification guides (SCGs).[1] The language has been incorporated in an ongoing revision of DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012; however, the Manual is undergoing final review.
- We recommended that the USD(I) direct Component reviews of Original Classification Authority (OCA) positions to ensure that the position is needed. On April 16, 2015, the USD(I) issued a memorandum directing DoD Components to validate each OCA position to assess whether that position is still required. However, of the 106 Security Managers we surveyed to determine whether their organization had conducted a review to establish the requirement for OCA authority, we found that 87 Components had not conducted a review, while 15 organizations had.
- We recommended that the USD(I), in coordination with the USD(AT&L), incorporate into policy that:
  - SCGs forwarded to the Defense Technical Information Center (DTIC) contain the requisite DD Form 2024, a form used to identify a change to the SCG, and signed by the appropriate OCA to ensure accountability.
  - DTIC not accept DD Forms 2024 that are not completely filled out and signed by the appropriate agency.
  - A time requirement for the submission of updated SCGs be established.
  - Reminders be sent to organizations as SCGs near biennial review requirements.

These requirements were incorporated into DoD Manuals 5200.01, Volume 1, and 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, which are undergoing review.

Recommendations

We are not making additional recommendations in this follow-up report because DoD has implemented, or is in the process of implementing, agreed-upon recommendations from our previous review. Updates to DoD Manuals 5200.01, Volume 1 and 5200.45 are in the staffing process and are close to approval and completion.

Management Comments and Our Response

We provided a discussion draft report to management for review and comment. Management concurred with our conclusions and did not have any comments to the discussion draft. Therefore, no written response to this report is required.

[1] SCGs contain a set of classification instructions from an OCA to derivative classifiers. These instructions identify elements of information on a specific subject that must be classified and the classifications' level and duration for each element.

Recommendations Table

Management	Recommendations Requiring Comment
Under Secretary of Defense for Intelligence	None
Under Secretary of Defense for Acquisition, Technology, and Logistics	None


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 1, 2016

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

SUBJECT: Follow up to DoD Evaluation of Over-Classification of National Security Information (Report No. DODIG-2017-028)

We are providing this report for your information and use. We determined if agreed-upon recommendations outlined in Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013, were implemented as agreed. We conducted this review in response to Public Law (PL) 111-258, "Reducing Over-Classification Act."

We found that agreed upon recommendations made in DODIG-2013-142 were implemented or are still in the process of being implemented. The Defense Security Service Center for Development of Security Excellence broadened its outreach efforts and implemented additional course offerings that are consistent with policy and tailored to original and derivative classifiers. Most personnel we surveyed have a critical element on security in their performance evaluations; however, some still do not. The Under Secretary of Defense for Intelligence (USD(I)) directed Component reviews of Original Classification Authority (OCA) positions to ensure those positions are needed; however, most Security Managers we surveyed had not conducted a review. Language has been incorporated into policy to revise template language in security classification guides (SCGs) for derivative classifiers who want to challenge the level at which information is classified; however, that policy is undergoing review. Language has also been incorporated into policy that SCGs forwarded to the Defense Technical Information Center (DTIC) be submitted and reviewed in a timely manner, forwarded with a completed DD Form 2024, and signed by the appropriate OCA to ensure accountability; however, that policy has not yet been issued in final.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. We provided a discussion draft report to management for review and comment. Management concurred with our conclusions and did not have any comments to the discussion draft. Therefore, no written response to this report is required.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7430, or the Project Manager at (703) 699-7214 (DSN 499-7214).

Anthony C. Thomas
Deputy Inspector General for
Intelligence and Special
Program Assessments

Contents

Introduction

Updates to Findings

Contents (cont'd)

Appendixes

Acronyms and Abbreviations


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

We determined whether the USD(I) implemented 13 recommendations, four in coordination with the USD(AT&L), as outlined in Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013, as agreed. We conducted this review in response to PL 111-258, "Reducing Over-Classification Act," which requires that the IG of each department or agency of the U.S. with an officer or employee who is authorized to make original classifications, in consultation with the ISOO[2] shall carry out no less than two evaluations of that department or agency or a component of the department or agency:

- to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component; and
- to identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

See Appendix A for the scope and methodology.

Background

PL 111-258 required that the IG's complete an initial evaluation by September 30, 2013. In response, the DoD OIG issued Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013, which discussed the results of the evaluation of the effectiveness of policies, procedures, rules, regulations, and management practices that may be contributing to persistent misclassification and over-classification in DoD.

In DODIG-2013-142, we found that applicable classification policies, procedures, rules, and regulations had been adopted; however, in some circumstances, they had not been followed or effectively administered. We also found that some policies, procedures, rules, regulations, and management practices might have contributed

[2] ISOO is responsible to the President for policy and oversight of the government-wide security classification system and the National Industrial Security Program. ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the Assistant to the President for National Security Affairs.

to persistent misclassification of material. The second evaluation was designed to review the progress made pursuant to the results of the first evaluation. This report addresses that requirement.

In addition, the law required that the IGs coordinate with each other and with the ISOO to ensure that evaluations follow a consistent methodology, as appropriate, that allows for cross-agency comparisons. In 2013, the Council of the Inspectors General on Integrity and Efficiency created an evaluation guide to promote consistency of evaluations conducted under PL 111-258.[3]

For this second evaluation, consistent with the 2013 report, we have used a working definition of "over-classification" that ISOO supplied: the designation of information as classified, when the information does not meet one or more of the standards for classification under section 1.1 of Executive Order (EO) 13526, "Classified National Security Information," December 29, 2009.[4]

Information Security Oversight Office On-Site Reviews of DoD Organizations

Between February 2014 and October 2015, the ISOO also conducted five on-site reviews of DoD organizations to determine the degree to which the classified national security information (CNSI) program was being implemented in accordance with EO 13526, and its implementing directive, 32 Code of Federal Regulation (CFR) Part 2001,[5] and to provide recommendations for improvement as needed. The reviews covered core elements of the CNSI program of each of the five organizations.

The reviews examined program management and oversight, security education and training, safeguarding, self-inspections, security violations, as well as information assurance program management and classified systems management. We discuss these reports and their findings throughout this report. A list of the ISOO reports can be found at Appendix A. A description of best practices discussed in these reviews is at Appendix D.

---

[3] For the 2013 evaluation, we used an evaluation guide that a working group of participating IGs, led by the DoD OIG, prepared for all IG offices participating in this government-wide effort on behalf of the Council of the Inspectors General on Integrity and Efficiency. The evaluation guide was intended to meet PL 111-258 requirements regarding the responsibilities of each participating department and agency. The working group was formed to ensure consistency in the evaluative process, comparable reporting, and the ability to compare results across agencies. The evaluation guide is on the Council of the Inspectors General on Integrity and Efficiency website: https://www.ignet.gov/content/reports-publications (under "List by Year," then "2013"), "A Standard User's Guide for Inspectors General Conducting Evaluations under Public Law 111-258, the Reducing Over-Classification Act."

[4] EO 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

[5] ISOO conducts reviews of classified materials generated by the agencies in order to evaluate the extent to which the materials have been classified and marked according to the requirements of EO 13526 and the Directive. The reviews also examine program management and oversight, security education and training, safeguarding, self-inspections, security violations, and classified information systems management to determine if these programs are also aligned with the guidance in EO 13526.

Fundamental Classification Guidance Review (FCGR) Program

EO 13526, Section 1.9, directed the initiation of the FCGR program, and requires agency heads to complete, on a periodic basis, a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. EO 13526 also required that the FCGR include an evaluation of classified information to determine if it meets the standards for classification, and that the reviews include OCAs and agency subject matter experts to ensure a broad range of perspectives.

The ISOO subsequently directed that the initial review be completed by June 27, 2012, and that reviews be completed every five years thereafter. The June 27, 2012, DoD report detailed the status of FCGR activities from 2011-2012, including a reduction of 413 SCGs, from 2,070 to 1,657.

DTIC officials who manage the central repository of DoD SCGs attributed increased compliance with SCGs guidelines to the efforts undertaken during the 2012 FCGR. Agencies will next provide FCGR status updates in October 2016 and February 2017, with final reports due by June 30, 2017.

On March 23, 2016, the Director of National Intelligence wrote a letter, "Addendum to the FY 2017 Fundamental Classification Guidance Review," to the Directors of the Central Intelligence Agency, Defense Intelligence Agency, the National Security Agency, the Geospatial-Intelligence Agency, the National Reconnaissance Office, the ISOO, and the USD(I), requesting the involvement of each organization in conducting four feasibility studies:

- Reducing the number of OCAs;
- Increasing discretionary declassification decisions;
- Creating an Intelligence Community-wide Classification Guide; and
- Eliminating CONFIDENTIAL from Agency guides.

The intent of the four feasibility studies is to determine if the results of the studies will further the goal for greater openness and reduced classification activity while protecting legitimate national security interests. The Director of National Intelligence requested a response to the four areas in the February 2017 update to the FCGR.

The ISOO reviews and the DoD FCGR program were conducted in accordance with guidance established in EO 13526 with the goal of assessing specific aspects of DoD CNSI programs. The ISOO reports discussed topics that are also addressed in this report, including program management and oversight, self inspections, and security education and training. The reports provide a basis for comparison of our followup efforts and a snapshot of agency programs during FY 2015. As a comprehensive review of agency classification guidance, the 2012 DoD FCGR report provided a baseline from which to conduct our 2013 review of SCGs, and informed the subsequent review of data for our current evaluation.

DODIG Report No. DODIG-2013-142

Overview of Findings

In DODIG-2013-142, we found that DoD organizations had adopted applicable classification policies, procedures, rules, and regulations; however, in some circumstances, organizations did not fully follow or effectively administer guidance as required. We also concluded that some policies, procedures, rules, regulations, or management practices may have contributed to persistent misclassification of material. While we did find some instances of over-classification, we did not conclude that those instances concealed violations of law, inefficiency, or administrative error; prevented embarrassment to a person, organization, or agency; restrained competition; or prevented or delayed the release of information not requiring protection in the interest of national security.[6] However, we did find several instances where the inaccurate use of dissemination control and handling markings could unnecessarily restrict information sharing.

Many of the issues we found were similarly reflected in organizational self-inspections and FCGR results, demonstrating that DoD was aware of weaknesses.[7]

In our 2013 report, we also included observations evaluating the effectiveness of policies for developing classification decisions, classification by derivative classifiers, effectiveness of self-inspection programs, and classification standards addressed both within DoD policy and by the Intelligence Community. Details of our previous observations, as well as our follow up to these observations, can be found in Appendix B.

---

[6] These classification limitations and prohibitions are articulated in Section 1.7 of EO 13526.

[7] EO 13526, Section 5.4(d)(4), requires that Component Senior Agency Official establish and maintain an ongoing self-inspection program, including regular reviews of representative samples of the agency's original and derivative classified actions. Self-inspections also evaluate the effectiveness of agency programs covering declassification, safeguarding, security violations, security education and training, and management and oversight. The results are reported annually to the ISOO.

National Defense Authorization Act for Fiscal Year 2015

House Report 113-446, accompanying H.R. 4435, the Howard P. "Buck" McKeon National Defense Authorization Act for FY 2015, directed the Secretary of Defense to submit "a report to the congressional defense committees not later than March 1, 2015, on the status and implementation of the recommendations found in DODIG–2013–142. The Secretary's report should include specific actions taken to implement the recommendations contained in the report and timeframes for implementing the remaining recommendations."

On April 9, 2015, on behalf of the Secretary of Defense, the USD(I) submitted a status report to the House and Senate Committees on Armed Services and Appropriations detailing completed actions as well as ongoing initiatives and timelines in response to the recommendations discussed in DODIG-2013-142.

In this followup review, we assess whether the actions discussed in the report that the DoD forwarded to Congress in response to our earlier recommendations were implemented.

Update to Finding A

Effectiveness of Security Program Management

The USD(I) is still in the process of implementing our previous recommendations to include a critical element on security in the performance evaluations of original and derivative classifier's and to revise policy to incorporate template language for SCGs. Based on a survey we conducted, we determined that as of July 27, 2016, 1,630 of the 1,988 (82 percent) original and derivative classifiers we surveyed have a critical element on security in their performance evaluations; however, 18 percent did not. We also found that 103 of 109 SCGs issued or revised since October 1, 2013, have template instructions for derivative classifiers who want to challenge the level at which information is classified. Including a critical element on security in the performance evaluations of original and derivative classifiers and revising policy to incorporate template language for SCGs are both in the process of being incorporated into an updated version of DoD Manual 5200.01, Volume 1.

Finding A from DODIG Report No. 2013-142

In our previous report we found that some DoD organizations had a critical element on security in their staff performance evaluations, while others did not.[8] This has been a requirement since at least 1997 but had not been enforced. Without the critical element for security in original and derivative classifier performance evaluations, there was little accountability for ensuring the proper marking and classification of documents. We also found that SCG template instructions for those who want to challenge improper classification did not encourage individuals to challenge improper classifications, consistent with the intent of EO 13526.

EO 13526 encourages individuals to challenge improper classifications and required organizations to establish processes for challenges to occur. Current policy does not require language that encourages challenges and provides appropriate citations to assist in the challenge process.

[8] Section 5.4(d)(7) of EO 13526 requires heads of agencies that originate or handle classified information to ensure that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of: (A) original classification authorities; (B) security managers or security specialists; and (C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

Recommendations A.1 and A.2.a through e from DODIG Report No. 2013-142

Recommendation A.1

We recommended that the USD(I) provide the implementation status of DoD Component actions to include a critical element on security in the Component's performance evaluations.

Recommendation A.2

We recommended that the USD(I) revise policy to incorporate template language for SCGs that is consistent with the intent of EO 13526, as follows:

a. ***Section 5.3 of EO 13526 and Enclosure 4, paragraph 22 of DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, contain guidance for individuals who wish to challenge information that they believe has been improperly or unnecessarily classified.***

b. ***Such challenges are encouraged and expected and should be forwarded through the appropriate channels to the office of primary responsibility.***

c. ***Pending final decision, handle and protect the information at its current classification level or at the recommended change level, whichever is higher.***

d. ***Challenges should include sufficient description to permit identification of the specific information under challenge with reasonable effort.***

e. ***Challenges should include detailed justification outlining why the information is improperly or unnecessarily classified.***

The OUSD(I) concurred with our recommendations, stating in its November 1, 2013, response to DODIG-2013-142, that it published the memorandum "Performance Appraisal Critical Element for the Protection of Classified Information," directing that as part of the Secretary of Defense's "top down" approach outlined in his October 18, 2012 memorandum, "Deterring and Preventing Unauthorized Disclosures of Classified Information," that DoD Components integrate security as a critical element into their performance evaluation system. The OUSD(I) further stated that it did not have responsibility or cognizance over the DoD's performance evaluation system.

The OUSD(I) stated that it would also draft language to revise existing policy to encourage classification challenges, and provide template language for SCGs.

USD(I) Response to Congress

In its 2015 response to Congress, the OUSD(I) stated that on June 12, 2013, the USD(I) directed heads of the DoD Components to integrate the critical element of security in the performance contract or other applicable rating system for original and derivative classifiers whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings as specified in section 5.4 of EO 13526.

In addition, the response stated that the OUSD(I) Human Capital Management Office was working to revise the DoD performance management regulation, DoD Instruction 1400.25, "DoD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Performance Management," to integrate the critical element of security in the performance evaluations of original and derivative classifiers.

The OUSD(I) also stated that it would emphasize classification challenge measures during the Defense Information Security Advisory Board (DISAB), an OUSD(I)-led forum for all Component Security Managers, and that it was also drafting policy to further emphasize and encourage classification challenges.

Management Actions

On June 12, 2013, the USD(I) directed heads of the DoD Components to integrate the critical element of security in the performance contract or other applicable rating system for certain personnel, including those specified in section 5.4 of EO 13526.

In addition, on May 7, 2016, the Under Secretary of Defense for Personnel & Readiness published DoD Instruction 1400.25, Volume 2011, "DoD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Performance Management." The OUSD(I) Human Capital Management Office, in conjunction with the Intelligence Community, added language to one of the performance elements in DoD Instruction 1400.25 for both non-supervisors and supervisors, emphasizing their responsibility to protect classified information in accordance with EO 13526. The Instruction requires that every Defense Intelligence employee be rated on this element.

DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, is currently being updated to encourage challenges of improper classification and enhance OCA involvement with the development and coordination of SCGs. DoD Manual 5200.45 is also being updated in conjunction with the Joint

Acquisition Protection and Exploitation Cell[9] initiative, identified by the Secretary of Defense in the April 2015 Cyber Security Strategy, to ensure cyber protection is addressed during SCG development.

In an ongoing update to the 2012 DoD Manual 5200.01, Volume 1, OUSD(I) is adding language to emphasize the responsibility of Component Heads to encourage classification challenges. One of the most important aspects of this update is incorporating template language for Component SCGs, consistent with the intent of EO 13526, to encourage challenges of improperly classified information. As of August 12, 2016, these updates included the following language:

- *Section 5.3 of EO 13526 and Enclosure 4, paragraph 22, "Challenges to Classification" of the Manual, contains guidance for individuals who wish to challenge information that they believe has been improperly or unnecessarily classified.*
- *Challenges are encouraged and expected and should be forwarded through the appropriate channels to the office of primary responsibility.*
- *Pending final decision, handle and protect the information at its current classification level or at the recommended change level, whichever is higher.*
- *Challenges should include sufficient description to permit identification of the specific information under challenge with reasonable effort.*
- *Challenges should include detailed justification outlining why the information is improperly or unnecessarily classified.*

Assessment of Management Actions

We determined that the recommendation to provide the implementation status to include a critical element on security in the performance evaluations of original and derivative classifier's and to revise policy to incorporate template language for SCGs were still in the process of being implemented.

In addition, to evaluate the effect of the measures taken by DoD in response to our recommendations, we surveyed 1,988 derivative classifiers in the Departments of the Navy and Air Force.[10] We also interviewed OUSD(I) security personnel to

[9] The Joint Acquisition Protection and Exploitation Cell is part of a key objective of Strategic Goal II, "Defend the DoD Information Network, Secure DoD Data, and Mitigate Risks to DoD Missions," of the DoD Cyber Strategy. Strategic Goal II states that "DoD must identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively. DoD must also plan and exercise to operate within a degraded and disrupted cyber environment in the event that an attack on DoD's networks and data succeeds, or if aspects of the critical infrastructure on which DoD relies for its operational and contingency plans are disrupted." The Joint Acquisition Protection and Exploitation Cell will link intelligence, counterintelligence, and law enforcement agents with acquisition program managers to prevent and mitigate data loss and theft. DoD will conduct comprehensive risk and damage assessments of cyber espionage and theft to inform requirements, acquisition, programmatic, and counterintelligence courses of action.

[10] For this evaluation, as well as in 2013, the Department of the Army conducted its own evaluation under PL 111-258.

discern the implementation status of including a critical element on security in the Component staff's performance evaluations and policy revisions to incorporate template language for SCGs. A majority of derivative classifiers surveyed (1,630 or 82 percent) stated that security was a critical element in their performance evaluations.

However, 357 derivative classifiers (18 percent) indicated that security was not a critical element in their performance evaluation.[11] The reasons provided for the absence of a critical element in these 357 responses ranged from individuals who worked in environments where security was not a core responsibility to those who worked in organizations that felt security was expected and therefore did not include security as a critical element in performance evaluations.

In addition, 71 percent of Security Managers identified security as a critical element in performance evaluations. This represents an improvement from our 2013 survey which showed that 64 percent of Security Managers identified security as a critical element. However, more work needs to be done, because 18 percent of derivative classifiers and 29 percent of Security Managers still did not indicate that security was a critical element in performance evaluations.

We also conducted a review of SCGs on the DTIC website that were revised or added from October 1, 2014 to July 28, 2016 in an effort to determine if SCGs have template instructions for derivative classifiers who want to challenge the level at which information is classified. The DTIC lists 197 updated or added SCGs during that period. Of that number, 109[12] were hyperlinked and applicable to this review. We found that 103 of 109 SCGs reviewed had some form of challenge language guidance. This represents a 94 percent compliance rate with existing policy and is consistent with guidance provided in EO 13526 that authorized holders of classified information should be able to challenge the classification status of the information in accordance with agency procedures.

We also asked the 1,988 DoD derivative classifiers if they were aware that DoD policy encourages classification challenges if information is incorrectly classified. We found that a majority of those surveyed (1,644, or approximately 83 percent) were aware that DoD guidance encourages the challenge of inaccurately classified information, while 17 percent were not aware. Moreover, 135 survey participants indicated that they have challenged incorrect classification levels either through

[11] The count totals 1,987 instead of 1,988 because one respondent's answer was unclear.

[12] Documents are hyperlinked on the DTIC website to allow users to access the .pdf file. The 88 SCGs that were not reviewed either did not have hyperlinks, were Department of Energy SCGs, contained guidance on how to complete SCGs, or were citations for classified SCGs.

formal processes (e.g., contacting the office of primary responsibility) or informal channels (e.g., seeking clarification). Of the SCGs reviewed, we still found some instances where challenge language was not consistent with guidance provided in EO 13526.

Conclusion

The USD(I) is still in the process of implementing the recommendations. The USD(I) issued a memorandum on June 12, 2013, directing heads of the DoD Components to integrate the critical element of security in the performance contract or other applicable rating system for original and derivative classifiers whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings as specified in section 5.4 of EO 13526.

On May 7, 2016, the requirement to include a critical element on security was incorporated into DoD Instruction 1400.25, Volume 2011, "DoD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Performance Management." However, of the 1,988 derivative classifiers we surveyed, 82 percent stated that security was a critical element in their performance evaluations, while 18 percent stated security was not a critical element in their performance evaluations.

In addition, ongoing updates to the 2012 DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, are incorporating template language for SCGs that is consistent with the intent of EO 13526; however, both Manuals are currently undergoing review and have not been finalized.

Update to Finding B

Effectiveness of Original Classification Authorities

We found that the OUSD(I) was still in the process of implementing the recommendation to direct Component reviews of OCA positions to ensure that the position is needed. On April 16, 2015, the USD(I) issued a memorandum directing DoD Components to validate each OCA position to assess whether that position was still required. However, of the 106 Security Managers we surveyed to determine whether their organization had conducted a review to establish the requirement for OCA authority, we found that 87 Components had not conducted a review, while only 15 organizations had.

Finding B from DODIG Report No. 2013-142

In our previous report we found that in some instances OCAs had not made many, if any, classification decisions, and a detailed review of those positions had not been conducted. OCAs inherited the classification authority of the position, and in some cases the requirements of the position had evolved and classification authorities were no longer needed. This likely resulted in a greater number of OCAs than needed, and as a consequence, security resources were allocated to support nonessential OCAs.

Recommendation B from DODIG Report No. 2013-142

Recommendation B

We recommended that the USD(I) direct Component reviews of OCA positions to ensure that the position is needed.

The OUSD(I) concurred with our recommendation, stating in its November 1, 2013, response to DODIG-2013-142, that it would develop a memorandum to direct Component reviews of OCA positions in accordance with the requirement that classification authority must be exercised an average of twice per year to qualify for retention of the OCA designation if an OCA does not issue and maintain a SCG.

Current Findings

In its 2015 response to Congress, the OUSD(I) stated that on a recurring basis it encouraged DoD Components to reduce OCA positions that were no longer required, and it was currently staffing a memorandum for USD(I) signature on this topic, which will direct DoD Components to validate each OCA position to assess whether that position is still required. The OUSD(I) anticipated completion, signature, and delivery of this memorandum by April 2015.

Management Actions

On April 16, 2015, the USD(I) issued a memorandum directing DoD Components to validate each OCA position to assess whether that position is still required.

On March 23, 2016, the Director of National Intelligence forwarded a letter, "Addendum to the FY 2017 Fundamental Classification Guidance Review," to the Directors of the Intelligence agencies, Director ISOO, and the USD(I) requesting the Directors' involvement in conducting four feasibility studies, one of which was a study regarding the feasibility of reducing the number of OCAs. The studies will evaluate whether it is possible to establish greater openness and reduced classification activity without compromising the protection of legitimate national security interests.

The ISOO requires FCGR status updates in October 2016 and February 2017, with a final report due to ISOO by 30 June 2017. The Director of National Intelligence requested the result of the feasibility study during the last update (February 2017) before the final FCGR reports are due.

The DNI requested participants to "Please comment on the feasibility of reducing the number of OCAs in your agency to the minimum number required and any negative impacts this might have on mission capabilities. The Office of the Director of National Intelligence (ODNI) undertook a similar initiative last year and reduced those with OCA from 24 to 10 by implementing a "use it or lose it" criterion. This did not negatively impact operations and actually saved time that had previously been spent ensuring the completion of annual training." So, the result is to state that it is possible to remove positions.

Assessment of Management Actions

We determined that the recommendation to direct Component reviews of OCA positions to ensure that the position is needed is still in the process of being implemented.

We surveyed 106 Security Managers to determine whether their organization had conducted a review to establish the requirement for OCA authority in their organization. We found that 87 Components had not conducted a review, while 15 organizations had. Four survey participants did not respond to the question. Of the 87 respondents who did not conduct OCA reviews, 29 (33 percent) indicated that they did not have anyone within their organization with OCA authority. Of the 15 organizations where OCA reviews were conducted, three decreased the number of positions with OCA authority. In total, five positions within the three organizations lost OCA designation.

We also surveyed OCAs to determine their level of original classification activity. Of the 17 OCAs surveyed, 12 (70 percent) had made classification determinations[13] and decisions, including revising or canceling SCGs, compared to 31 percent in our previous report. In total, 12 OCAs made 38 classification decisions.

A review of Navy and Air Force Standard Form 311s, "Agency Security Classification Management Program Data,"[14] for FYs 2014 and 2015 revealed that reviewed organizations reported a decrease in the number of OCAs. From FY 2014 to FY 2015, Navy OCAs decreased from 82 to 67, while Air Force OCAs decreased from 98 to 90 during the same period.

Also during that same period, DoD Standard Form 311s showed that overall, DoD OCAs decreased from 462 to 429, indicating that reviews of original classifying authorities are occurring across the DoD enterprise.

Conclusion

The OUSD(I) is in the process of implementing the recommendation. The USD(I) issued a memorandum on April 16, 2015, directing Component reviews of OCA positions to ensure the position is needed.

However, of the 106 Security Managers we surveyed to determine whether their organization had conducted a review to establish the requirement for OCA authority, we found that 87 Components had not conducted a review, while 15 organizations had. These numbers indicate that execution at the organizational level to reduce the number of OCAs is not complete.

The 2016 Director of National Intelligence letter to Directors of the Central Intelligence Agency, Defense Intelligence Agency, the National Security Agency, the Geospatial-Intelligence Agency, the National Reconnaissance Office, the ISOO, and the USD(I), requesting the involvement of each in reducing the number of OCAs, and any action taken as a result of the feasibility study would have an impact on the number of OCAs and the implementation of this recommendation.

[13] An original classification determination is an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

[14] The SF 311 is the data collection form that every Executive Branch agency submits on an annual basis reporting the total number of original classification authorities, classification decisions, mandatory review requests, and declassification decisions for that particular agency. The results from these forms are reported in ISOO's Annual Report to the President.

Update to Finding C

Effectiveness of Component Statistical and Cost Reports

The USD(I), in coordination with the USD(AT&L), is in the process of implementing recommendations to incorporate into policy that SCGs forwarded to the DTIC be submitted and reviewed in a timely manner, forwarded with a completed DD Form 2024 (a form used to identify a change to the SCG), and signed by the appropriate OCA to ensure accountability. The requirements were incorporated into drafts of DoD Manuals 5200.01, Volume 1, and 5200.45; however, those Manuals have not yet been issued in final.

Finding C from DODIG Report No. 2013-142

In our previous report, we found that although most SCGs were on the DTIC website, more effective management of the SCGs was needed to ensure their accuracy and OCA involvement. While organizations may have updated SCGs, this information was not always provided in a timely manner to DTIC. In the absence of updated SCGs, derivative classifiers ran the risk of citing wrongly classified or unnecessarily classified information potentially resulting in the unnecessary allocation of resources to protect improperly classified materials.

Recommendations C1 through C4 from DODIG Report No. 2013-142

Recommendation C

We recommended the USD(I), in coordination with the USD(AT&L), incorporate into policy that:

1. ***SCGs forwarded to the DTIC must be forwarded with the requisite DD Form 2024, and signed by the appropriate OCA to ensure accountability.***
2. ***DTIC not accept DD Forms 2024 that are not completely filled out and signed by the appropriate agency.***
3. ***A time requirement for the submission of updated SCGs be established.***
4. ***Reminders be sent to organizations as SCGs near biennial review requirements.***

The OUSD(I) and OUSD(AT&L) concurred with our recommendations, stating in their November 1, 2013, response to DODIG-2013-142 that they would coordinate to ensure that revised Information Security policy would be responsive to the recommendation.

USD(I) Response to Congress

In its 2015 response to Congress, the OUSD(I) stated:

- The requirement for OCAs to submit their SCGs to DTIC with a DD Form 2024 is described in DoD Manual 5200.01, Volume 1, Enclosure 6, and would reinforce the requirement through a change to DoD Manual 5200.45, which will begin coordination within the DoD by December 2015.
- The requirement for completed and signed DD Forms 2024 would be reinforced in a change to DoD Manual 5200.45.
- DoD Manual 5200.01, Volume 1, Enclosure 6 requires OCAs to review SCGs at least every five years.
- Specific to SCGs, OUSD(I) stated that it would collaborate with DTIC to develop a methodology to send reminders to DoD Component OCAs when Component SCGs are scheduled for review and update.[15]

The OUSD(I) further stated that it will also reinforce the requirement to submit SCGs to DTIC with a DD Form 2024 and completed and signed DD Forms 2024 in an Information Security "Policy Short" memorandum; however, "Policy Short" memorandums no longer exists.[16]

OUSD(I) also stated that DoD conducted a comprehensive FCGR in 2012. As a result of the FCGR, more than 97 percent of DoD's SCGs were updated and/or declared current. It also reported that in accordance with the five year review cycle, DoD is on track and on schedule to begin the next scheduled comprehensive oversight review in 2017.

Specific to SCGs, OUSD(I) stated that it would collaborate with DTIC to develop a methodology to send reminders to DoD Component OCAs when the DoD Components SCGs are scheduled for review and update.[17]

[15] We received additional documents that support OUSD(I) statements that policies, discussed in Appendix C, are being updated.

[16] We were informed by OUSD(I) representatives that policy shorts no longer exist, and that they would reinforce the requirement through revisions of DoD Manuals 5200.45 and 5200.01, Volume 1.

[17] We received additional documents that support OUSD(I) statements that policies, discussed in Appendix C, are being updated.

Management Actions

The USD(I), in coordination with the USD(AT&L) incorporated into DoD Manuals 5200.01, Volume 1, Enclosure 6 and DoD Manual 5200.45 that SCGs forwarded to DTIC be submitted and reviewed in a timely manner, forwarded with a completed DD Form 2024, signed by the appropriate OCA to ensure accountability, and that reminders will be sent by DTIC to organizations as security classification guides near their five year required reviews. However, DoD Manuals 5200.01, Volume 1 and DoD Manual 5200.45 are undergoing staffing and have not been finalized.

OUSD(I) provided draft policies, DISAB meeting notes, and presentations to support their 2015 response to Congress regarding ongoing efforts to increase coordination between Components and the DTIC repository with the goal of improving the relevancy of resident SCGs.

We spoke with DTIC representatives who stated that they will support the OUSD(I) with the SCG program through coordination on policy updates. OUSD(I) is the proponent of the policy and DTIC is the repository for SCGs that are also available online at the DTIC website. DTIC will assist OUSD(I) when OUSD(I) is developing the methodology for sending reminders to OCAs about the requirement to review and update organizational SCGs in accordance with DoD policy.

In addition to attending DISAB meetings, DTIC representatives stated a preference for regular meetings at least annually to discuss and share information regarding SCGs and the DTIC repository.

Assessment of Management Actions

We determined that the recommendation to incorporate into policy that SCGs forwarded to the DTIC be submitted and reviewed in a timely manner, forwarded with a completed DD Form 2024, a form used to identify a change to the SCG, and signed by the appropriate OCA to ensure accountability was still in the process of being implemented.

We reviewed SCGs to determine the level of Component compliance with policy. Our office conducted a review of SCGs located on the DTIC website, updated or added from October 1, 2014 to July 28, 2016. DTIC lists 197 updated or added SCGs during that time. Of that number, 109 were hyperlinked and related to the DoD.

We reviewed all 109 SCGs that were updated or created after FY 2013 as a baseline of comparison. We found improvement in the number of SCGs that contained the requisite DD Form 2024. As noted in our 2013 report, we reviewed 254 SCGs. One hundred twelve (44 percent) of the SCGs included the DD Form 2024.

For this second evaluation, we reviewed 109 SCGs revised or added since the beginning of FY 2014. Of the 109 reviewed, 94 (approximately 86 percent) included the form. This represents a marked increase in the level of compliance with existing DoD policy that requires the form to be submitted with approved SCGs.

We also found similar increases in the number of SCGs that accurately referenced EO 13526 as the basis for classification, regrading, or declassification of information. Specifically, we found that 102 of the 109 reviewed SCGs that were revised or added since the beginning of FY 2014 correctly referenced EO 13526 as opposed to the earlier EO 12958. This represents a compliance rate of 94 percent, and is an improvement when compared to our 2013 evaluation in which only 45 percent of the 254 SCGs reviewed correctly referenced EO 13526.

In addition to post FY 2013 SCGs, we randomly selected 106 SCGs from the DTIC repository to determine the timeliness of submissions. We still found issues that would suggest that some organizations are not submitting updated SCGs in a timely manner. Of the 106 guides reviewed, 42 (approximately 40 percent) had not met the requirement for a review every five years as required by policy.

We also found that 39 (approximately 37 percent) still referenced EO 12958 as the basis for classification determinations. Finally, 4 of the 106 reviewed SCGs in the DTIC repository contained declassification dates that had already occurred. These numbers indicate that some work still needs to be done to improve the process for submitting SCGs. Revised policy and the upcoming 2017 FCGR should assist with improving these errors.

Conclusion

The USD(I), in coordination with the USD(AT&L), are in the process of implementing the recommendations by incorporating verbiage into DoD Manuals 5200.01, Volume 1 and 5200.45, that SCGs forwarded to DTIC be submitted and reviewed in a timely manner, forwarded with a completed DD Form 2024, signed by the appropriate OCA to ensure accountability, and that reminders will be sent by DTIC to organizations as security classification guides near their five year required reviews.

However, the recommendations were not fully implemented because DoD Manuals 5200.01, Volume 1 and 5200.45 are undergoing staffing and have not been finalized.

Update to Finding D

Effectiveness of DoD Security Education and Training

The OUSD(I) implemented recommendations to develop a plan to enhance outreach to the security community to expand awareness of the Defense Security Service Center for Development of Security Excellence (DSS CDSE), and to ensure that original and derivative classifiers receive timely and relevant training. We found that the DSS CDSE has implemented additional course offerings that are consistent with policy and tailored to original and derivative classifiers. In addition, the DSS CDSE has increased delivery methods for security training courses and broadened its outreach efforts, with the goal of improving timeliness of training provided to original and derivative classifiers.

Finding D from DODIG Report No. 2013-142

In our previous report we found that overall, security training and education was effective; however, many interviewees expressed the view that security education and training was challenging for a number of reasons, ranging from availability and course content to delivery. Organizations varied their training programs based on their individual operating tempo, their need to tailor their training, and circumstances affecting their ability to deliver training to their personnel.

The organizational variances in training likely affected original and derivative classifiers' awareness of new training requirements and improved methodologies. In addition, personnel may have missed required training deadlines as a consequence of training inconsistencies. Although the DSS's CDSE offered courses that met policy requirements and could be delivered in various ways, personnel were unaware of both the CDSE and the courses. Without additional outreach to improve awareness of security training and education, DoD personnel could be unaware of all available courses.

Recommendation D.1 and D.2 from DODIG Report No. 2013-142

Recommendation D

We recommended the USD(I), develop a plan to:

1. ***Enhance its outreach to the security community to expand awareness of the CDSE.***
2. ***Ensure all original and derivative classifiers receive relevant and timely training that is tailored to current policy, procedures, rules, and regulations.***

The OUSD(I) concurred with our recommendations, stating in its November 1, 2013, response to DODIG-2013-142, that it had been working on several fronts with the DSS to increase awareness of the CDSE. These efforts included greater awareness of available security professionalization and certification programs and available online security training. The OUSD(I) stated that it also worked closely with the DSS's CDSE to develop portable and accessible training for biennial derivative classification training and for annual OCA training to provide readily accessible online training tools needed across DoD for these requirements.

OUSD(I) stated it would continue to work with DoD Components to develop a process to monitor and track the relevancy and timeliness of training for original and derivative classifiers. OUSD(I) also said that a memorandum would be developed to further emphasize training requirements and to conduct a functional data call across the DoD Components to request that they report on annual training completed under the responsibility and authority of assigned OCAs.

USD(I) Response to Congress

In its 2015 response to Congress, the OUSD(I) stated that it reviews annual security training requirements with DSS and CDSE staff to improve existing courses, or develop new course offerings for the DoD. OUSD(I) indicated that recent examples of such collaboration to ensure accurate classification and avoidance of over-classification included development of training and job aids for original classification, derivative classification, and marking of classified information.

OUSD(I) reported that CDSE personnel are invited to attend meetings of the DISAB, a forum for all Component Security Managers, and help develop its agenda. The DISAB thus serves as a key forum for DoD Information Security professionals to learn about CDSE offerings and training. CDSE security web based training links are featured on the OUSD(I) Security Policy and Oversight Division website to reinforce available training opportunities.

OUSD(I) also reported that it monitors the original and derivative classifier training of each DoD Component annually during the mandatory Component Self-Inspections to ensure completeness and compliance with DoD Manual 5200.01, Volume 3, Enclosure 5.

Management Actions

The DSS CDSE created a Security Awareness Hub. This website serves as a destination for accessing security awareness courses for DoD, other U.S. Government, and cleared industry personnel who do not require transcripts to fulfill security training requirements. A certificate is provided after the course is completed; however, there is no record maintained by CDSE.

CDSE maintains records of additional eLearning and instructor-led courses. The information is available on a CDSE Learning Management System called the Security Training, Education, and Professionalization Portal.

In August 2016, CDSE completed its Voice of the Community review. The Voice of the Community was a review undertaken by CDSE to gain a better understanding of customer and stakeholder wants and needs. For CDSE, the Voice of the Community served as a:

- report card that captures the community's holistic experience with CDSE;
- measurement of customer satisfaction;
- tool to increase trust and respect with customers and stakeholders;
- objective, third-party perspective;
- insight into potential offering improvements; and
- collection of customer usage and demographic data.

CDSE also discovered that respondents:

- value CDSE's products and services;
- use CDSE to meet their primary security training, education, and certification needs;
- desire more products and services;
- believe CDSE should stay on top of security developments and do more to advertise current content;
- believe the main concerns with CDSE deal with technology (e.g., website navigation, unable to save courses);
- recognize the utility of CDSE products and there are opportunities to further enhance the value; and
- lack of time and budget are the most common barriers to customer usage; however, network and technical issues are significant challenges.

CDSE reported to us that it will use this data to emphasize quality and value, further communicate the value of the CDSE, advocate for improved technology, and focus on emerging trends. Additionally, CDSE has also developed a recommended program of study for original and derivative classifiers.

During the fourth quarterly DoD Security Training Council (DSTC)[18] meeting on September 9, 2016, the DSTC voted to establish a Security Education, Training, and Awareness Working Group. The Security Education, Training, and Awareness Working Group will focus on identifying community best practices for security awareness training, evaluating outreach practices to enhance dissemination of security awareness and mandatory training, and identification of security training awareness needs.

Assessment of Management Actions

We determined that the recommendation to develop a plan to enhance outreach to the security community to expand awareness of the DSS CDSE, and to ensure that original and derivative classifiers receive timely and relevant training was implemented.

We surveyed 1,988 derivative classifiers to determine the level of awareness about the CDSE and available course offerings. We found that of the 1,830 derivative classifiers who responded to this question, 973 (approximately 53 percent) had not heard of the CDSE. However, 1,793 (approximately 90 percent of all surveyed derivative classifiers) had received biennial derivative classification training.

While the first percentage may indicate that greater outreach is needed, the second percentage reflects that training might occur through systems that interface with CDSE, but reside on organizational-specific training sites. This aligns with what we learned during an interview of CDSE personnel regarding training that occurs through systems that interface with CDSE, but reside on organizational-specific training sites.

For example, we were informed that CDSE provides security training to the Air Force, which is hosted on an Air Force website. The Air Force keeps track of the students taking the courses with the primary goal of ensuring that they meet requirements to receive relevant and timely training that is tailored to current

[18] The DoD Security Training Council serves as an advisory body on DoD security education and training to the USD(I) and is managed by the Director of the DSS as the functional manager for the execution of DoD security training. The DSTC provides a forum for DoD entities to discuss and coordinate security education and training issues and policies, recommend education and training standards and criteria, identify emerging education and training needs, and promote professional development and certification programs for the security practitioner workforce. The DSTC serves as the governance board for the Security Professional Education Development Certification Program. Membership in the DSTC is comprised of DoD entities with security responsibilities and others as determined by the Chair.

policy, procedures, rules, and regulations. However, they don't require the students to acquire a training certificate, so the student would take a CDSE-developed course, but without requesting a completion certificate at the end would be unaware that it was a CDSE course.

This occurs with other websites/training systems where CDSE-provided training is overlaid on the host website/training system. The users may not be aware that they are accessing CDSE sites until they are required to get certificates.

Additionally, DoD Manual 5200.01, Volume 1, states that DSS provides information security education and training for DoD as required by DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13, 2014. However, there is no mention of CDSE. So even if a student was familiar with the policy, they would be unaware that the CDSE is the office in the DSS that provides the training.

OUSD(I) has worked with DSS to improve awareness of the CDSE at the organizational level through engagement at the DISAB, and the DSTC, the inclusion of CDSE links on OUSD(I)'s security website, and a commitment to clarify CDSE roles and responsibilities in policy updates where applicable.

In addition, the DSTC provides an opportunity for members to learn about CDSE course offerings. The CDSE security web based training links are featured on the OUSD(I) Security Policy and Oversight Division web site to reinforce available training opportunities.

To improve the quality of training, OUSD(I)'s Security Policy and Oversight Division collaborates with DSS and CDSE staff on annual security training requirements. Recent collaborative efforts have resulted in training and job aids for original classification, derivative classification, and marking of classified information. OUSD(I) monitors the effectiveness of training through the review of mandatory Component self-inspections to ensure compliance with established policy.

Another example of the benefit of using the DSS CDSE was highlighted in a February 13, 2014, review conducted by ISOO, "Results of the On-site Review at U.S. Cyber Command (CYBERCOM)."

In the report, ISOO recommended to U.S. Cyber Command that, "The Defense Security Service's (DSS) Center for the Development of Security Excellence (CDSE) is an excellent source for the security training needed to enhance CYBERCOM's security education and training program, especially in the areas of derivative classification and marking of classified documents."

Conclusion

The OUSD(I) implemented the recommendations by increasing delivery methods for security training courses and broadened its outreach efforts, with the goal of improving timeliness of training provided to original and derivative classifiers, through the establishment of a Security Education, Training, and Awareness Working Group and CDSE-initiated Voice of the Community review, increasing outreach while determining the needs of stakeholders.

Additionally, ongoing initiatives, including a Security Awareness Hub, additional eLearning and instructor-led courses, and the Security Training, Education, and Professionalization Portal support our findings that CDSE has implemented additional course offerings that are consistent with policy and tailored to original and derivative classifiers.

These efforts, along with policy updates and coordination at the organizational level, are consistent with DODIG-2013-142 recommendations that DoD enhance outreach to the security community and ensure that training is tailored to current policy, procedures, rules, and regulations.

Appendix A

Scope and Methodology

This follow-up evaluation was conducted from October 2015 to September 2016, in accordance with Quality Standards for Inspection and Evaluation that the Council of the Inspectors General on Integrity and Efficiency issued. Those standards require that we plan and perform the evaluation to obtain sufficient evidence for our findings and conclusions based on our stated objective. To accomplish the objective, we:

- submitted surveys and received responses from 1,988 Air Force and Navy derivative classifiers. The information was entered into an Access database which was used to analyze responses and identify trends;
- surveyed OCAs and Security Managers and received 106 responses. This information was also entered into an Access database for evaluation and trends analysis;
- reviewed 254 classified documents to include e-mails, examined documents submitted by Service Security Managers, and reviewed information resulting from post FY 2013 parametric searches of documents residing on Secret Internet Protocol Router Network Intelink.[19] We entered information into a Secret Internet Protocol Router Network-examined self-inspection reporting results for FYs 2013, 2014, and 2015;
- examined Standard Forms 311, "Agency Security Classification Management Program Data" for FYs 2013, 2014, and 2015;
- reviewed SCGs at the DTIC website revised or added after September 30, 2014 through July 28, 2016 (DTIC lists 197 updated or added SCGs from FY 2014 to July 28, 2016. Of that number, 109 were hyperlinked and applicable to this review. We entered information from the SCGs into an Access database for evaluation and trends analysis);
- received documents from and conducted interviews of OUSD(I) security personnel;
- interviewed DTIC personnel to gain information specific to the DTIC processes and the DTIC SCG repository; and
- consulted with ISOO and coordinated throughout the evaluation with other IG offices, during both evaluations as the Act directs, to ensure our evaluations followed a consistent methodology to allow for cross agency comparisons.

[19] Intelink is a group of secure intranets used by the U.S. Intelligence Community. It provides an essential capability for the U.S. intelligence community and its partners to share information, collaborate across agencies, and conduct business.

We received results from evaluations by the ISOO and the Defense Threat Reduction Agency, who used their own procedures to write findings and recommendations. The DoD OIG did not verify the information provided.

As we did in 2013, we evaluated the information security programs of the Departments of the Navy and of the Air Force. We evaluated these departments because they represented organizations, as described in EO 13526, that would have information eligible for classification, the unauthorized disclosure of which could reasonably be expected to cause identifiable or explainable damage to the national security.

Computer-Processed Data

We did not rely on computer-processed data to perform this evaluation.

Use of Technical Assistance

We did not receive any technical assistance for this evaluation.

Prior Coverage

During the last 5 years, DoD OIG has issued one report that addressed issues specific to this followup evaluation. Unrestricted DoD OIG reports are at http://www.dodig.mil.

GAO

During the last 5 years, GAO issued no reports addressing topics specific to this follow-up evaluation.

DoD OIG

Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013

Information Security Oversight Office

During the last 5 years, the Information Security Oversight Office issued five reports addressing issues specific to the DoD:

ISOO Review, "Results of the On-site Review at U.S. Cyber Command (CYBERCOM)," February 13, 2014

ISOO Review, "On-site Review at Joint Base Langley-Eustis," October 7, 2014

ISOO Review, "On-site Review and Appraisal at the Chief of Naval Operations (CNO)," December 18, 2014

ISOO Review, "On-site Review of the Defense Advanced Research Projects Agency (DARPA)," April 16, 2015

ISOO Review, "On-site Review of the Office of the Joint Chiefs of Staff (JCS)," October 13, 2015

Appendix B

Update on Observations

Observations from DODIG Report No. 2013-142

In our 2013 report, we observed the effectiveness of policies for developing classification decisions, classification by derivative classifiers, effectiveness of self-inspection programs, and Intelligence Community Cross-Cutting Issues. While there was need for improvement in all areas, because DoD was in the early stages of addressing these challenges, we believed the most effective method of oversight was to monitor these challenges and then identify and assess DoD's improvements in our 2016 report under PL 111-258.

Assessment of Management Actions

After reviewing Annual Senior Agency Official Self-Inspection Program[20] details, we determined that the self-inspection program description, assessment and summary, specific discrepancy reports, and successful practices, still provide a comprehensive picture of DoD's overall security program management efforts.

In 2013, we identified instances where dissemination control markings were incorrectly applied, which potentially impeded the sharing of information. For this report, we reviewed 254 classified documents obtained through data calls and pulled from Intelink searches on the SECRET Internet Protocol Router Network.

We noticed improvements in the marking of documents with an error rate of 63 percent versus 70 percent. We also found that the error rate for reviewed e-mails decreased from 100 percent in the 2013 report to 85 percent for this current evaluation. This could be reflective of the use of classification management tools, as well as training. Of the 106 security managers surveyed, 46 or 43 percent identified the presence of email classification management tools within their organization.

We previously mapped DoD issuances to EO 13526 and 32 CFR, Part 2001, to assist our review to ensure policies were followed and adopted at the organizational level. Our review of policy updates showed that policies for developing classification decisions, guiding derivative classifier decisions, and protecting intelligence sources and methods were still aligned with EO 13526.

[20] EO 13526 and 32 CFR Part 2001.60, require agencies to establish and maintain an ongoing self-inspection program and to report the results of self-inspection programs annually. This program provides Senior Agency Officials designated by each DoD Component with the information needed to oversee and assess the effectiveness of each agency's CNSI program.

We also determined that DoD policy provides guidance on managing dissemination control markings, especially as it pertains to information regarding intelligence sources, methods, or activities.

Conclusion

Our review of DoD policy updates confirmed that policies are still aligned with EO 13526. Moreover, in our review of SCGs, we found no instances where information was originally classified for reasons other than the defined areas for classification. We also reviewed 254 classified documents and noted a decrease in the percentage of documents with errors from 70 percent to 63 percent. Derivative classifying has improved due to enhanced policy and training efforts, and the use of classification management tools. This positive trend is consistent with our current assessment that ongoing initiatives, policy improvements, and outreach are helping minimize over-classification.

As a result of our analysis of 2014 and 2015 DoD self-inspection reports, we found that the self-inspection programs still provide a comprehensive picture of DoD's overall security program management efforts.

DoD policy provides guidance on managing dissemination control markings, especially as it pertains to information regarding intelligence sources, methods, or activities. While there is room for enhancing the accuracy of classification markings, there has been continual improvement since our 2013 report.

Appendix C

Assessment of the Status and Implementation of Recommendations in DoD Office of Inspector General Report (DODIG-2013-142) as Reported to Congress in 2015 by the Under Secretary of Defense for Intelligence

House Report 113-446, accompanying H.R. 4435, the Howard P. "Buck" McKeon National Defense Authorization Act for FY 2015, requests the Secretary of Defense submit a report to the congressional defense committees not later than March 1, 2015, on the status and implementation of the recommendations found in the DoD OIG's report, ''DOD Evaluation of Over-Classification of National Security Information'' (DODIG–2013–142). The report, submitted by the USD(I) on behalf of the Secretary of Defense, detailed specific actions taken on recommendations and included timeframes for implementing remaining recommendations. The following table reflects the verbatim text submitted to Congress on April 9, 2015, by the USD(I) and the DoD OIG assessment of the status and implementation of the recommendations in DODIG-2013-142.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
Recommendation A.1 – We recommend that the Under Secretary of Defense for Intelligence:		
A.1 – Provide the implementation status of DoD Component actions to include a critical element on security in the Component's performance evaluations.	Completed Action: On June 12, 2013, the USD(I) directed the heads of the DoD Components to integrate the critical element of security in the performance contract or other applicable rating system for certain personnel, including those specified in section 5.4 of EO 13526. An extensive list of actions, initiatives and policies completed in 2013 and 2014 is at attachment.	☐ Completed/Verified ☒ In Process ☐ Other The USD(I) did direct the heads of the DoD Components to integrate the critical element of security in the performance evaluations for original and derivative classifiers; however, our analysis shows that not all derivative classifiers have the critical element of security in their performance evaluations.
	Ongoing Initiative/Action: The USD(I) Human Capital Management Office (HCMO) is working to revise the DoD performance management regulation (DoD Instruction 1400.25). That revision is currently being coordinated within the Department in March 2015.	☒ Completed/Verified ☐ In Process ☐ Other This initiative was completed on May 7, 2016, when the requirement to include a critical element on security was incorporated into DoD Instruction 1400.25, Volume 2011, "DoD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Performance Management."
	The DoD Components are also in the process of adjusting/updating Component policies, performance appraisal systems, and performance contracts, as applicable.	☐ Completed/Verified ☒ In Process ☐ Other Based on our analysis, there were no updated Component policies. We did determine that as of July 27, 2016, 1,630 of 1,988 (82 percent) original and derivative classifiers we surveyed have a critical element on security in their performance evaluations.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
Recommendation A.2 – We recommend that the Under Secretary of Defense for Intelligence revise policy to incorporate template language for security classification guides that is consistent with the intent of EO 13526, as follows:		
A.2.a – Section 5.3 of EO 13526 and Enclosure 4, paragraph 22 of DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, contain guidance for individuals who wish to challenge information that they believe has been improperly or unnecessarily classified.	Completed Action: DoD Manual 5200.01, Volume 1 "DoD Information Security Program: Overview, Classification, and Declassification," February 2, 2012, Enclosure 4 (in paragraph 22) established such "Challenges to Classification" procedures within the Department and requires DoD personnel who have substantial reason to believe that information is improperly or unnecessarily classified, to communicate that belief to their security manager or the original classification authority (OCA) to bring about any necessary correction. These challenge procedures are encouraged among Components to resolve issues involving potentially over-classified information.	☐ Completed/Verified ☒ In Process ☐ Other OUSD(I) has incorporated the language for encouraging challenges as stated in Section 5.3 of EO 13526 in DoD Manual 5200.01, Volume 1; however, DoD Manual 5200.01, Volume 1 is undergoing final review.
	Ongoing Initiative/Action: OUSD(I) will emphasize these challenge measures during a forum for all Component Security Managers in March 2015. OUSD(I) Security Policy & Oversight Directorate (SPOD) is also drafting an Information Security "Policy Short" memorandum to further emphasize and encourage classification challenges in April 2015.	☐ Completed/Verified ☐ In Process ☒ Other OUSD(I) could not implement this initiative because Policy Shorts no longer exist; however; language encouraging challenges has been incorporated in DoD Manual 5200.01, Volume 1; however, DoD Manual 5200.01, Volume 1 is undergoing final review (see below).
	Ongoing Initiative/Action: DoD guidance regarding classification challenge procedures will be further strengthened in a revision to Volume 1 of DoD Manual 5200.01 (DoD-M). SPOD is in the process of drafting a change to this Volume to fully address this recommendation, as well as other recommendations, as described below. We anticipate initiating informal coordination within the Department by May 2015.	☐ Completed/Verified ☒ In Process ☐ Other For this initiative, OUSD(I) has incorporated the language for encouraging challenges as stated in Section 5.3 of EO 13526 in DoD Manual 5200.01, Volume 1; however, DoD Manual 5200.01, Volume 1 is undergoing final review.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
A.2.b – Such challenges are encouraged and expected and should be forwarded through the appropriate channels to the office of primary responsibility.	Completed Acton: The procedures described in DoD-M 5200.01, Volume 1 Enclosure 4 paragraph 22 not only "encourage and expect" such challenges, but they explicitly direct DoD personnel to contact their component security manager or the OCA to obtain clarification or to challenge the classification, as appropriate.	☐ Completed/Verified ☒ In Process ☐ Other OUSD(I) has incorporated the language stated in Section 5.3 of EO 13526 in DoD Manual 5200.01, Volume 1; however, DoD Manual 5200.01, Volume 1 is undergoing final review.
	Ongoing Initiative/Action: To better manage the lifecycle of classified information, SPOD is developing a DoD pilot project to identify and examine opportunities to bring forward classification challenges in the Military Departments and smaller DoD Components that cannot be effectively and efficiently resolved at a lower level-in effect, to work the "supply" side of potential Over-Classification situations. This project will be an agenda item at the meeting of the Defense Information Security Advisory Board (DISAB) in March 2015.	☐ Completed/Verified ☒ In Process ☐ Other The OUSD(I) has not yet begun this initiative.
A.2.c – Pending final decision, handle and protect the information at its current classification level or at the recommended change level, whichever is higher.	Completed Action: The procedures described in DoD-M 5200.01, Volume 1 Enclosure 4 paragraph 22 specifies that information that is the subject of a classification challenge shall remain classified and continue to be safeguarded unless and until a decision is made to declassify it.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language concerning the handling and protection of current or recommended classification level was added to DoD Manual 5200.01, Volume 1, Enclosure 4, paragraph 22, which is currently undergoing review.
	Ongoing Initiative/Action: To further strengthen this policy, our response to this part of Recommendation A will be accomplished via the forthcoming change to DoD-M 5200.01, Volume 1 described above.	☐ Completed/Verified ☒ In Process ☐ Other DoD Manual 5200.01, Volume 1 is currently undergoing review.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
A.2.d – Challenges should include sufficient description to permit identification of the specific information under challenge with reasonable effort.	Completed Action: The procedures described in DoD-M 5200.01, Volume 1 Enclosure 4 paragraph 22 specify that formal challenges to classification shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language from Section 5.3 of EO 13526 was added to DoD Manual 5200.01, Volume 1, Enclosure 4, paragraph 22, which is currently undergoing review.
	Completed Action: To help better explain and demonstrate the differences between formal (infrequent) and informal (nearly daily, recurring) classification challenge procedures, in January 2014, we invited US GAO representatives to review one such informal challenge that OUSD(I) SPOD and DoD CIO jointly lodged in response to a major NSC-level initiative that was over-classified. The DoD successfully petitioned the NSC to downgrade the classification associated with the initiative, based on informal action officer level communications, a methodology by which the bulk of classification challenges are handled throughout the OSD staff and DoD Components.	☒ Completed/Verified ☐ In Process ☐ Other We were informed by OUSD(I) representatives that this meeting had taken place; however, it was after we published our 2013 report. Also, for this follow up effort, based on 1,988 DoD derivative classifiers we surveyed, we knew that derivative classifiers were aware that DoD policy encourages classification challenges if information is incorrectly classified. Moreover, 135 survey participants indicated that they have challenged incorrect classification levels either through formal processes (e.g., contacting the office of primary responsibility) or informal channels (e.g., seeking clarification).
	Ongoing Initiative/Action: To further strengthen this policy, our response to this part of Recommendation A will be accomplished via the forthcoming change to DoD-M 5200.01, Volume 1 described above.	☐ Completed/Verified ☒ In Process ☐ Other DoD Manual 5200.01, Volume 1 is currently undergoing review.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
A.2.e – Challenges should include detailed justification outlining why the information is improperly or unnecessarily classified.	Completed Action: The procedures described in DoD-M 5200.01, Volume 1 Enclosure 4 paragraph 22 specify that challenges to classification made by DoD personnel shall also include the reason why the challenger believes that the information is improperly or unnecessarily classified.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language from Section 5.3 of EO 13526 was added to DoD Manual paragraph 22, which is currently undergoing review.
	Ongoing Initiative/Action: To further strengthen this policy, our response to this part of Recommendation A will be accomplished via the forthcoming change to DoD-M 5200.01, Volume 1 described above.	☐ Completed/Verified ☒ In Process ☐ Other DoD Manual 5200.01, Volume 1 is currently undergoing review.
Recommendation B – We recommend that the Under Secretary of Defense for Intelligence:		
Direct Component reviews of OCA positions to ensure that the position is needed.	Completed Action: SPOD on a recurring basis encourages DoD Components to reduce OCA positions that are no longer required.	☐ Completed/Verified ☒ In Process ☐ Other On April 16, 2015, the USD(I) issued a memorandum directing DoD Components to validate each OCA position to assess whether that position is still required. However, of the 106 Security Managers we surveyed to determine whether their organization had conducted a review to establish the requirement for OCA authority, we found that 87 Components had not conducted a review, while 15 organizations had.
	Ongoing Initiative/Action: SPOD is currently staffing a memorandum for USD(I) signature on this topic, which will direct DoD Components to validate each OCA position to assess whether that position is still required. We anticipate completion, signature, and delivery of this memorandum by April 2015.	☒ Completed/Verified ☐ In Process ☐ Other On April 16, 2015, the USD(I) issued a memorandum directing DoD Components to validate each OCA position to assess whether that position is still required.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
Recommendation C – We recommend that the Under Secretary of Defense for Intelligence, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics, incorporate into policy that:		
C.1 – Security Classification Guides forwarded to the Defense Technical Information Center must be forwarded with the requisite DD Form 2024, and signed by the appropriate Original Classification Authority to ensure accountability.	Completed Action: The requirement for OCAs to submit their SCGs to Defense Technical Information Center (DTIC) with a DD Form 2024 is already described in DoD Manual 5200.01, Volume 1, Enclosure 6.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language from Section 2.2 of EO 13526 was added to DoD Manual 5200.01, Volume 1 Enclosure 6, which is currently undergoing review.
	Ongoing Initiative/Action: USD(I) will reinforce this requirement in the Information Security "Policy Short" memorandum described above and through a change to DoD-M 5200.45, which will begin coordination within the Department by December 2015.	☐ Completed/Verified ☐ In Process ☒ Other Policy Shorts no longer exist. Instead, OUSD(I) is in the process of updating DoD Manuals 5200.45 and 5200.01, Volume 1; however, those policies are undergoing review.
C.2 – Defense Technical Information Center not accept DD Forms 2024 that are not completely filled out and signed by the appropriate agency.	Ongoing Initiative/Action: The requirement for completed and signed forms will be reinforced in a forthcoming draft Information Security "Policy Short" (mentioned above) in April 2015 and in the change to DoD-M 5200.45 (described above) to begin coordination by December 2015.	☐ Completed/Verified ☐ In Process ☒ Other Policy Shorts no longer exist. Instead, OUSD(I) is in the process of updating DoD Manuals 5200.45 and 5200.01, Volume 1; however, those policies are undergoing review.
C.3 – A time requirement for the submission of updated SCGs be established.	Completed Action: DoD-M 5200.01, Volume 1, Enclosure 6 requires OCAs to review SCGs at least every five years or sooner as needed. OCAs are required to submit a DD Form 2024 annotated with the date of the next scheduled review.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language from Section 2.2 of EO 13526 was added to DoD Manual 5200.01, Volume 1, Enclosure 6, which is currently undergoing review.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
C.4 – Reminders be sent to organizations as SCGs near biennial review requirements	Completed Action: DoD conducted a comprehensive Fundamental Classification Guidance Review (FCGR) in 2012. As a result of this effort, more than 97% of DoD's SCGs were updated and/or declared current. IAW the 5 year review cycle, DoD is on track and on schedule to begin the next scheduled comprehensive oversight review in 2017.	☐ Completed/Verified ☒ In Process ☐ Other Clarifying language from Section 2.2 of EO 13526 was added to DoD Manual 5200.01, Volume 1 Enclosure 6, which is currently undergoing review. SCGs have improved and, as with the 2012 FCGR, the 2017 FCGR will provide a further opportunity for enhancements – especially with the close involvement of the Director of National Intelligence.
	Ongoing Initiative/Action: OUSD(I) SPOD will collaborate with DTIC to develop a methodology to send reminders to DoD Component OCAs when their SCGs are scheduled for review and update. This initiative is an agenda item for the DISAB meeting in March 2015.	☐ Completed/Verified ☒ In Process ☐ Other OUSD(I) is coordinating with DTIC (OUSD(I) is the proponent for the policy, while DTIC maintains the repository for the SCGs) and will invite DTIC to the December 2016 DISAB, followed by regularly scheduled meetings thereafter, to discuss refining processes.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
Recommendation D – We recommend that the Under Secretary of Defense for Intelligence develop a plan to:		
D.1 – Enhance its outreach to the security community to expand awareness of the Center for Development of Security Excellence (CDSE).	Completed Action: OUSD(I) SPOD reviews annual security training requirements with DSS and CDSE staff. As a result of this collaboration, we then work to improve existing courses, or develop new course offerings for the DoD. Recent examples of such collaboration to ensure accurate classification and avoidance of over classification include development of training and job aids for: Original Classification, Derivative Classification, and marking of classified information.	☒ Completed/Verified ☐ In Process ☐ Other The OUSD(I) implemented the recommendations through increased collaboration with DSS CDSE. The DSS CDSE increased delivery methods for security training courses and broadened its outreach efforts, with the goal of improving timeliness of training provided to original and derivative classifiers, through the establishment of a Security Education, Training, and Awareness Working Group and CDSE-initiated Voice of the Community review, increasing outreach while determining the needs of stakeholders.
	Completed Action: CDSE personnel are invited to attend meetings of the DISAB, a forum for all Component Information Security managers, and help develop its Agenda. The DISAB thus serves as a key forum for DoD Information Security professionals to learn about CDSE offerings and training. CDSE security web based training links are featured on the Security Policy and Oversight Division web site to reinforce available training opportunities.	☐ Completed/Verified ☒ In Process ☐ Other The DISAB is a meeting for Information Security Managers where CDSE officials can brief on new courses, methods of delivery, etc. Many DoD Security reps visit the OUSD(I)'s Security Policy and Oversight Division website. So the exposure to CDSE officials and/or their courses and products is passed along to the Component Security officials.
	Ongoing Initiative/Action: The OUSD(I) plans to expand awareness of the CDSE by clarifying its role and capabilities in a forthcoming change to DoD-M 5200.01, Volume 3 and to start coordination of that change in April 2015.	☐ Completed/Verified ☐ In Process ☒ Other Regarding this initiative, through our analysis of DoD Manual 5200.01, Volume 3, the policy broadly discusses security training and education, but does identify DSS, the higher-level organization for CDSE, as a viable alternative for training needs.

Recommendation	OUSD(I) 2015 Response	OIG Assessment of Status of Recommendations
D.2 – Ensure all original and derivative classifiers receive relevant and timely training that is tailored to current policy, procedures, rules, and regulations.	Completed Action: OUSD(I) monitors the OCA and derivative classifier training of each DoD Component annually during the mandatory Component Self-Inspections to ensure completeness and compliance with DoD-M 5200.01 Volume 3 Enclosure 5.	☒ Completed/Verified ☐ In Process ☐ Other Ongoing initiatives, including a Security Awareness Hub, additional eLearning and instructor-led courses, and the Security Training, Education, and Professionalization Portal support our findings that CDSE has implemented additional course offerings that are consistent with policy and tailored to original and derivative classifiers.

Appendix D

Information Security Oversight Office – Best Practices

Information Security Oversight Office On-Site Reviews

The ISOO reviewed Cyber Command (CYBERCOM), the Defense Advanced Research Projects Agency (DARPA), The Office of the Chief of Naval Operations, Joint Base Langley – Eustis, and the Joint Chiefs of Staff, to determine the degree to which the CNSI program was being implemented in accordance with EO 13526 and its implementing directive, 32 CFR Part 2001, and to provide recommendations for improvements, as needed. Additionally, the reviews also appraised the policies, procedures, and practices that are currently in place to protect information that is not classified but still requires protection based on law, regulation, or Government-wide policy. During the reviews, the ISOO identified the following best practices:

Cyber Command

- **Information Assurance**: CYBERCOM has targeted online training available from work or home. The staff is certified in accordance with Baseline Level Requirements outlined in DoD Directive 8570, "Information Assurance Workforce Improvement Program," and proactive measures are in place to ensure authorized and secured access to information.
- **Cyber Security**: CYBERCOM applies the principle of least privilege which promotes minimal user profile privileges based on a user's job requirements. Least privilege ensures mission effectiveness and mitigates the risk of classified information compromise. In addition, CYBERCOM employs a multi-factor authentication policy for computer login and trains personnel to report computer incidents via a Computer Security Incident report. Finally CYBERCOM strictly adheres to National Security Agency policies governing any and all use of personal electronic devices.
- **Policy, Program Management, and Safeguarding Practices**: CYBERCOM has a number of policies in place that inform agency personnel of the measures necessary to protect sensitive information. These policies identify specific information types as well as the measures necessary to ensure their protection and timely dissemination to authorized recipients. CYBERCOM's operations security Critical Information List provides employees with detailed information on what to protect and how to protect it. CYBERCOM also operates a "clean desk" policy where no classified or sensitive information is left out after normal working hours. Burn bags used by individual employees are secured in lockable containers at the end of each work day.

- **Training**: Training is tracked using an Electronic Learning Management System. Annual training includes Privacy Awareness Training and Introduction to Information Security. Information Security training reinforces information security policies and procedures related to classification, operations security, privacy, and the Freedom of Information Act. ISOO noted that Critical Information List reference guides were found on employee workstations, near computers, phones and fax machines along with operations security awareness posters and forms. Overall, ISOO found CYBERCOM's training and awareness program to be impressive.

Defense Advanced Research Projects Agency

- **Program Management**: DARPA Security and Intelligence Division develops a monthly statistical report that tracks metrics for information, personnel, and industrial security programs. The monthly status reports provide the Agency Head and Senior Agency Official with a timely snapshot of DARPA's on-going security status.
- **Safeguarding**: DARPA maintains a Classified Document Registry which is responsible for the accounting, receipting, transmission, internal dissemination and destruction of classified materials. The Classified Document Registry also performs all classified media operations and conducts data transfers across all classified DARPA networks. ISOO concluded that these efforts represented DARPA management's resolve to effectively safeguard and account for the CNSI information under its control.
- **Security Violations**: DARPA's security incident reports reference the training received by the offender relating to the specific incident, as well as the currency of that training. This practice allows for security managers to pinpoint specific areas that need to be emphasized during recurring security training.
- **Information Assurance Program Management and Classified System Management**: ISOO identified DARPA as an early adopter of the Defense Information Systems Agency Assured Compliance Assessment Solution tool used for asset discovery, security risk assessment and identification, network scanning, and policy scans which support internal guidelines. DARPA also successfully implemented the Crisis Action Team Incident Response Tracking System which provides an automated tool for incident management and reporting. ISOO noted that DARPA was an early adopter of a Risk Management Framework for information assurance.

- **Cyber Security**: DARPA has a Cyber Action Response Team that focuses on prevention, preparation, planning, incident management, recovery, mitigation, remediation, post incident analysis, and lessons learned. Moreover, 98 percent of the DARPA cybersecurity/information assurance workforce meets the DoD baseline certification requirements. DARPA has a very robust training tracking system that monitors certification compliance every 30, 45, and 90 days.

Chief of Naval Operations

- **The Office of the Chief of Naval Operations Security Coordinator Program**: The Office of the Chief of Naval Operations Security Coordinator program is comprehensive and ensures effective implementation of the security standards in place across the Chief of Naval Operations' organization.
- **Electronic Shielding**: The Command's use of electronic shielding enclosures (i.e., Black Hole Faraday Bags) to protect their open storage areas from the electronic emissions resulting from the storage of personally owned telecommunication devices in equipment lock boxes was noted as a best practice.
- **Security Reinforcement**: Command staff members who violate security procedures that result in a security incident or violation are required to brief their co-workers on their actions at the next all-hands meeting of their organization. This best practice instills the importance of compliance with security requirements, provides a focus on incidents occurring in their specific organization, and provides a venue for reinforcing proper security practices.
- **Systems Access**: Joint Worldwide Intelligence Communications System access has an enforced prerequisite. A security proficiency test prerequisite exists to demonstrate knowledge and attitude of employees regarding the protection of the physical and especially, information assets of that organization.
- **Electronic Spillage Tracking Tool**: The Electronic Spillage Action Form is an effective tool to report loss or compromise of classified information which ensures that such incidents are properly investigated, identify dangerous practices, and that necessary actions are taken to negate or minimize impact.
- **Information Assurance**: Information Assurance awareness training is provided via different sources and is constantly reinforced. Command Information Assurance Managers and training officers are responsible for tracking and reporting compliance to meet annual Federal Information Security Management Act requirements.

- **Least Privilege**: The Command applies the principle of least privilege to ensure mission effectiveness and to mitigate the risk of classified information compromise. Not only must the asset of information be secured, the hardware to access information must also be safeguarded from unauthorized access. The Command institutes a multi-factor authentication policy for computer login resulting in stronger cybersecurity procedures.
- **Personal Electronic Devices Security**: The Command strictly adheres to DoD and Command policies governing any and all use of Personal Electronic Devices. Interviews revealed that Command personnel have been inculcated to accept this adherence as second nature.
- **Security Coordinators Appointments**: Coordinators are appointed in writing. The Command Security Manager maintains a current listing of all appointed Security Coordinators.
- **Security Guidance**: Security serviced activities have Standard Operating Procedures, internal memorandums, or guidance that highlight the responsibilities of the Security Coordinator as well as assigned personnel. Newly assigned personnel are provided a copy of these procedures.
- **File Exchange System**: The Command uses a secure file exchange system (Safe Access File Exchange) to securely send For Official Use Only files and/or files containing personally identifiable information to recipients inside and outside the Command.

Joint Base Langley – Eustis

- The Command created a unique database to track classified contracts. The Command/Information Protection office has developed a comprehensive database that allows for the tracking of on-going classified contracting actions at both installations.
- Security self-inspection program criteria is included in the Management Internal Control Toolbox process. The Management Internal Control Toolbox promises to provide decision makers an effective way to track trends and other issues developed as a result of the security self-inspection reporting process.
- The classified systems management program is a comprehensive and well-designed program consisting of proactive incident handling techniques employing a quick reaction checklist which provides incident handling guidance when an individual suspects there has been spillage.
- Command access to classified information is closely managed and delivered to the desktop via thick, thin, and ultra-thin clients. The command uses a server-based computing model in which the end user's computing device has no local storage.

- The Command Emergency Management program is defined as a cross-functional program that integrates procedures and standards for planning, logistical requirements, emergency response actions, emergency response guidelines and exercises, and evaluations.
- Command policies and procedures collectively establish a security framework that addresses the protection of sensitive information from its initial designation or identification through authorized release as well as incident investigation and mitigation.
- All Unit Security Managers are appointed, in writing, by their commanding officer.
- Unit maintains a current listing of all appointed security managers. Currently, the Command has over 200 appointed Security Managers.
- Unit maintains a SharePoint site for Unit Security Managers that contains up-to-date training and awareness materials.
- Unit developed a number of templates that serve to standardize the way the Unit Security Manager program is implemented throughout the Command. In addition, all Unit Security Managers maintain a "Security Manager's Handbook."
- Required annual training for Service personnel (including contract personnel) is delivered and tracked using Electronic Learning Management Systems. Unit specific training is delivered and tracked by Unit Security Managers and supervisory personnel training records (i.e., certificates, sign-in sheets, etc.) are retained within each unit.
- The Command has developed a quarterly newsletter to address security issues and topics. This product contains the names and contact information for all security managers within the Command. This product reinforces security practices and procedures related to day-to-day operations.

Joint Chiefs of Staff

- The DD Form 254 provides security requirements and classification guidance on classified contracts. The Command instituted a formalized electronic tracking and approval process that requires formal concurrence before the form can be issued.
- The Command has developed an Information Security Continuity Book that provides flowcharts for tracking security reporting processes. The mapping of the security functions and use of flowcharts to delineate required security functions is a best practice that should be shared with other DoD elements to ensure a continuity of process and conformity to requirements.

- The Command provides consistent Information Assurance training and effectively enforces user compliance with training requirements. The training is very specific, is tracked via a portal and addresses the protection of Personally Identifiable Information, safeguarding of classified information, and information otherwise deemed sensitive.
- Self-reporting is encouraged. Individuals responsible for information assurance incidents are subject to appropriate administrative, disciplinary, or criminal action.
- The Command displays a high level of commitment to security for classified systems with the implementation of a comprehensive cyber training and incident handling program. The staff displayed a proactive, progressive, and coordinated approach to detecting and responding to cyber events and incidents.
- ISOO also noted the use of collaboration dashboard tools to create real time situational awareness. The executive dashboard works by collecting real-time information into one place in a more accessible format.

Acronyms and Abbreviations

CDSE	Center for Development of Security Excellence
CFR	Code of Federal Regulations
CNSI	Classified National Security Information
CYBERCOM	Cyber Command
DARPA	Defense Advanced Research Projects Agency
DISAB	Defense Information Security Advisory Board
DSS	Defense Security Service
DSTC	DoD Security Training Council
DTIC	Defense Technical Information Center
EO	Executive Order
FCGR	Fundamental Classification Guidance Review
IG	Inspector General
ISOO	Information Security Oversight Office
OCA	Original Classification Authority
PL	Public Law
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
SCG	Security Classification Guide
SF	Standard Form
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I)	Office of the Under Secretary of Defense for Intelligence

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
www.dodig.mil/pubs/email_update.cfm

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098