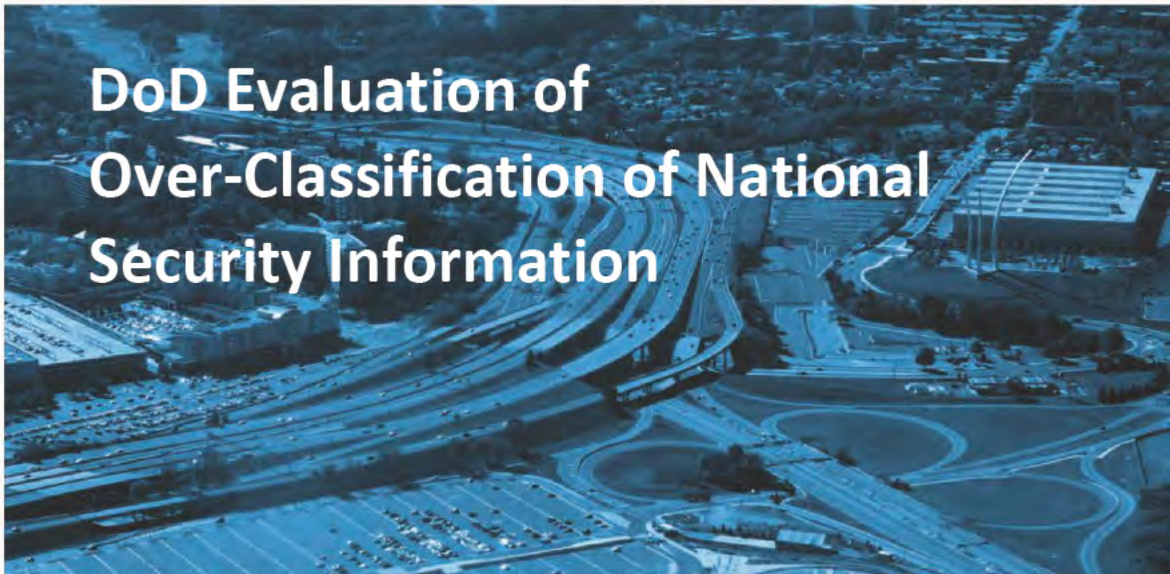
Report No. DODIG-2013-142

Inspector General

Department of Defense

September 30, 2013

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 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.

Fraud, Waste and Abuse

HOTLINE

1.800.424.9098 • www.dodig.mil/hotline

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

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

September 30, 2013

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

SUBJECT: DoD Evaluation of Over-Classification of National Security Information (Report No. DoDIG-2013-142)

We are providing this report for your review and comment. This is the first of two reports designed to evaluate the effectiveness of policies, procedures, rules, regulations and management practices that may be contributing to persistent misclassification and over-classification within the Department. Our second evaluation will review progress made pursuant to the results of this evaluation and completed no later than September 30, 2016. We issued a draft of this report on September 16, 2013.

We considered comments from the Director of Security Policy and Oversight, Office of the Deputy Under Secretary of Defense for Intelligence and Security and Acting Assistant Secretary of Defense for Research and Engineering, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics in preparing the final report. Management concurred with our recommendations; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments on Recommendations A1, A2, B, C1, C2, C3, C4, D1, and D2 by October 31, 2013.

We appreciate the courtesies extended to the staff. Please direct questions to [redacted] at (703) 699-[redacted] (DSN 499-[redacted] or the Project Manager at (703) 699-[redacted] (DSN 499-[redacted].

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

(U) THIS PAGE INTENTIONALLY LEFT BLANK

Results in Brief

DoD Evaluation of Over-Classification of National Security Information

September 30, 2013

Executive Summary of DODIG-2013-142

What We Did

This is the first of two reports that Public Law 111-258, Section 6(b) requires, mandating Inspectors General of Federal departments, or agencies with an officer or employee who is authorized to make original classifications, to: (A) assess whether applicable classification policies, procedures, rules, or regulations have been adopted, followed, and effectively administered; and (B) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material. In this report, we address eight areas associated with classification management and control marking programs. For the second report due under Public Law 111-258 on September 30, 2016, we will focus on follow-up efforts to recommendations outlined in this report.

What We Found

We found that applicable classification policies, procedures, rules, and regulations have been adopted; however, in some circumstances, they had not been followed or effectively administered.

We also concluded that some policies, procedures, rules, regulations or management practices may be contributing to persistent misclassification of material. While we did find some instances of over-classification, we do not believe 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. 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-assessments and fundamental classification guidance review results, demonstrating that DoD is aware of weaknesses and is striving to improve. The most common discrepancy was incorrect marking of documents. Many of our interviewees commented on the availability and robustness of training.

While room for improvement still exists, DoD continues to make advances in program management, reporting costs, reporting of security classification activities, and in advancing policies that will help constrain over-classification.

What We Recommend

We recommend that the Under Secretary of Defense for Intelligence and for Acquisition, Technology, and Logistics carry out the recommendations outlined in this report and continue to leverage the new Defense Security Enterprise, especially with regard to ensuring that Original Classification Authorities are fully engaged and accountable.

Management Comments and Our Response

Both the Under Secretary of Defense for Intelligence and the Under Secretary for Acquisition, Technology, and Logistics concurred with the recommendations; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments. Please see the recommendations table on the back of this page.

Visit us on the web at www.dodig.mil

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Intelligence	A1, A2, B, C1, C2, C3, C4, D1, D2	
Under Secretary of Defense for Acquisition, Technology, and Logistics	C1, C2, C3, C4	

* Please provide comments by October 30, 2013

Acronyms and Abbreviations

C.F.R.	Code of Federal Regulations
DNI	Director of National Intelligence
DSE	Defense Security Enterprise
DSEAG	Defense Security Enterprise Advisory Group
DSE ExCom	Defense Security Enterprise Executive Committee
DSS	Defense Security Service
E.O.	Executive Order
GAO	Government Accountability Office
IC	Intelligence Community
IG	Inspector General
ISOO	Information Security Oversight Office
JWICS	Joint Worldwide Intelligence Communication System
OCA	Original Classification Authority
ODNI	Office of the Director of National Intelligence
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OSD	Office of the Secretary of Defense
P.L.	Public Law
SAO	Senior Agency Official
SF	Standard Form
SIPRNET	SECRET Internet Protocol Router Network
USD(I)	Under Secretary of Defense for Intelligence

Distribution:

Senate Committee on Homeland Security and Governmental Affairs

Senate Select Committee on Intelligence

Senate Committee on Appropriations, Subcommittee on Defense

House Committee on Homeland Security

House Committee on Appropriations, Subcommittee on Defense

House Committee on Oversight and Government Reform

House Permanent Select Committee on Intelligence

Director, Information Security Oversight Office

Table of Contents

Introduction

Objective

In accordance with Public Law (P.L.) 111-258, Section 6(b), and in consultation with the Information Security Oversight Office (ISOO),[1] our objective is to evaluate the policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material; and ascertain if the applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered. This project will facilitate the timely reporting required by the Public Law to address efforts by DoD to decrease over-classification; and promote information sharing and transparency in operations in compliance with the law.

Background

Executive orders since 1940 have directed government-wide classification standards and procedures. On December 29, 2009, President Obama signed Executive Order (E.O.) 13526, "Classified National Security Information," which establishes the current principles, policies, and procedures for classification. The E.O. prescribes a uniform system for classifying, safeguarding, and declassifying national security information. E.O. 13526 also reflects the President's expressed belief that this nation's progress depends on the free flow of information, both within the Federal Government and to the American people. Accordingly, protecting information critical to national security and demonstrating a commitment to open government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

Under E.O. 13526, classified information that has been determined to require protection against unauthorized disclosure to prevent damage to national security must be marked appropriately to indicate its classified status.

[1] 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 National Security Council.

Information may be originally classified[2] only by Original Classification Authorities (OCAs): these are individuals authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to initially classify information. OCAs must receive training on proper classification prior to originally classifying information and at least once per calendar year after that. By definition, original classification precedes all other aspects of the security classification system, including derivative classification,[3] safeguarding, and declassification. Information on the six-step process for determining an original classification decision is detailed in Appendix A, Observation A.

All personnel with an active security clearance can perform derivative classification, unless an agency limits this activity to specific personnel. All personnel who apply derivative classification markings must receive training on the proper application principles of E.O. 13526 prior to derivatively classifying information and at least once every two years thereafter. Information may be derivatively classified from a source document or documents, or by using a classification guide.

Authorized holders of information (including authorized holders outside the classifying organization) who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of information.

Federal Government organizations that create or hold classified information are responsible for its proper management. Classification management includes developing security classification guides (SCGs) that an OCA uses to provide a set of instructions 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.

One of the most effective ways to protect classified information is through the application of standard classification markings or dissemination control markings. Effective program management also includes comprehensive mandatory training for classifiers and a robust self-inspection program.

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

[3] Derivative classification is incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly-developed material consistent with the classification markings that apply to the source information. It includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Federal departments and agencies also may have systems of restrictive caveats that can be added to a document in the form of dissemination control and handling markings. These restrictions are not classifications in and of themselves; rather, they identify the expansion or limitation on distributing the information. These markings are in addition to, and separate from, the level of classification. Only those external dissemination control and handling markings approved by ISOO -- or approved by the Director of National Intelligence (DNI) for intelligence and intelligence-related information--may be used by agencies to control and handle the dissemination of classified information under agency regulations, policy directives, and guidelines which are issued under E.O. 13526. Such approved markings must be uniform and binding on all agencies and must be available in a central registry.

Two significant changes to the classification program under the issuing of E.O. 13526 involve making classified information accessible, to the maximum extent possible, to authorized holders. If significant doubt exists about the appropriate level of classification, *information shall be classified at the lower level*. Additionally, *if significant doubt exists about the need to classify information, it should not be classified.*

The term "over-classification" is not defined in national policy. E.O. 13526 defines "classification" and "declassification," but not this term. During our evaluation and in this report, we have used a working definition of "over-classification," which 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 E.O. 13526.

Scope and Methodology

This evaluation was conducted from October 2012 to September 2013, 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, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. To accomplish our evaluation, we:

- examined fundamental classification guidance review (FCGR) results;
- examined self-inspection reporting results;
- examined Standard Forms 311, "Agency Security Classification Management Program Data";

- reviewed relevant policies, regulations, and related studies;
- reviewed 1,260 classified documents;
- reviewed 342 SCGs;
- conducted a survey of Defense Component security managers, and original and derivative classifiers;
- interviewed 21 original classification authorities and 129 derivative classifiers;
- interviewed key Department officials responsible for security training and related policy development and implementation; and
- interviewed officials responsible for the Department's information security program.

We also used an evaluation guide that a working group of participating IGs, led by the OIG DoD, 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 P.L. 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 website: www.ignet.gov/CIGIE Reports and Periodicals/List by Year/2013/, "A Standard User's Guide for Inspectors General Conducting Evaluations under Public Law 111-258, the Reducing Over-Classification Act."

As the Act directs, we consulted with ISOO and coordinated throughout the evaluation with other IG offices with the goal of ensuring that our evaluations followed a consistent methodology to allow for cross-agency comparisons.

The evaluation focused on eight areas: General program management responsibilities; OCAs; original classification; derivative classification; self-inspections; reporting; security education and training; and Intelligence Community (IC) cross-cutting issues.

To discern whether departmental policies and practices were consistent with E.O. 13526 and 32 C.F.R., Part 2001, we used the following evaluation tools that ISOO developed:

- an agency regulation implementing assessment tool;
- methodology for determining whether an original classification decision is appropriate;
- original classification authority interview coverage;
- methodology for determining the appropriateness of a derivative classification decision; and
- derivative classifier interview coverage.

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

We evaluated the information security programs of the following organizations:

- Department of the Navy;
- Department of the Air Force; and
- Combatant Commands.

We evaluated these departments and entities because they represented organizations, as described in E.O. 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.

We did not evaluate declassification issues because ISOO recently completed its five-year on-site assessment of agency declassification programs. Details are in the 2012 Annual Report to the President, of June 20, 2013, and is at http://www.archives.gov/isoo/reports/. This oversight and assistance program garnered significant measureable improvements in the quality of declassification reviews that executive branch departments and agencies conducted. ISOO will continue its assessment program in a manner that sustains this high level of quality. Assessments focused on three areas of concern: missed equities, inappropriate referrals, and improper exemptions.

Finding A

Effectiveness of Security Program Management

We found that some organizations had a critical element on security in their performance evaluations, while others did not. This has been a requirement since at least 1997 but has not been enforced. Without the critical element for security in performance evaluations, there is little accountability for ensuring the proper marking and classification of documents. We also found that SCG template instructions for those who want to challenge classification was not consistent with the intent of E.O. 13526. Current policy does not require language that encourages challenges and provides appropriate citations to assist in the challenge process. Therefore, derivative classifiers do not have adequate information on how to challenge a classification or assurance that the information they do have is supported in law and regulation, which can negatively impact information sharing if information is incorrectly classified or misclassified and allowed to remain unchallenged.

We also found that while security program management needs improvement, DoD has made significant progress in this area. We mapped DoD issuances to E.O. 13526 and 32 C.F.R., Part 2001, and as a result, found that policies were adopted at the Office of the Secretary of Defense-level, although they had not yet been adopted at the agency level, which may contribute to persistent misclassification of material. To significantly enhance security program management and provide a governance mechanism to bring about an enterprise approach to strategic oversight and advocacy of DoD security capabilities, the USD(I) published, on October 21, 2012, DoD Directive 5200.43, "Management of the Defense Security Enterprise," creating, for the first time, a Defense Security Enterprise (DSE) and attendant strategic framework to address security issues.

Security is a Department-wide priority necessary to protect its resources. Management of an organization's security program can encompass many security disciplines, use extensive resources, and incorporate various policies. Some finding areas (for example, self-inspection, training and education, and reporting) would be aligned under the security program management. However, for this report's purposes, we have also categorized those areas separately to further highlight the role they play to protect classified national security information. Additionally, we have added a section on IC cross-cutting issues to emphasize those areas that are associated with the IC, such as external dissemination control and handling markings that the DNI approves that may affect sharing of information.

General Program Management

In a June 2006 evaluation of DoD's information security program, the Government Accountability Office (GAO) found that a lack of oversight and inconsistent implementation of the DoD's information security program increased the risk of misclassification. Misclassifying national security information impedes effective information sharing, can provide adversaries with information to harm the United States and its allies, and can cause the U.S. to incur millions of dollars in avoidable administrative costs. GAO identified weaknesses in the areas of classification management training, self-inspections, and security classification guide management.

Since August 2010, the Office of the Deputy Inspector General for Intelligence and Special Program Assessments, OIG, DoD, has conducted a series of assessments of Security within DoD, as follows: Tracking and Measuring Security Costs; Training, Certification and Professionalization; Security Policy; and the soon-to-be published Classification and Grading of Security Positions. We will continue to do oversight of DoD's security programs. We will update the progress of security program management in our 2016 report under P.L. 111-258.

This section will focus on the core issues related to managing the classified national security information program. General program management refers to the responsibilities of departments and agencies carrying out the program under E.O. 13526. These responsibilities include the agency head demonstrating personal commitment to the program, committing necessary resources to ensure its effective implementation, and appointing a senior agency official (SAO) to direct and administer the program. The SAO's responsibilities include:

- overseeing the program established under E.O. 13526;
- issuing implementing regulations;
- establishing and maintaining an on-going self-inspection program;
- ensuring that designating and managing classified information is included as a critical rating element in the systems used to rate OCAs, security managers or security specialists, and all other personnel whose duties significantly involve creating or handling classified information, including those who apply derivative classification markings;

- establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance as needed to personnel on proper classification; and
- establishing and maintaining security education and training programs.

Security is a mission-critical function of DoD, and properly executed, has a direct impact on all DoD missions and capabilities and on the national defense. We reviewed the classification management program and the use of dissemination control markings to ensure the following:

- that necessary resources have been dedicated for effectively carrying out the program;
- that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information; and
- that an SAO has been designated to direct and administer the program.

The Under Secretary of Defense for Intelligence (USD(I)) is the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense regarding security. In this capacity, the USD(I) exercises the Secretary of Defense's authority, direction, and control over the Defense Agencies and DoD Field Activities that are Defense security Components and exercises planning, policy, and strategic oversight over all DoD security policy, plans, and programs. The USD(I) serves as the DoD Senior Security Official under E.O. 13526, and advises the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Heads of other DoD Components on developing and integrating risk-managed security and protection policies and programs, except for Nuclear Physical Security.

The USD(I) also develops, coordinates, and oversees carrying out DoD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DoD Special Access Program security, as well as research, development, and acquisition protection.

To significantly enhance security program management and provide a governance mechanism to bring about a united approach to strategic oversight and advocacy of DoD security capabilities, the USD(I) published DoD Directive 5200.43, "Management of the Defense Security Enterprise," which:

- establishes policy and assigns responsibilities for managing the DSE;
- establishes the DSE Executive Committee (DSE ExCom) and provides direction for a comprehensive DSE policy and oversight framework and governance structure to safeguard personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences;
- deconflicts the DSE from other DoD security-related functions, such as force protection, and provides for the alignment, synchronization, support, and integration of those related security functions;
- assigns responsibilities related to the DSE to the Defense Security Executive; and
- provides a common lexicon for the DSE.

Since the DSE's creation, the USD(I) has advanced enterprise management of security by chairing the DSE ExCom (the Deputy Under Secretary of Defense for Intelligence and Security serves as the chair), and the DSE Advisory Group (DSEAG -- the Director, Security Policy and Oversight Directorate, Office of the Deputy Under Secretary of Defense for Intelligence and Security [DUSD(I&S)] serves as the chair).

The DSE ExCom:

- advises the USD(I), as the Defense Senior Security Official, on security policy and training; provides recommendations on key policy decisions and opportunities for standardization and improved effectiveness and efficiency; and on carrying out cross-functional security policy coordination;
- oversees carrying out the Defense security framework;
- approves the strategic plan and monitors its execution;
- commissions reviews and in-depth studies of security issues and, based on the results, makes recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging security challenges;
- reviews resource investments and priorities and recommends changes to the Defense security program to the USD(I), through the Defense Security Executive;

- assists with developing a Defense security framework that integrates, across all security levels, personnel, physical, industrial, information, and operations security, as well as special access program security policy and critical program information protection policy. This framework must align with, and be informed by, other DoD security and security-related functions (e.g., counterintelligence, information assurance, nuclear physical security, chemical and biological agent security, foreign disclosure, security cooperation, technology transfer, export control, cyber security, anti-terrorism, force protection, mission assurance, critical infrastructure, and insider threat policy);

- provides a forum for identifying, documenting, and disseminating best practices, including those associated with security risk management; and

- identifies performance measures to be used to assess the effectiveness of the Defense security program and its contribution to mission success.

To focus on the most challenging enterprise security issues, the DSEAG charters project teams, on an as needed basis, to develop solutions to some of the most pressing DSE priorities. A few key initiatives being addressed by current project teams include reforming the personnel security investigation process, quantifying security-related costs across the Department, developing an enterprise-wide risk methodology, establishing a Defense Security Enterprise Architecture, improving continuous evaluation capabilities, and professionalizing the security workforce.

The Security Policy and Oversight Directorate has also established the Defense Security Oversight and Assessment Program (DSOAP) to address an Office of the USD(I) (OUSD(I)) strategic priority to put into operation Defense security policies and transform the security community. The program is a collaborative engagement designed to assess the effectiveness of security policies in the operational environment. Oversight visits enable OUSD(I) to:

- identify best practices and lessons learned for trend analysis and program improvement;

- develop and issue security policies that are current, operationally relevant, adaptable, and informed by an assessment of risk;

- execute an effective outreach and oversight program to improve security policy and inform the DSE strategic direction;
- identify and champion security best practices and enterprise capabilities; and
- capture Component issues with DoD security policy in order to improve policy (gaps, conflicts, lack of clarity).

As part of its strategic framework, the DSE has developed three key goals to aid in making better risk-based mitigation decisions regarding threats and security vulnerabilities related to all DoD assets across the DSE, as follows:

- standardize security functions across DoD to achieve synergistic execution and enhance operations;
- allocate security resources to demonstrate a return on investment; and
- improve individual performance to develop a cadre of highly-skilled security professionals

From a program management perspective, the DSE can begin to effectively address many of its challenging security issues by collaborating with DoD senior leaders and security subject matter experts, and through DSE members. These members are:

- the DoD Component security program executives designated by the Secretaries of the Military Departments and the Chairman of the Joint Chiefs of Staff;
- representatives of the Under Secretaries of Defense for:
    - (Comptroller)/Chief Financial Officer;
    - Acquisition, Technology, and Logistics;
    - Policy; and
    - Personnel and Readiness;
- the DoD Chief Information Officer;
- the Director of Administration and Management;
- the DoD General Counsel;
- the Director, DoD Special Access Program Central Office; and
- the Director, Counterintelligence Directorate, Office of the DUSD(I&S).

Effectiveness of Classification Management Policies and Control Marking Guidelines

Standardized classification and control markings are the primary means by which the IC protects intelligence sources, methods, and activities. Properly applying and using these markings promotes information sharing while allowing the information to be properly safeguarded from inadvertent or unauthorized disclosure. Agencies are required to issue regulations to carry out their classified national security information programs in accordance with E.O. 13526 and 32 C.F.R. Part 2001.

We used an "Agency Regulation Implementing Assessment Tool," which ISOO provided. The tool focuses on eight key areas for determining if applicable classification policies, procedures, rules, and regulations have been adopted in accordance with E.O. 13526 and 32 C.F.R. Part 2001. On April 2, 2013, the USD(I) published DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," and on February 24, 2012, the USD(I) published DoD Manuals 5200.01, in four volumes:

- Volume 1 -- DoD Information Security Program: Overview, Classification, and Declassification;
- Volume 2 -- DoD Information Security Program: Marking of Classified Information;
- Volume 3 -- DoD Information Security Program: Protection of Classified Information; and
- Volume 4 -- DoD Information Security Program: Controlled Unclassified Information (CUI)

We mapped these issuances to E.O. 13526 and 32 C.F.R., Part 2001. As a result, we found that policies were adopted at the Office of the Secretary of Defense-level. We subsequently provided the regulation assessment tool to component-level IGs to map Office of the Secretary of Defense-level issuances to the agency-level policy issuances. We found that most agency policies had not yet been updated to reflect the guidance provided in the four volumes of DoD Manuals 5200.01.

DoD Manual 5200.01, Volume 2, "Marking of Classified Information," February 24, 2012, Appendix 2 to Enclosure 4, discusses dissemination control markings for intelligence information.

Intelligence Community Directive (ICD) 710, "Classification Management and Control Markings System," June 21, 2013, governs the carrying out and oversight of the IC classification management and control markings system, which provides the framework for accessing, classifying, disseminating, and declassifying intelligence and intelligence-related information to protect sources, methods, and activities. The IC markings system is implemented and maintained through the Controlled Access Program Coordination Office (CAPCO) Register and Manual.

ICD 710 applies to the IC and to such elements of any other department or agency, as may be designated an element of the IC by the President or jointly by the DNI and the head of the department or agency concerned. ICD 710 applies, under EO 13526, Section 6.2(b), to the handling of intelligence and intelligence-related information and, under EO 13556, "Controlled Unclassified Information," November 4, 2010, Section 6(b), to the handling of unclassified intelligence or intelligence-related information that requires safeguarding through dissemination controls. Also see Appendix A, Observation D.

Performance Evaluations

E.O. 13526 requires that the performance contract or other system used to rate civilian or military personnel performance includes the designating and managing of classified information as a critical element or item to be evaluated in the rating of OCAs, security professionals, or other personnel whose duties significantly involve handling classified information, including derivative classifiers.

Dating to at least 1997, DoD has required that the performance appraisal contain a critical element. This policy (previously stated in DoD 5200.1-R, "Information Security Program," paragraph C1.1.2.1., and now rescinded) stated: "Management of classified information shall be included as a critical element or item to be evaluated in the rating of original classification authorities, security managers or specialists, and other personnel whose duties primarily involve the creation or handling of classified information," and is now found in DoD Manual 5200.01, Volume 1, Enclosure 2, paragraph 7h. We found that carrying out this requirement ranged from organizations not having the critical element in their appraisals, to organizations that have maintained this language since the original requirement.

On June 12, 2013, the USD(I) published a 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," DoD Components integrate the requirements into their performance evaluation system. It also directs that Components give the Director, Security Policy and Oversight Directorate, Office of the DUSD(I&S), an estimated date, no later than September 30, 2013, for Component implementation. This requirement also includes information system security personnel, if their duties involve access to classified information and information system personnel (e.g., system administrators) with privileged access to classified systems or network resources.

Once implementation plans are received, we will monitor the carrying out of the performance appraisal critical element tasking for protecting classified information and report the results in our 2016 report under P.L. 111-258.

Classification Challenges

Authorized holders of information who, in good faith, believe that the information's classification status is improper are encouraged and expected to challenge the information's classification status. An agency head or senior agency official should establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures should ensure that: Individuals are not subject to retribution for bringing such actions; an opportunity is provided for review by an impartial official or panel; and individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel.

DoD Manual 5200.01 -- Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, Enclosure 4, Section 6, states: "If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the OCA to bring about any necessary correction. This may be done informally or by submitting a formal challenge to the classification."

During our interviews, few instances were encountered where interviewees challenged a classification, and in those instances where challenges were made, interviewees said they were satisfied with how the challenge was resolved. Interviewees said that training successfully addressed classification challenges.

Our office examined 254 SCGs available online, which revealed that only 37.5 percent of SCGs included guidance for individuals who want to challenge or question the level of classified information. Such guidance is consistent with Section 1.8 of E.O. 13526 which states that "authorized holders of information who, in good faith, believe that its classification status is improper are *encouraged and expected* to challenge the classification status of the information." SCGs that include classification challenge guidance allow for a transparent process that provides derivative classifiers with the means to question the classification of potentially improperly classified information.

Such guidance also provides derivative classifiers with the assurance that the challenge process is supported. Current guidance for classification challenges as set forth in DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, reads as follows: "Classification Challenges.

If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR [office of primary responsibility]."

While this provides for classification challenges, it does not reflect the intent of E.O. 13526 which states that such challenges are "encouraged." Moreover, the paragraph does not provide derivative classifiers with the appropriate citations to help in the challenge process.

Incentives for Accurate Classification

Public Law 111-258, Section 6(a) states that "In making cash awards under chapter 45 of title 5, United States Code, the President or the head of an Executive agency with an officer or employee who is authorized to make original classification decisions or derivative classification decisions may consider such officer's or employee's consistent and proper classification of information."

We did not find information related to incentives for accurate classification in the policies we reviewed, nor did we find any instances where organizations provided incentives for accurate classification, whether cash or otherwise.

Sanctions

E.O. 13526 provides that officers and employees of the U.S. Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 13526 or predecessor orders; classify or continue classifying information in violation of this order or any implementing directive; create or continue a special access program contrary to this order's requirements; or contravene any other provision of this order or its implementing directives. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

If the ISOO Director finds a violation of the order, the Director shall file a report with the agency head or to the SAO so that corrective steps, if appropriate, may be taken. We found that policy covered sanctions, and OCAs and derivative classifiers were aware of possible sanctions. Our interviewees did not provide any instances where a sanction had been imposed.

The agency head, SAO, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying E.O. 13526 classification standards. The agency head or SAO shall take appropriate and prompt corrective action and notify the ISOO Director when certain violations occur.

DoD Manual 5200.01 -- Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, Enclosure 3, Section 17, states: DoD military and civilian personnel may be subject to criminal or administrative sanctions if they knowingly, willfully, or negligently:

- disclose to unauthorized persons information properly classified;
- classify or continue the classification of information;
- create or continue a special access program contrary to the requirements of DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010;
- disclose controlled unclassified information to unauthorized persons; or
- violate any other provision of the Manual.

Sanctions include, but are not limited to: warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss, or denial of access to classified information and/or CUI, and removal of classification authority. Criminal prosecution may also be undertaken in accordance with sections 801-940 of title 10, U.S.C. (also known as "The Uniform Code of Military Justice") and other applicable U.S. criminal laws.

If an individual is delegated to have OCA demonstrates reckless disregard or a pattern of error in applying classification standards, the appropriate official shall, as a minimum, remove the offending individual's OCA.

Conclusion

We found that while security program management needs improvement, DoD has made significant progress in this area. Since August 2010, the Office of the Deputy Inspector General for Intelligence and Special Program Assessments, OIG, DoD, has conducted a series of assessments of Security within DoD, as follows: Tracking and Measuring Security Costs; Training, Certification and Professionalization; Security Policy; and the soon-to-be published Classification and Grading of Security Positions. We will continue to do oversight of DoD's security programs. We will update the progress of security program management in our 2016 report under P.L. 111-258.

We mapped DoD issuances to E.O. 13526 and 32 C.F.R., Part 2001, and, as a result, found that policies were adopted at the Office of the Secretary of Defense-level, but had not yet been adopted at the agency level. While some organizations had a critical element on security in their performance evaluations, the USD(I) directed that Components provide, no later than September 30, 2013, an estimated date for implementation for all DoD Components –- we will monitor and report on this implementation's progress in our 2016 report under P.L. 111-258.

We found few instances where interviewees challenged a classification, and in those instances where challenges were made, interviewees said they were satisfied with how the challenge was resolved. Interviewees said that their training successfully addressed classification challenges. We found that policy covered sanctions and OCAs and derivative classifiers were aware of possible sanctions. We did not find any situation where a sanction had been imposed. We also found no incentives existed for accurate classification either in policy or organizational programs.

To significantly enhance security program management and provide a governance mechanism to bring about an enterprise approach to strategic oversight and advocacy of DoD security capabilities, the USD(I) published, on October 21, 2012, DoD Directive 5200.43, "Management of the Defense Security Enterprise," creating, for the first time, a DSE and attendant strategic framework to address security issues. The USD(I) has also created the DSE ExCom and the DSEAG to provide senior-level guidance, involvement, organization, and focus to critical security issues.

Recommendations, Management Comments, and Our Response

A. We recommend that the Under Secretary of Defense for Intelligence:

1. Provide the implementation status of DoD Component actions to include a critical element on security in the Component's performance evaluations.

2. Revise policy to incorporate template language for security classification guides that is consistent with the intent of E.O. 13526, as follows:

   a. Section 5.3 of Executive Order 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.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with our recommendations.

Our Response

The Under Secretary of Defense for Intelligence concurred with our recommendations; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments by October 30, 2013.

Finding B

Effectiveness of Original Classification Authorities

We found that [in some instances] OCAs had not made many, if any, classification decisions. A detailed review of those positions had not been conducted. OCAs inherit the classification authority of the position, and in some cases the requirements of the position have evolved and classification authorities are no longer needed. This could result in the unnecessary allocation of security resources to support nonessential OCAs, as well as having more OCAs than are essential for producing classified national security information.

Each OCA we interviewed had received training and to ensure the effectiveness of their decisions, relied heavily on their security staffs. OCAs do not remain in their positions for an extended time.

This section will focus on the individuals who have the authority to initially classify information –- these are the OCAs. An OCA is delegated in writing, according to position, by the President, the Vice President, or by an agency head or other official designated by the President, to initially classify information.

DoD Manual 5200.01, Volume 1, Enclosure 4, states OCAs shall be approved only when:

- there is a demonstrable and continuing need to exercise OCA during the normal course of operations. (As a general rule, absent a security classification guide, an OCA must exercise this authority an average of twice a year to justify and retain designation as an OCA.);
- such demonstrable and continuing need cannot be met through issuance of security classification guides by existing OCAs in the chain of command;
- referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical for reasons such as geographical separation; and
- sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making.

The responsible OCA shall issue security classification guidance for each system, plan, program, project, or mission involving classified information. Classification guidance may be in the form of a memorandum, plan, order, or letter, or issuance of a security classification or declassification guide.

OCAs shall develop, as appropriate, automatic and systematic declassification guidance for use in review of records that are of permanent historical value and 25 years old or older. This guidance shall be published in the appropriate classification or declassification guide.

Where classification guidance is issued in the form of an SCG, the OCA shall ensure the guide is reviewed and updated.

As a general rule, classification authority must be exercised an average of twice a year to qualify for retention of the OCA designation if an OCA does not issue and maintain an SCG.

Designation of Original Classification Authority, Program Knowledge, and Training

OCAs, also called original classifiers, include the President, Vice President, Secretary of Defense, the Secretaries of the Military Departments, and other DoD officials who have been specifically delegated this authority in writing. When OCA is granted, OCAs are delegated classification authority specific to a level of classification and cumulative downwards. For example, an OCA appointed with Top Secret classification authority may classify information at the Top Secret, Secret, and Confidential levels. An OCA appointed with Confidential classification authority may only classify information at the Confidential level.

OCAs may only classify information that is under their area of responsibility, such as a specific project, program, or type of operation. For example, it would be inappropriate for an air wing commander to classify information about a Navy undersea warfare program.

We determined that OCAs were properly designated. We conducted interviews of OCAs to evaluate their knowledge of classification management procedures. The interviews were intended to help gauge if these individuals' job position required having OCA and if the individuals have expert knowledge of the information and classification requirements to ensure that information is not over-classified.

We found that OCAs had received the required training and had satisfactory knowledge of classification principles and procedures.

Most OCAs interviewed had made few, if any, original classification decisions; had not been confronted with classification challenges -- either as one who made such a challenge or as an OCA who might have to respond to such a challenge; had sparingly used classification guides; or created classification guides/guidance. As a general rule, classification authority must be exercised an average of twice a year to qualify for retention of the OCA designation if an OCA does not issue and maintain an SCG.

Conclusion

We found that OCAs were properly designated, knowledgeable of classification requirements to ensure that information is not over-classified, and received the required training. We also found that most of the OCAs interviewed had made few, if any, original classification decisions or been confronted with classification challenges to classification decisions.

Recommendation, Management Comments, and Our Response

B. We recommend that the Under Secretary of Defense for Intelligence direct Component reviews of OCA positions to ensure that the position is needed.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with our recommendations.

Our Response

The Under Secretary of Defense for Intelligence concurred with our recommendation; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments by October 30, 2013.

Finding C

Effectiveness of Component Statistical and Cost Reports

Although SCGs are now on the DTIC website, more effective management of the SCGs is needed to ensure their accuracy and OCA involvement. While organizations may have updated SCGs, this information is not always provided in a timely manner to DTIC. In the absence of updated SCGs, derivative classifiers run the risk of citing wrongly classified or unnecessarily classified information potentially resulting in the unnecessary allocation of resources to protect improperly classified materials.

DoD's annual estimates of original and derivative classification decisions are unreliable because those decisions are based on data from DoD components that were derived using different assumptions about what should be included and about data collection and estimating techniques.

This section focuses on how well DoD gathers information and reports on the state of its security program. Determining DoD's effectiveness will be based on the evaluation of the accuracy of statistics, the fundamental classification guidance review, self-inspection results, and program costs, as reported to ISOO. While not all-inclusive, this section will discuss DoD's policies for incorporating essential elements for reporting, such as statistical reporting (SF-311); accounting for costs (Cost Report); and fundamental classification guidance review results.

Statistical Reporting

Standard Form (SF) 311 is used to collect data from Executive branch agencies that create and/or handle classified national security information. Requested information includes the number of original classification authorities, number of original and derivative classification decisions, number of mandatory declassification review requests and appeals, number of pages declassified, number of inspections conducted, and number of classification guides. The results from these forms are included in the annual report to the President. Executive Order 13526, "Classified National Security Information," and its government-wide implementing directive, 32 C.F.R. Part 2001, require Executive branch agencies to report statistics related to their security classification programs to ISOO.

In a June 2006 report, GAO stated that DoD's estimate of how many original and derivative classification decisions it makes annually is unreliable because those decisions are based on data from the DoD components that were derived using different assumptions about what should be included and about data collection and estimating techniques.

Nevertheless, this estimate is reported to the President and to the public. If the processes for collecting and manipulating data are properly implemented, data reliability could be improved, but only if the processes address the underlying lack of uniformity in how the individual DoD components are collecting and manipulating their data to arrive at their estimates.

We found the same lack of uniformity with respect to the collection of SF 311 data throughout DoD. However, DoD and other federal government agencies that use SF 311 have been working with ISOO to make this form more relevant.

Each fiscal year, DoD Components are required to submit a consolidated SF 311 report concerning their Information Security Classification Management Program. The SF 311 report should include a total number of classification decisions regardless of media -- electronic presentations, email, official correspondence or memoranda, photographs, reports and/or intelligence products, web pages, and wiki articles and blog articles.

Previously, ISOO asked agencies to report only the number of classified "finished products," a term which originated in the paper-based era and was often not easily applied in the electronic environment. However, because of the increasing use of the electronic environment to share and disseminate information, we need to consider more than just the "finished product" concept and instead count all classification decisions, regardless of the type of media. It was further requested that each reporting agency adjust its counting or sampling methodology to include such web applications as email, wikis, and blogs.

ISOO initiated discussions with agency representatives to explore reforms of the SF 311 reporting process. The consensus from these discussions focused on the need for a proposal to change the reporting requirements in Part E, "Mandatory Declassification Review Requests and Appeals." That section of the SF 311 was updated, and ISOO remains open for further discussion on improving the form.

Accounting for Costs

An FY 2012 ISOO cost report found that combined costs for Government and industry security classification activities amounted to $10.96 billion. This is a decrease from FY 2011 of $1.66 billion, or 13 percent. ISOO reports annually to the President on the estimated costs associated with agencies' implementation of E.O. 13526, and E.O. 12829, as amended, "National Industrial Security Program."

ISOO relies on the agencies to estimate and report the costs of the security classification system. Even if reporting agencies had no security classification activity, many of their reported expenditures would continue in order to address other, overlapping security requirements, such as work force, facility and information systems protection, mission assurance operations, and similar needs.

DoD Directive 5200.43 and the DSE Strategic Plan require quantifying security costs. The DSE has created a framework for collecting security costs. The intent is to quantify the cost of security resources regardless of whether they are funded via security or non-security budgets or whether they support security, in part or in total.

Fundamental Classification Guidance Review (FCGR) Results:

In June 2006, GAO found that some of the DoD components and subordinate commands that were examined routinely did not submit copies to a central library, as required, of their SCGs, and documentation that identifies which information needs protection and the reason for classification. Also, some did not track their classification guides to ensure they were reviewed at least every five years for currency, as required. DoD personnel cannot be assured that they are using the most current information to derivatively classify documents. DoD is studying ways to improve its current approach to making security classification guides readily available, Department-wide.

We found that all SCGs were on the DTIC website, with the exception of SCGs marked sensitive or classified.

On April 2, 2013, USD(I) published DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," which requires OCAs to:

- issue and disseminate security classification guidance for each system, plan, program, project, or mission involving classified information under their jurisdiction;
- review security classification guidance issued under their authority once every five years to ensure currency and accuracy or sooner when necessitated by significant changes in policy or in the system, plan, program, project, or mission; and to update the guides as required;
- revise, whenever necessary for effective derivative classification, SCGs issued under their authority;
- provide copies of any security classification guides issued under their authority, as required by DoD Manual 5200.01, Volume 1, Enclosure 6;
- cancel security classification guides when all information the guide specified as classified has been declassified, or when a new classification guide incorporates the classified information covered by the old guide and no reasonable likelihood exists that any information not incorporated by the new guide shall be the subject of derivative classification; and
- coordinate with the Department of Energy, Office of Classification, through the Deputy Assistant Secretary of Defense for Nuclear Matters, whenever OCAs develop or revise SCGs with Restricted Data (RD) or Formerly Restricted Data (FRD) information.

Agencies completed the first executive branch-wide FCGR in FY 2012, a major investment in combating over-classification and limiting secrecy to only that information absolutely necessary to protect the national security. Twenty-five agencies with original classification authority conducted comprehensive reviews of their classification guidance, streamlining, and consolidating of 3,103 classification guides to reflect current circumstances.

As of June 27, 2012, DoD initiated a FCGR on 2,070 SCGs, retiring/cancelling 413 FCGRs, and reporting 1,657 FCGRs as active/current. The DoD FCGR program is a high-interest item for the DSEAG.

With respect to ODNI guidance to the IC, the Defense Intelligence Agency, Geospatial-Intelligence Agency, National Security Agency, and National Reconnaissance Office reported their FCGR execution status directly to ISOO, with a copy provided to the USD(I).

These reviews' purpose was to ensure that guidance reflects current circumstances regarding what information warrants continued classification. Additionally, the reviews identified information that no longer requires classification and can be expedited for declassification. The reviews helped agencies ensure proper classification of information vital to national security, while avoiding over-classification and unnecessary classification of records.

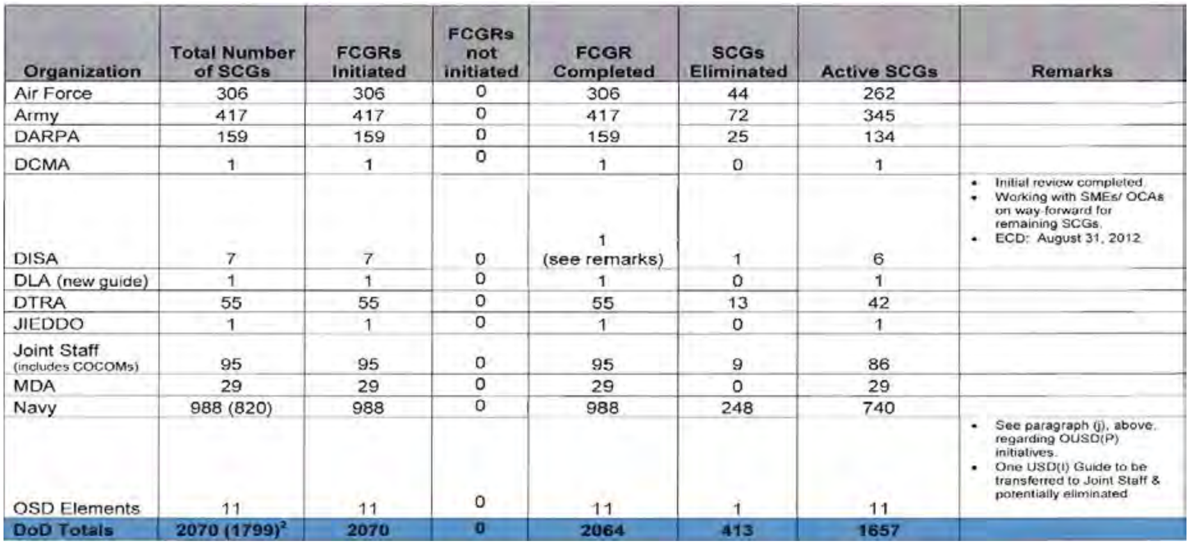
E.O. 13526 directed that the FCGR program be initiated. The order required all federal agencies with significant classification programs to review their classification guidance, and then provide summaries of their reviews to the ISOO Director by July 2012. DoD completed its review within the specified timeframe and submitted its information to ISOO. The final report detailed the status of FCGR activities from 2011-2012 and results achieved to date.

E.O. 13526 also required that these comprehensive reviews of an agency's classification guidance, particularly classification guides, continue periodically to ensure that guidance reflected current circumstances and to identify classified information that no longer required protection and could be declassified. The next review is scheduled to be completed in 2017 and every five years thereafter.

The OUSD(I) administered the review of SCGs throughout DoD. The goal was to centralize SCGs in a repository to ensure the accessibility of guidance to DoD components, and in accordance with E.O. 13526, to update guidance to eliminate redundancies and inaccuracies.

As a result of these efforts, 97 percent of DoD's SCGs were updated and/or declared current, and 20 percent of DoD's non-compartmented[4] SCGs were eliminated. The overarching efforts are reflected below.

DOD COMPONENT-BY-COMPONENT FINAL REPORT
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW



Organization	Total Number of SCGs	FCGRs Initiated	FCGRs not initiated	FCGR Completed	SCGs Eliminated	Active SCGs	Remarks
Air Force	306	306	0	306	44	262	
Army	417	417	0	417	72	345	
DARPA	159	159	0	159	25	134	
DCMA	1	1	0	1	0	1	
DISA	7	7	0	1 (see remarks)	1	6	• Initial review completed • Working with SMEs/ OCAs on way-forward for remaining SCGs. • ECD: August 31, 2012
DLA (new guide)	1	1	0	1	0	1	
DTRA	55	55	0	55	13	42	
JIEDDO	1	1	0	1	0	1	
Joint Staff (includes COCOMs)	95	95	0	95	9	86	
MDA	29	29	0	29	0	29	
Navy	988 (820)	988	0	988	248	740	
OSD Elements	11	11	0	11	1	11	• See paragraph (j), above, regarding OUSD(P) initiatives. • One USD(I) Guide to be transferred to Joint Staff & potentially eliminated
DoD Totals	**2070 (1799)[2]**	**2070**	**0**	**2064**	**413**	**1657**	

We conducted an independent review of SCGs to ensure that accessible information was both current and appropriately classified. To that end, SCGs were pulled from a centralized repository at the Defense Technical Information Center (DTIC), which serves the DoD community as the largest central resource for DoD and government-funded information related to science, technology, engineering, and business. DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, directs organizations to provide a copy of approved SCGs to the Administrator, DTIC, which, in turn, makes the SCGs accessible online to DoD elements.

[4] A term-of-art concerning information that is not derived from intelligence sources, methods, or analytical processes that requires special handling.

DTIC lists 1,822 active SCGs, and of that number, only 1,138 SCGs were linked to documents we were able to review. To ensure consistency with the FCGR, we reviewed SCGs from the Army, Navy, Air Force, Joint Staff, Defense Advanced Research Projects Agency, Defense Threat Reduction Agency, and the Missile Defense Agency. Based on the numbers reflected in the FCGR report, the statistically-supportable stratified sample sizes were determined for SCGs from the respective organizations. The following chart reflects the applied methodology.

Optimum Sample Size for Proportions

Confidence Level	90%
Precision (ME)	5%
z-value	1.645

Organization	Stratum Size	Error Rate	w.sqrt(pq)	wpq	est. sample size	min n	Sample size
Army	345	0.2	0.08	0.03	33.07	30	34
Navy	740	0.2	0.18	0.07	70.93	30	71
Air Force	262	0.2	0.06	0.03	25.11	30	30
DARPA	134	0.2	0.03	0.01	12.84	30	30
MDA	29	0.2	0.01	0.00	2.78	30	29
Joint Staff	86	0.2	0.02	0.01	8.24	30	30
DTRA	42	0.2	0.01	0.00	4.03	30	30
Total	1,638		.40	.16			254

est. sample	156.6	157
tot sample size	254	
Reference:	Cochran, Wm. G. Sampling Techniques, 3rd Ed. 1977 pp. 108-110	

The recommended sample size for some organizations exceeded the number of SCGs available for review. In addition, as noted above, some SCGS were not accessible through the unclassified DTIC site. However, our office did review a total of 254 SCGs.

The review revealed some problems with the guides, which are available on the DTIC website. Guidance from as early as 1997 (Information Security Program, January 1997, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence) required organizations to submit DD Form 2024s, "DoD Security Classification Guide Data Elements," with their approved SCGs. The form allows for greater transparency in determining offices of primary responsibility and OCAs for associated SCGs. Of the 254 SCGs reviewed, less than 44 percent contained this form.

Moreover, 55 percent of the documents reviewed still reference E.O. 12958, which was superseded by E.O. 13526 which was signed on December 29, 2009, as the basis for classification, regrading,[5] or declassification of information, and 4.7 percent contained declassification dates that had already occurred. DoD completed its FCGR in July 2012 and, as noted previously, E.O. 13526 was signed almost three years earlier. As the central repository for unclassified SCGs, the information contained with the DTIC should reflect the most up-to-date guidance for all DoD elements.

Conclusion

We found that DoD's annual estimates of original and derivative classification decisions is unreliable because those decisions are based on data from DoD components that were derived using different assumptions about what should be included and about data collection and estimating techniques. Although SCGs are now on the DTIC website, more effective management of the SCGs is needed to ensure their accuracy and OCA involvement.

Recommendations, Management Comments, and Our Response

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:

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.

2. Defense Technical Information Center 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.

[5] Regrading refers to changing a classification to the appropriate level based on the information being either overgraded (higher than appropriate) or undergraded (lower than appropriate).

4. Reminders be sent to organizations as SCGs near biennial review requirements.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with our recommendations.

Under Secretary of Defense for Acquisition, Technology and Logistics Comments

The Under Secretary of Defense for Intelligence concurred with our recommendations.

Our Response

The Under Secretary of Defense for Intelligence and the Under Secretary of Defense for Acquisition, Technology and Logistics concurred with our comments; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments by October 30, 2013.

Finding D

Effectiveness of DoD Security Education and Training

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 vary 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. This could result in original and derivative classifiers being unaware of the new requirements, improved methodology, or an inability to meet required deadlines. Although the DSS's CDSE offers courses that meet policy requirements and can 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 may be unaware of all available courses.

This section will focus on the effectiveness of DoD's security education and training program(s). While previous sections highlighted training for OCAs and derivative classifiers, this section will not only bring those two training efforts into sharper focus, but will also highlight the efforts of training (including initial, annual refresher, and specialized training) provided to those with security clearances who play an important role in understanding the protection of classified national security information. This section will discuss, briefly, the extent to which DoD put in a security education and training program, in accordance with E.O. 13526 and 32 C.F.R. Parts 2001.70 and 2001.71. It will also indicate whether DoD polices require initial training, refresher training, specialized training, and training for OCAs, and persons who apply derivative classification markings, and whether the policies require suspending OCA and derivative classification authority if these personnel fail to meet the training requirements.

Training and Education Policy

DoD Manual 5200.01, Volume 3, Enclosure 5, states the requirement for security education and training to:

- provide necessary knowledge and information to enable quality performance of security functions;

- promote understanding of DoD Information Security Program policies and requirements and their importance to national security and national interests;
- instill and maintain continued awareness of security requirements; and
- assist in promoting a high degree of motivation to support program goals.

The Manual states that initial, refresher, training for OCAs, and specialized training must be given to persons who apply original and derivative classification markings. It also requires suspending OCA and derivative classification authority if these personnel fail to meet the training requirements.

The Manual further states that security education and training may be accomplished by establishing programs within the DoD Component, or using external resources, such as the CDSE, or a combination of the two. Security education and training shall be conducted continuously, not periodically. Other information and promotional efforts will supplement periodic briefings, training sessions, and other formal presentations to ensure that awareness and performance quality is continually maintained.

The training will include defining a security incident, a violation, and a compromise of classified information, examples of each, and explaining the criminal, civil, and administrative sanctions that may be taken against an individual who fails to comply with program requirements or fails to protect classified information from unauthorized disclosure.

Using job performance aids[6] and other substitutes for formal training is encouraged if determined to be the most effective way to achieve program goals. Circulating directives or similar material on a read-and-initial basis shall not be considered as the sole means of fulfilling any of the Enclosure's specific requirements. While no central tracking system exists, each organization tracks training to ensure that required periodic training is conducted.

[6] Performance aids are sometimes called job aids, which is defined as a repository for information, processes, or perspectives that is external to the individual and that supports work and activity by directing, guiding, and enlightening performance. For example, CDSE uses an OCA DeskTop Reference and a Derivative Classification Training guide, which are used as job performance aids.

CDSE Curriculum Revised to Meet the Requirements of E.O. 13526

OCA and Derivative classifier curriculum complies with the requirements outlined in E.O. 13526 and DoD Manual 5200.01, Volumes 1-4. OCA and Derivative classifiers have the option of receiving their required and refresher training through various training platforms, to include instructor-led, eLearning, job aids, videos, shorts, and webinars. Functional areas taught by CDSE include:

- General Security;
- Cybersecurity;
- Industrial Security;
- Information Security;
- International Security;
- Operations Security;
- Personnel Security;
- Physical Security;
- Sensitive Compartmented Information;
- Special Access Programs; and
- Counterintelligence

CDSE's Education Division offers graduate-level courses designed specifically to develop leaders for the DoD security community. Courses are delivered using a collaborative online learning environment and are available to U.S. military and government employees worldwide. No tuition or fees are required; however, some courses require purchasing textbooks. Most courses have received the American Council on Education's College Credit Recommendation Service ACE College Credit recommendation.

CDSE's Training Division embraces the training challenges that the DoD security community currently faces. With an eye toward innovation, the Training Division offers diverse training courses and products presented through a variety of learning platforms. The Training Division's courses and products continuously meet the needs of each target population's needs and are streamlined to the contemporary learner's performance requirements and busy schedules.

The Security Professional Education and Development program is a DoD security workforce professionalization initiative that DSS administers through the CDSE. The Security Professional Education and Development program supports achievement of community-defined skill standards and serves as a foundation for security workforce professionalization. The Security Professional Education and Development program focuses on three critical elements: Education, Training, and Certification. Detailed information on the Security Professional Education and Development program is in DoD OIG Report No. DoDIG-2011-001, "Assessment of Security Within the Department of Defense – Training, Certification, and Professionalization," October 6, 2011.

The CDSE has a number of ways it conducts outreach, as follows:

- Facebook -- http://www.facebook.com/#!/pages/CDSE-Center-for-Development-of-Security-Excellence/111635548863732. CDSE uses Facebook to relay information about upcoming classes and new products. CDSE also relays information from other sources about the work that DoD accomplishes. The account was created in April 2010 and is updated regularly.

- Twitter -- https://twitter.com/TheCDSE. Since its creation in September 2010, CDSE has posted 516 tweets, providing information on upcoming courses, new course releases, as well as other CDSE news that target populations may find important.

- The CDSE YouTube Channel -- http://www.youtube.com/user/dsscdse. CDSE has over 14,500 combined views of the videos and presentations on its YouTube Channel. The channel's contents include video job aids, informational videos, and recorded webinars.

The CDSE also periodically sends an electronic newsletter called the "CDSE Flash" that provides a multitude of updates, including those about training. The newsletter is extremely informative. But it can only be sent to those individuals who have taken a CDSE course where they provided their email addresses. However, by forwarding the newsletter to all the security managers, they could send it to all of their organization's original and derivative classifiers, where these individuals could get updates on new training and other matters.

However, organization security representatives could ensure, through increased outreach, that OCAs and Derivative Classifiers are provided CDSE information. Such outreach would also ensure that these individuals are kept aware that training opportunities are always available.

We should emphasize that some organizations had very comprehensive and, depending on the mission, tailored training programs. However, CDSE can provide consistency in security education and training for both DoD and industry.

Conclusion

We found that policy requires initial, refresher, specialized training, and training for OCAs and persons who apply derivative classification markings. It also requires suspending OCA and derivative classification authority if these personnel fail to meet the training requirements. Several persons we interviewed did not know of the DSS, and were not aware of the CDSE and its course offerings.

Recommendation, Management Comments, and Our Response

D. We recommend that the Under Secretary of Defense for Intelligence develop a plan to:

1. Enhance its outreach to the security community to expand awareness of the Center for Development of Security Excellence.

2. Ensure all original and derivative classifiers receive relevant and timely training that is tailored to current policy, procedures, rules, and regulations.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with our recommendations.

Our Response

The Under Secretary of Defense for Intelligence concurred with our recommendation; however, management did not provide information to identify what actions will be taken and the date on which recommendations will be completed. Therefore, we request additional comments by October 30, 2013.

Appendix A: Observations

We evaluated the effectiveness of policies for developing classification decisions; classification by derivative classifiers; effectiveness of self-inspection programs; and IC Cross-Cutting Issues. While there is need for improvement in all areas, because DoD is in the early stages of addressing these challenges, we believe the most effective method of oversight is to monitor these challenges and then identify and assess DoD's improvements in our 2016 report under P.L. 111-258. We will also provide information to the IC IG as needed as issues arise during this period. Our observations of these evaluation areas are as follows:

Observation A. Effectiveness of Policies for Developing Classification Decisions

We found that the policy for developing classification decisions is effective. We also found no instances where information was originally classified for reasons other than the defined areas for classification.

While we did find some instances of over-classification, we do not believe 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 that did not require protection in the interest of national security. However, we did find several instances where the inaccurate use of dissemination control and handling markings unnecessarily restricted information sharing.

This observation section will focus on the core issues of original classification to include the appropriateness of original classification decisions and the proper marking of classified information, which may include proper application of dissemination control markings.

Original Classification Decision Process

Original classification is the act of making an initial decision that information requires protection in the interest of national security and could be expected to cause damage if subjected to unauthorized disclosure. It is a six-step process in which the classifier must answer specific questions at each step and make considerations and decisions before classifying information. This process is designed to help OCAs make quality classification decisions, as outlined in the Defense Security Service (DSS), Center for Development of Security Excellence (CDSE).[7] The steps in the OCA desktop reference guide are described as follows:

Step 1 -– Determination of Official Government Information

The OCA must determine if the information being considered for classification is official. "Official" in this context is defined as information owned by, produced by or for, or under the control of the U.S. Government. Without the Government having some official interest in the information, classification is not an option. If the information is not official, the process stops at Step 1, as the information would be ineligible for classification. The Government would have to acquire proprietary or other official interests before information could be classified. Defining information as "official" may sometimes cause confusion. Some information may fall within the criteria of the Patent Secrecy Act of 1952 and/or may require guidance from legal counsel. If the information is deemed official, the OCA would move to Step 2 in the decision process.

Step 2 -- Determination of Eligibility for Classification

The OCA must consider if the information is eligible for classification, and if it is eligible, determine if the information is limited or prohibited from being classified.

Eligibility for Classification

If the information under consideration for classification cannot be placed in one or more of eight categories, it cannot be classified. The eight categories of information that E.O. 13526 currently identifies that can be considered for classification are:

[7] The CDSE provides DoD with a security center of excellence for professionalizing the security community and for being the premier provider of security education and training for DoD and industry under the National Industrial Security Program. The CDSE provides development, delivery, and exchange of security knowledge to ensure a high-performing workforce capable of addressing security challenges.

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to national security;
- U.S. Government programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security; and
- weapons of mass destruction.

The information is not eligible for classification if another OCA has already classified it or if classification guidance is not already available in the form of security classification guides, plans, or other memorandums. Within DoD, the majority of existing classification guidance is indexed and issued via the Defense Technical Information Center (DTIC), at www.dtic.mil.

Classification Prohibitions and Limitations

Once information has been determined eligible for classification, the OCA must determine if the information is limited or prohibited from being classified. In accordance with E.O. 13526, information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

- conceal violations of law, inefficiency, or administrative error;
- prevent embarrassment to a person, organization, or agency;
- restrain competition;
- prevent or delay the release of information that does not require protection in the interest of national security.

Limitations to classifications include:

- basic scientific research information not clearly related to national security should not be classified;

- information that has been declassified and released to the public under proper authority may be reclassified only when the information may be reasonably recoverable without bringing undue attention to the information. This means that:

    - most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from these individuals, and

    - if the information has been made available to the public via such facilities as U.S. Government archives or reading rooms, it can be or has been withdrawn from public access without significant media, public attention, or notice.

- DoD Component Heads, other than the Secretaries of the Military Departments, should submit recommendations for reclassification of information under their jurisdiction to the Secretary of Defense through the USD(I). Recommendations for reclassification must include, on a document-by-document basis:

    - a description of the information;

    - all information necessary for the original classification decision in accordance with E.O 13526, including classification level of the information and declassification instructions to be applied.

    - when and how the information was released to the public.

    - an explanation as to why the information should be reclassified. Include the applicable reason in accordance with E.O. 13526 and describe what damage could occur to national security and what damage may have already occurred as a result of the release.

    - the number of recipients and/or holders and how they will be notified of the reclassification.

    - how the information will be recovered; and

  - whether the information is in the custody of the National Archives and Records Administration and whether the Archivist of the United States must be notified of the reclassification.

Step 3 -– Determination of the Impact on National Security

Another essential decision OCAs must make before they can say the information has been classified is to determine the potential for damage to national security if unauthorized release occurs. If it is determined that no potential exists for damaging national security, the information will not be classified. If the potential exists for damage to national security and the information is determined eligible for classification as defined in Step 2, the information is then determined classified.

While it is not required to prepare a written description of the potential for damage to national security before the information can be classified, OCAs must be able to defend their decision and identify or describe the potential damage if their decision is questioned or challenged. It is recommended that the OCA justify this decision in writing at the time when it is made so that when others assume their OCA responsibilities, they will have proper information.

The OCA must also consider both the impact of classification itself, how over-classification could potentially impede the operational effectiveness of entities that need the information to complete their mission, and the possibility of protection. If classification is applied or reapplied, a reasonable possibility must exist that the information can be protected from unauthorized disclosure.

Step 4 -- Determination of Appropriate Classification Level

The OCA must evaluate the impact of classification in order to identify the appropriate classification level. The OCA must determine how sensitive the information is, what the potential damage to national security would be if the information was not protected, and assign a classification level based on that determination. The OCA must use reasoned judgment to consider the extent of potential damage.

The classification levels are defined in relation to their potential damage to national security:

- If unauthorized disclosure of the information could reasonably be expected to cause exceptionally grave damage to national security, it should be classified as TOP SECRET.

- If unauthorized disclosure of the information could reasonably be expected to cause serious damage to national security, it should be classified as SECRET.

- If unauthorized disclosure of the information could reasonably be expected to cause damage to national security, it should be classified as CONFIDENTIAL.

Step 5 -- Determination of Classification Duration

After determining the level of classification, the OCA must determine the duration of classification. This involves reviewing the level of classification to determine downgrading requirements and declassification when it is determined that the information no longer requires classification.

Downgrading:

The OCA must evaluate the information to determine if a future specific date or event could occur that results in diminishing the damage to national security to the point that allows for lowering the classification level. If a change occurs in the information's sensitivity, the OCA will need to assign a date or event for downgrading that information. If the OCA determines that the sensitivity will not decrease or cannot make a determination on decreased sensitivity, the OCA will proceed to determine the declassification instructions.

Declassification:

The OCA must make declassification determinations for all classification decisions. When considering the duration of classification, the OCA must follow these guidelines:

- if the OCA knows of a date within 10 years where the potential for damage from compromise is no longer a national security concern, then that date is assigned as the declassification date;

- if the OCA cannot determine a date, but can identify an event that is expected to occur within the next 10 years where the potential for damage from compromise is no longer a national security concern, then that event is assigned as the declassification instruction;

- if the OCA determines that information requires protection beyond 10 years of the original classification, the OCA may assign a date or event up to, but not exceeding, 25 years from the date of the original decision;

- human intelligence exemption -– An OCA shall apply the “50X1-HUM” exemption with no date of declassification when classifying information that could be expected to reveal the identity of a confidential human source or human intelligence source. Only OCAs having jurisdiction over such information may use this designation;

- weapons of mass destruction exemption –- An OCA shall apply the “50X2-WMD” exemption with no date of declassification when classifying information that could be expected to reveal the development, production, or use of weapons of mass destruction. Only OCAs having jurisdiction over such information may use this designation;

- the 25X markings are applied when information is exempt from 25-year automatic declassification, and cannot be used unless the specific information has been approved through the Interagency Security Classification Appeals Panel, generally in the form of a declassification guide. Such information must be incorporated into classification guides. The classification guide would include the specific element of information and the level of classification. (Examples of how this works would be “25X4, 20401010” or “25X9, 20300125.”) When the 25X marking is applied, the “Declassify on” line would include the symbol “25X” and a brief reference to that category and the new date or event for declassification. For a complete list of the exemptions, refer to E.O. 13526; and

- information classified in accordance with the Atomic Energy Act of 1954, as amended (Restricted Data and Formerly Restricted Data), is exempt from declassification requirements. For Restricted Data, classification decisions are codified in the Department of Energy Classification Guide. For Formerly Restricted Data, classification decisions are documented in the Joint Department of Energy/DoD Classification Guide.

Step 6 -- Providing and Communicating Guidance for Derivative Classification

The OCA’s final step in the original classification decision process is designating the information as classified and to communicate the decision. Three methods exist for communicating the decision.

- SCGs/declassification guides;
- Properly-marked source documents; and
- outline classification instructions on a DD Form 254, "DoD Contract Security Classification Specification."

The preferred method for communicating classification decisions is to communicate it through an SCG. The least common method for communicating the decision is to outline classification instructions on a DD Form 254, which identifies all contractor-specific security requirements and guidance. Its rare use may occur when a contract is required and needs classification instructions, but a classification guide is unavailable.

Once the decision is communicated, the decisions will be used by others who must work with the information to make proper derivative classification decisions and ensure the information is properly protected from unauthorized disclosure. OCAs have the vital task of effectively communicating their decisions.

Security Classification Guide Analysis

Because the SCG is the preferred method for communicating classification decisions, we conducted a review of 254 SCGs that were available online at the DTIC website to determine the accuracy of information and identify areas for improvement. SCG content was consistent with established guidance. The SCGs contained valid reasons for classification and consistently provided declassification guidance.

We found no instances where information was classified for reasons other than the defined areas for classification. Based on our review, OCAs are effectively making classification determinations on information that derivative classifiers will use. Finding D does identify some areas of concern regarding SCG administration and management. However, these concerns do not reflect issues with classification determinations or the procedures used to make classification decisions.

Conclusion

We found that the policy for developing classification decisions is effective. For a vast majority of documents, we found no instances where information was classified for reasons other than the defined areas for classification.

Observation B. Classification by Derivative Classifiers

Current standards and guidance exist for derivative classifiers; however, guidance is conflicting in some cases and not updated in others. Absent consistent policies and coordinated training, persistent misclassification of classified documents will continue. However, as stated in Finding A, we mapped DoD issuances to E.O. 13526 and 32 C.F.R., Part 2001, and as a result policies were adopted at the Office of the Secretary of Defense-level, but had not yet been adopted/promulgated at the agency level.

This section will focus on the core issues relating to derivative classification and the individuals who make derivative classification decisions. All personnel with an active security clearance can perform derivative classification. All personnel who apply derivative classification markings must receive training on the proper application principles of E.O. 13526 prior to derivatively classifying information and at least once every two years thereafter. Information may be derivatively classified from a source document or documents, or through using a classification guide.

Derivative classifiers identified issues with conflicting and confusing marking standards. The issues identified in the document review section reflect inconsistent standards and guidance with respect to the marking of derivatively classified documents. This is particularly evident with emails. The documents exemplify the application of varying standards in the marking of derivatively classified documents. The documents also provide evidence of the disparate methods that derivative classifiers employ to resolve classification discrepancies, which can adversely affect the sharing of classified information with key stakeholders and individuals with an identified need to know.

Input from Derivative Classifiers

We reviewed comments from derivative classifiers to assess their knowledge of the classification process and the appropriateness of derivative classification actions. To that end, we asked if derivative classifiers had encountered issues with the classification of similar information at differing levels, inaccurate portion markings, conflicting guidance and the constraints that control markings might place on information sharing. We found that a majority of respondents have encountered similar information classified at different levels.

Respondents also noted the conflicting guidance regarding dissemination control markings. (See Appendix A, Observation D for further details on dissemination control markings.) A majority also received no training on the process for challenging information they believed to be inappropriately classified.

Our review of a sample of classified documents indicates that these inconsistencies have resulted in improperly and inaccurately marked documents, with several instances of misclassification and a few instances of over-classification. Absent consistent policies and coordinated training, persistent misclassification of classified documents will continue. These incongruities burden derivative classifiers, who, as a result, resolve discrepancies inconsistently. Inappropriately classified information can also impede the sharing of information with stakeholders and individuals with a legitimate need-to-know.

When asked if they had ever encountered similar information classified at different levels, more than 60 percent of derivative classifiers queried responded affirmatively. Of that number, 18 percent indicated that when they tried to resolve classification inconsistencies, the guidance was neither clear nor consistent. The majority of respondents who encountered differing levels of classification for the same information chose to use the higher classification level to mark their derivative documents, using a better-safe-than-sorry approach to classification.

Sixty eight percent of respondents identified concerns with the consistent application of portion markings in classified documents, while 27 percent expressed specific concerns with the system of dissemination controls. Specific comments included the need for more training using portion markings and classification authority blocks to correspond with new guidance. One respondent noted the presence of conflicting and non-authoritative policies citing organizational, ISOO, and Controlled Access Program Coordination Office (CAPCO) guidance that is not always in harmony.

Review of Classified Documents

We conducted an independent review of classified documents to determine the prevalence of improperly and inaccurately marked documents. We reviewed 220 classified documents for consistency in portion markings, dissemination controls, classification authorities, and declassification guidance. In total, we found that 70 percent of the 220 documents reviewed had classification discrepancies. Moreover, 23 documents, or approximately 10 percent, were misclassified or over-classified.

A majority of the documents (52 percent) had issues with the classification block to include incorporating new guidance regarding the “classified by” line. Without the “classified by” information, in the event of a challenge, a successful potential challenge is problematic. Other documents still cited E.O. 12958 for classification authorities and declassification exemptions.

One-hundred percent of emails we reviewed contained errors in marking or classification. To improve, DoD is working on efforts to enhance proper classification in the electronic environment to ensure meeting the requirements of Section 1.6 and 2.1 of E.O. 13526. Of particular concern is the amount of misclassification historically seen in routine information and emails on classified information systems. This misclassification is often abetted by default email marking tool settings that allow the user to accept the default without further consideration of whether other markings are required by the email's content. To address this situation, DoD is working to issue technical guidance to system administrators requiring:

- email marking tools be deployed to all classified information systems;
- the tools be configured with no default setting; and
- the requirement for a classification marking be enforced by the tool/technical solution.

Specific examples of over-classification included a document that referenced information from an open-source publicly-available report on corruption. The derivative classifier classified the analysis of the information citing no classification authority. Another instance involved a template automatically marked SECRET even though the entire content was shown to have "nothing significant to report."

Conclusion

Derivative classifiers identified issues with conflicting and confusing marking standards. Moreover, they noted that supporting guidance is not always updated to reflect current classification standards. Derivative classifiers also expressed frustration regarding ever-changing standards and the sometimes unclear and inconsistent processes applied to resolve classification concerns. However, as stated in Finding A, we mapped DoD issuances to E.O. 13526 and 32 C.F.R., Part 2001, and as a result policies were adopted at the Office of the Secretary of Defense-level, but had not yet been adopted/promulgated at the agency level.

The issues identified in the document review section reflect inconsistent standards and guidance regarding the marking of derivatively classified documents. This is particularly evident with emails, where those we reviewed displayed some form of marking or classification error. The documents exemplify the application of varying standards in the marking of derivatively classified documents, and provide evidence of the disparate methods employed by derivative classifiers to resolve classification discrepancies. These inconsistencies can adversely affect the sharing of classified information with key stakeholders and individuals with an identified need-to-know.

We will continuously monitor DoD's progress to strengthen these efforts, especially as it relates to agency efforts to update policy to fully align with Office of the Secretary of Defense-level policy, as well as classification management in the electronic environment, and report the progress in our 2016 report under P.L. 111-258.

Observation C. Effectiveness of Self-Inspection Programs

We found that for the self-inspection programs the description, assessment and summary, specific discrepancy reports, and successful practices provided a comprehensive picture of DoD's overall security program management efforts.

This section will focus on the effectiveness of the agency self-inspection program. Section 5.4(d)(4) of E.O. 13526, and 32 C.F.R. Part 2001.60 requires SAOs to establish self-inspection programs and issues reports annually on these programs to the ISOO Director. The reports provide information about the structure and implementation of the agency's self-inspection program and details this program's findings, which the SAO established to help oversee the agency's classified national security information program.

Throughout our evaluation, our findings were similar to those reporting in the DoD Self-Inspection Program below.

Self-Inspection Reporting

E.O. 13526, Section 5.4(d), requires agencies to establish and maintain ongoing self-inspection programs, and report each year to the ISOO Director on those programs. Self-inspections evaluate the effectiveness of agency programs covering original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight. In addition, self-inspections include regular reviews of representative samples of agencies' original and derivative classification actions; these samples must encompass all agency activities that generate classified information, and appropriate agency officials must be authorized to correct misclassification actions.

The USD(I) developed its comprehensive DoD report based on the security posture information received from the SAOs of the following DoD entities:

- the Department of the Army;
- the Department of the Navy;
- the Department of the Air Force;
- the Joint Staff;
- the Missile Defense Agency;
- the Defense Advanced Research Projects Agency;
- the Defense Threat Reduction Agency; and
- the designated federal entities -- the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and the National Reconnaissance Office.

Self-Inspection Program Policy

- DoD Manual 5200.01, Enclosure 2, Volume 1, paragraph 7d, requires SAOs to establish and maintain an ongoing self-inspection and oversight program to evaluate and assess the effectiveness and efficiency of the DoD Component's implementation of that portion of the information security program pertaining to classified information.

- DoD Manual 5200.01, Enclosure 2, Volume 1, paragraph 7d(3), requires self-inspections to be conducted at least annually, with the frequency established based on program needs and classification activity. DoD Component activities that originate significant amounts of classified information should be inspected at least annually. Annual reports on the Component's self-inspection program should be submitted, as required, by ISOO and/or USD(I).

DoD Self-Inspection Results

Description of the DoD Self-Inspection Program

In accordance with E.O. 13526 and 32 C.F.R. Part 2001, and ISOO memorandum of June 29, 2012, agencies were required to establish and maintain an ongoing self-inspection program, which includes the regular reviews of representative samples of the agency's original and derivative classification actions.

DoD is a large department, comprised of more than 40 major Components. The USD(I) is designated as the SAO for the DoD Self-Inspection Program. DoD Manual 5200.01, Volumes 1-3, carry out E.O. 13526 and 32 C.F.R., Part 2001. DoD Components are required to carry out an information security program to protect classified national security information.

To this end, a standard checklist was developed and forwarded to the Components to use when developing their annual self-inspection reports. Some Components used already-established methods to conduct their self-inspections and some used the USD(I)-provided template. USD(I) received approximately 40 separate self-inspection reports. DoD Components used a variety of work methods to conduct self-inspections.

These methods included interviews of employees and contractors by security professionals, security managers, and designated teams; reviews of representative samples of their classified information (document and electronic storage media) based on unit or organizational mission; and inspections of facilities handling classified materials. Inspection schedules vary, but were conducted annually, quarterly, and randomly, as necessary.

The DoD self-inspections evaluated general adherence to the principles and requirements of E.O. 13526 and 32 C.F.R., Part 2001, and the overall effectiveness and implementation of requirements from DoD Manual 5200.01 Volumes 1-3, covering:

- Original Classification
- Derivative Classification
- Declassification

- Safeguarding
- Security Violations
- Security Education and Training
- Management and Oversight

The DoD Self-Inspection Program included and assessed all DoD Components that create, generate, produce, or handle classified information. Components were tasked with analyzing their findings and taking measures to correct any deficiencies discovered during the self-inspection process.

Components submitted their reports to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) Security Policy and Oversight Directorate, where submissions were consolidated and then forwarded to ISOO.

Assessment and Summary

Original Classification: All DoD OCAs are designated as such in writing and have received formal, documented training. If DoD OCAs are found to be non-compliant for any reason, their authority is suspended until they are in compliance. Components with OCAs reported that 100 percent of these individuals have received required training and understand their responsibilities. DoD Components reported no specific issue items or material weaknesses during the self-inspection.

Derivative Classification: Within DoD, all cleared personnel who generate or create information that is derivatively classified should ensure that the derivative classification is made in accordance with DoD Manual 5200.01. No specific, individual delegation of authority is required. During this inspection period, most Components reported that 90 to 100 percent of their derivative classifiers received training and know about their responsibilities as derivative classifiers (See Finding D with regard to security education and training). DoD Components reported no specific issue items or material weaknesses during the self-inspection.

Declassification: DoD policy provides specific guidelines pertaining to declassification and who is authorized in the Department to declassify information. Declassification does not authorize releasing the information to the public. DoD Components reported no specific issue items or material weaknesses during self-inspection. However, this issue remains of high interest with both the OUSD(I) and the DoD Inspector General as the requirements of the "Reducing Over-Classification Act" are carried out.

Safeguarding: Each Component in DoD has policies and procedures in its possession governing the proper safeguarding of classified national security information. DoD policy states that Components should have a system of control measures that ensure that access to classified information is limited to authorized persons. DoD is effectively applying agency-wide safeguarding measures for classified information in accordance with Department policies. DoD Components reported no specific issue items or material weaknesses during the self-inspection.

Security Violations: On October 18, 2012, the Secretary of Defense mandated that all DoD Components use the central DoD-wide security reporting system that USD(I) established, in addition to existing reporting requirements. This serves to strengthen accountability in the DoD reporting system. DoD has also established an Unauthorized Disclosure Team whose mission is to prevent and deter DoD personnel from unauthorized disclosure of classified information. In addition, DoD, in collaboration with the DNI, developed a strategic plan to address unauthorized disclosures. This plan will integrate and strengthen DoD's processes to report, assess damage, and monitor implementation of administrative, management, and investigative actions. DoD Components reported no specific issue items or material weaknesses during the self-inspection.

Security Education and Training: DoD policy states that all personnel, including DoD civilians, military members, and on-site support contractors, receive an initial orientation about the DoD Information Security Program. This orientation is designed to define classified information, produce a basic understanding of security policies and principles, notify personnel of their responsibilities within the security program, and inform personnel of the administrative, civil, and/or criminal sanctions that can be applied, when appropriate. All DoD personnel with continuing access to classified information must also receive annual refresher training that reinforces the policies, principles, and procedures covered in their annual and specialized training.

Security education and training is accomplished either by established programs within the Component or by using external resources, such as the CDSE of the DSS. Some DoD Components choose combining internal and external resources. DoD training includes initial training, annual refresher, OCA, derivative, and specialty training. DoD Components reported no specific issue items or material weaknesses during the self-inspection.

Management and Oversight: The SAO that the head of the DoD Component appoints has day-to-day responsibility for the direction, carrying out, and oversight of the Component's information security program and for its efficient and effective implementation. One of the Component SAO's responsibilities is to establish and maintain an ongoing self-inspection and program oversight function. All DoD Components are in compliance with DoD policy relating to management and oversight.

DoD Components reported no specific issue items or material weaknesses during the self-inspection. USD(I) is responsible for strategic oversight of DoD security program implementation.

The DSOAP operates in support of this oversight effort. The DSOAP was not designed to conflict with, or circumvent Components' existing oversight mechanisms, but is a collaborative endeavor intended to assess the effectiveness of security policies in operational environments. Oversight visits have allowed for trend analysis and program improvements.

Specific Discrepancy Reports

During the self-inspection process, DoD Components reported various discrepancies with corrective action taken or planned. The following are the most common discrepancies discovered:

- missing overall classification on the top, bottom, front, and the back of the classified document;
- missing portion markings;
- electronic media not properly marked;

- end-of-day checks not conducted;
- multiple sources, but these sources are not listed;
- improper creation and marking of classified products; and
- point/talking papers containing classified information improperly marked.

Successful Practices

DoD Components identified best practices, as required in DoD policy, as follows:

- using SharePoint to make available all information Security Managers need to manage their program and share unit best practices;
- creating and using an Electronic Security Manager Handbook;
- providing and maintaining open communications between different levels of management structure within the organization;
- establishing online training tools to improve ability to track completion of training requirements;
- issuing the recently-developed quarterly Security Newsletter that provides informational security articles, security updates, and upcoming security courses;
- maintaining an automated security incident reporting program;
- maintaining complete inventories of all classified documents and electronic media to provide precise tracking of classified holdings;
- developing organization derivative classification training;
- reviewing the process for public release of information;
- maintaining a central Security Education and Awareness mailbox with all questions answered by close of business;

- tracking of mandatory annual security and derivative classifier training by the Human Resources Information System of Record, which enhances better oversight of training completion rates; and

- developing a comprehensive security database, which reflects final adjudication and investigation of security incidents.

Conclusion

We found that the description, assessment and summary, specific discrepancy reports, and successful practices offered a comprehensive picture of DoD's security program management efforts. Additionally, based on our review of each entity's self-inspection report, interviews, and questionnaire analysis, the DoD self-assessment report's information does provide an excellent opportunity to understand weaknesses, opportunities, and successful practices for program improvement.

Observation D. Intelligence Community Cross-Cutting Issues

We found instances where dissemination control markings were incorrectly applied, which could unnecessarily restrict the sharing of information. However, we also found that DoD policy states that dissemination of information regarding intelligence sources, methods, or activities should be consistent with directives that the DNI issued. DNI Directives are electronically available to DoD personnel, as is the CAPCO Register and Marking Implementation Manual,[8] on the Joint Worldwide Intelligence Communications System (JWICS) and SECRET Internet Protocol Router Network (SIPRNET).

For IC components within the DoD, this section will focus on the organization's ability to adequately carry out appropriate ODNI-issued IC guidance related to classification management, and classification and control markings. It will also determine if ODNI-issued IC policies, procedures, rules, regulations, or management practices may have, or are contributing to, persistent misclassification; or have resulted in the lack of access for DoD programs to ODNI-produced classified documents or information. The section is also intended to inform and facilitate an understanding about whether –- and the extent to which –- national intelligence information is being provided to appropriate parties without delay or unnecessary restrictions.

[8] The [Controlled Access Program Coordination Office] CAPCO Register and Manual includes all markings authorized for use with classified or unclassified intelligence information, as applicable, to communicate one or more of the following: classification type and level, controlled access programs, foreign government information, dissemination controls, disclosure and release determinations, and other warnings.

DoD Policy Related to Intelligence Community Guidance

Defense Intelligence Components and personnel working with intelligence and intelligence-related information under DNI's purview refer to ICD 710, the "Authorized Classification and Control Markings Register" -- the "CAPCO Register" -- and the IC Classification and Control Markings Implementation Manual for guidance on marking and dissemination of classified and unclassified intelligence information. The CAPCO Register and associated Marking Implementation Manual are available electronically on the JWICS and SIPRNET. IC-wide guidance and criteria (i.e., ICDs, Intelligence Community Policy Guidance, and CAPCO Register and Manual, etc) are referenced in DoD policy.

Certain dissemination control markings are authorized for use only on intelligence information. Among these are "NOFORN,"[9] "RELIDO,"[10] and "IMCON."[11] DoD Intelligence Components refer to policy and implementing guidance that the DNI issued on marking intelligence and intelligence-related information and products under the DNI's purview. Information on intelligence control markings is in DoD Manual 5200.01, Volume 2, Appendix 2, February 24, 2012, to help those involved in other DoD activities to understand the meaning and use of such markings.

Based on our analysis, interviews, and response to questionnaires, the NOFORN dissemination control marking was seemingly the most misunderstood dissemination control marking, with the possibility of having a detrimental impact on sharing with coalition partners. NOFORN is applied to classified intelligence that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission from the information's originator; however, in some instances, legitimately releasing the information to foreign partners is not carefully considered.

[9] NOFORN (Not Releasable to Foreign Nationals) is applied to classified intelligence that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the information's originator.

[10] RELIDO (Releasable by Information Disclosure Official) is a dissemination control marking that may be applied to national intelligence information to indicate that the originator has authorized Designated Intelligence Disclosure Officials, or their designee, to make further release determinations in accordance with existing foreign disclosure policy and procedures.

[11] IMCON (Controlled Imagery) is used to protect sources and analytic methods associated with the geospatial intelligence discipline that are particularly vulnerable to countermeasures, and if disclosed or released, could negate or measurably reduce the effectiveness of those methodologies.

NOFORN's overuse was also mentioned, with one respondent saying that personnel sometimes placed NOFORN with no supporting requirement aimed at ensuring their products are not released to foreigners. Additional comments on NOFORN's use cited the constraints it presented when organizations needed to share information with non-U.S. allies. In one instance, a "Foreign Disclosure Officer" was asked to release the required information. Once approval was secured, the information was shared only to discover that the partners already had the information and had undergone a similar process with their "Foreign Disclosure Officer" to pass the information to the United States.

One respondent acknowledged that the reflexive marking of a SECRET document with NOFORN was a problem, citing a concern that some people believe that without NOFORN, information was automatically shared with partner nations. The respondent said that personnel did not realize that SECRET information is automatically not released and that mechanisms (e.g., tetragraphs) exist to regulate the release of information without needing to apply the additional control of a NOFORN caveat. The "conflicting guidance from the Intel community" was also cited as a concern, resulting in adding confusing marking requirements.

Reflecting the above comments, 26 percent of derivative classifiers that were questioned identified the unnecessary use of dissemination control markings. A small number (five percent) said that dissemination control markings prevented the release of information to stakeholders or persons with a verified need-to-know.

Conclusion

We found instances where dissemination control markings were incorrectly applied, which could cause unnecessary restriction of information sharing. However, we also found that DoD policy addressing dissemination of information regarding intelligence sources, methods, or activities, was consistent with DNI-issued directives. DNI directives are electronically available, as is the CAPCO Register and Marking Implementation Manual, on JWICS and SIPRNET. Because dissemination control markings of intelligence information are the DNI's purview, we will monitor and comment further for the 2016 report under P.L. 111-258.

Appendix B

Computer-Processed Data

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

Use of Technical Assistance

During the evaluation, we requested and received technical assistance from the DoD Office of Inspector General Quantitative Methods Division (QMD). We worked with QMD during our planning phase.

Prior Coverage

In the last seven years, the GAO issued one report on DoD's Information Security program. Unrestricted GAO reports are at http://www.gao.gov. The DoD OIG has issued three reports discussing security within the DoD. DoD OIG reports are at http://www.dodig.mil/Ir/reports.

You can obtain information about the Department of Defense Office of Inspector General from DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012; and DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013. Our website is www.dodig.mil.

GAO

GAO Report No. GAO-06-706, "DoD Can More Effectively Reduce the Risk of Classification Errors," June 30, 2006.

DoD OIG

DoD OIG Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense: Tracking and Measuring Security Costs," August 6, 2010.

DoD OIG Report No. DoDIG-2012-001, "Assessment of Security Within the Department of Defense: Training, Certification, and Professionalization," October 6, 2011.

DoD OIG Report No. DoDIG-2012-114, "Assessment of Security Within the Department of Defense: Security Policy," July 27, 2012.

Center for Development of Security Excellence (CDSE) Course Offerings

DoD's CDSE offers several different activities designed to train and educate those charged with original and derivative classification duties. CDSE's eLearning "Original Classification Course" is 90 minutes long and provides the policy guidance for, and purpose of, original classification. The course defines original classification, identifies OCA requirements and qualifications, reviews the six steps of the original classification decision process, discusses original classification limitations and prohibitions, explains the basis for determining classification levels and duration, and lists the authorized means for providing classification guidance. The target audience for this course is DoD military, civilian, and contractor personnel who propose, prepare, develop, or help with original classification decisions. Information on this course is at: http://cdse.edu/catalog/elearning/IF102.html.

In addition to the eLearning course, CDSE also has a downloadable "Original Classification Authority Desktop Reference Guide," to assist the same target audience with each of the six steps involved in the original classification process. That document is on the CDSE job aids web page at: http://cdse.edu/documents/cdse/oca-desktop-reference.pdf.

CDSE also offers a Security Short titled "Requirements for OCAs," which provides an overview of the changes for OCAs resulting from the issuing of E.O. 13526. It includes a brief review of the six steps of the original classification process and highlights the mandatory annual training requirement, as well as sanctions that can be imposed for failure to timely complete that training. The short can be viewed at: http://cdse.edu/shorts/information-security.html#.

Original Classification is also discussed in two of CDSE's instructor-led courses; the "DoD Security Specialist Course," and the "Information Security Management Course."

For derivative classifiers, CDSE offers a two-hour eLearning course titled "Derivative Classification" that explains how to derivatively classify national security information from a classification management perspective. The course discusses the responsibilities associated with derivatively classifying information, describes the process and methods for derivatively classifying information, identifies authorized sources to use when derivatively classifying information, and explains how to apply authorized sources through derivatively classifying information based on the concepts of "contained in," "revealed by," and "compilation." The target audience for this course is DoD military, civilian, and contractor personnel responsible for derivatively classifying national security information. Information on this course is at: http://cdse.edu/catalog/elearning/IF103.html. In addition to accessing the course through our Learning Management System (Security Training, Education, and Professionalization Portal –- STEPP), this course is available for access on an outside website that does not require registration. The link is: http://cdsetrain.dtic.mil/derivative/.

CDSE is also developing a "Derivative Classification Refresher Course" that is expected to be launched near the first part of FY 2014. The course will serve as a tool for derivative classifiers to obtain the required biennial training to maintain their derivative classification duties.

In addition to the eLearning course, CDSE also has a downloadable "Derivative Classification Training Guide" to assist the same target audience with understanding the derivative classification process. The guide is on the CDSE job aids web page at: http://cdse.edu/documents/cdse/DerivativeClassification.pdf.

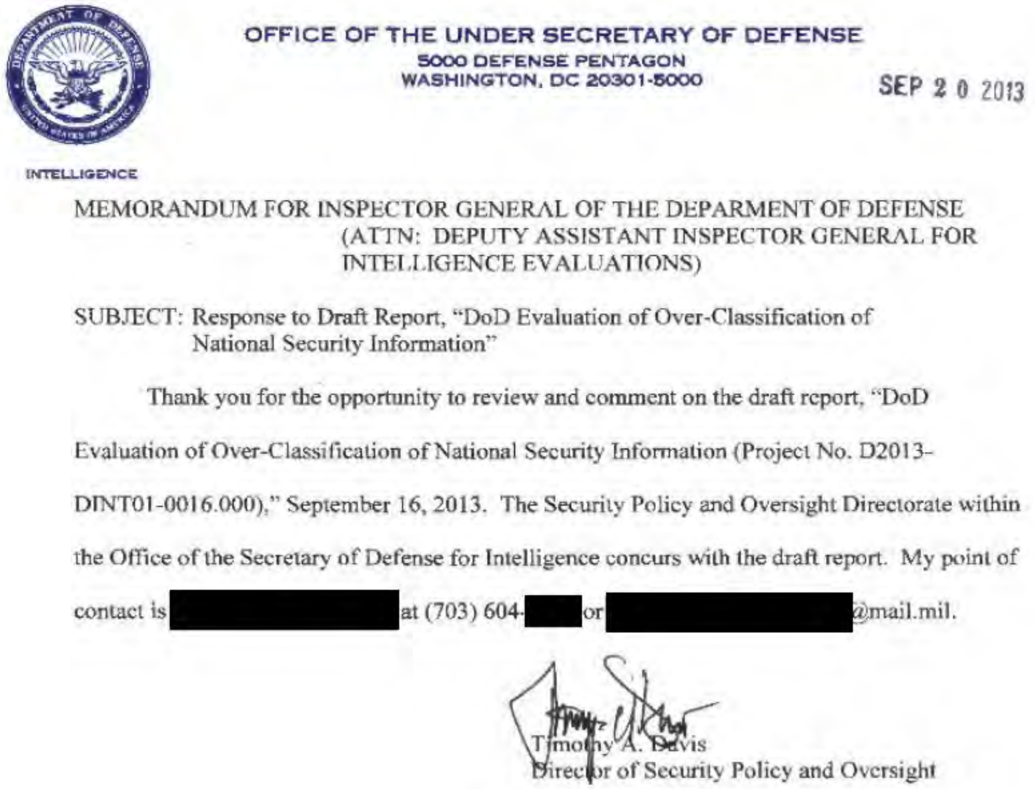
In the area of classification conflicts, CDSE offers a 30-minute eLearning course titled "Classification Conflicts and Evaluations" that gives a broad overview of the classification challenge process. Students examine the process for formal challenges to classification decisions, the role of the Interagency Security Classification Appeals Panel, and the process for mandatory review. Information on that course can be seen at: http://cdse.edu/catalog/elearning/IF110.html.

The Course and Product Book has been updated and provides the latest CDSE course offerings. The Course and Product Book is at: http://www.cdse.edu/documents/cdse/courses-products-Aug2013.pdf

The link to the student guides for CDSE courses, which includes the updates for E.O. 13526 and DoD Manual 5200.01, Volumes 1 through 4, can be accessed once you log into a STEPP account at:
https://stepp.dss.mil/Sumtotal82/app/taxonomy/learnerSearch/LearnerSearch.aspx?RootNodeID=-1&NodeID=5452&UserMode=0

Management Comments

Under Secretary of Defense for Intelligence Comments



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

SEP 2 0 2013

INTELLIGENCE

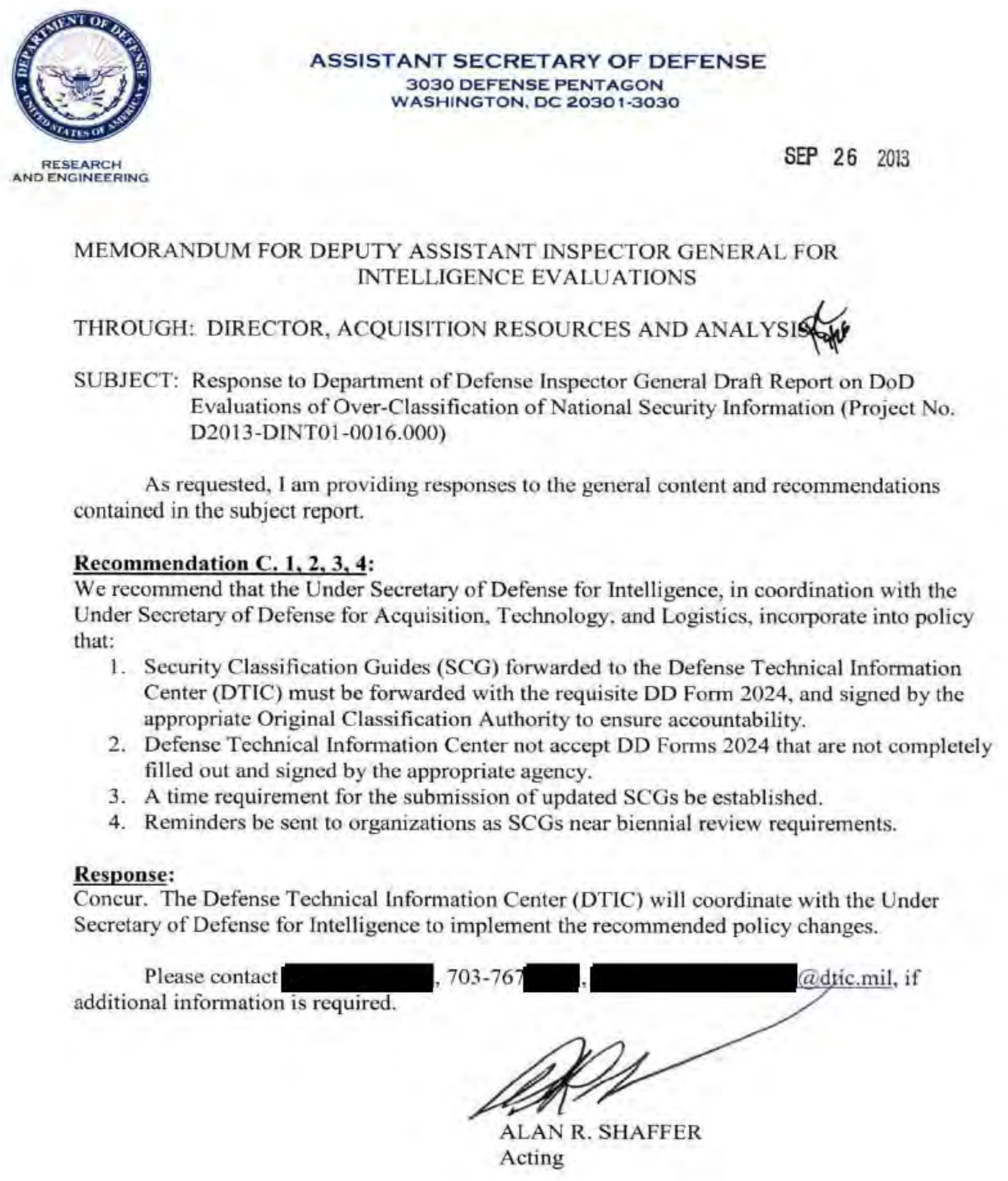
MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARMENT OF DEFENSE
(ATTN: DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INTELLIGENCE EVALUATIONS)

SUBJECT: Response to Draft Report, "DoD Evaluation of Over-Classification of National Security Information"

Thank you for the opportunity to review and comment on the draft report, "DoD Evaluation of Over-Classification of National Security Information (Project No. D2013-DINT01-0016.000)," September 16, 2013. The Security Policy and Oversight Directorate within the Office of the Secretary of Defense for Intelligence concurs with the draft report. My point of contact is [redacted] at (703) 604-[redacted] or [redacted]@mail.mil.

Timothy A. Davis
Director of Security Policy and Oversight

Under Secretary of Defense for Acquisition, Technology and Logistics Comments



ASSISTANT SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

SEP 26 2013

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR INTELLIGENCE EVALUATIONS

THROUGH: DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS

SUBJECT: Response to Department of Defense Inspector General Draft Report on DoD Evaluations of Over-Classification of National Security Information (Project No. D2013-DINT01-0016.000)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendation C. 1, 2, 3, 4:
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:

1. Security Classification Guides (SCG) forwarded to the Defense Technical Information Center (DTIC) must be forwarded with the requisite DD Form 2024, and signed by the appropriate Original Classification Authority to ensure accountability.
2. Defense Technical Information Center 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.

Response:
Concur. The Defense Technical Information Center (DTIC) will coordinate with the Under Secretary of Defense for Intelligence to implement the recommended policy changes.

Please contact [redacted], 703-767[redacted], [redacted]@dtic.mil, if additional information is required.

ALAN R. SHAFFER
Acting

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD IG Director for Whistleblowing & Transparency. For more information on your rights and remedies against retaliation, go to the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

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

Congressional Liaison
703.604.8324

DoD Hotline
800.424.9098

Media Contact
Public.Affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report-request@listserve.com

Twitter
twitter.com/DoD_IG

Department of Defense | INSPECTOR GENERAL

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