Description of document:	National Security Agency (NSA) Inspector General (OIG) report on reducing over-classification 2013
Requested date:	08-October-2013
Release date:	15-September-2025
Posted date:	20-Oct-2025
Source of document:	National Security Agency Attn: FOIA/PA Office Inspector General 9800 Savage Road, Suite 6932 Fort George G. Meade, MD 20755-6932 Fax: 443-479-3612 Online FOIA Submission Form FOIA.gov

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 75336A
15 September 2025

This responds to your Freedom of Information Act (FOIA) request dated 8 October 2013 asking for "a copy of the NSA Inspector General report (due September 30, 2013) on reducing over-classification required in Section 6 of the Reducing Over-Classification Act (H.R. 553)." A copy of your request is enclosed. Your request has been processed under the FOIA and the document you requested is enclosed. Certain information, however, has been protected in the enclosure.

This Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605).

In addition, personal information regarding individuals has been withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

Please be advised that the Agency reasonably foresees that disclosure of the withheld information would be harmful to an interest that is protected by the identified exemption.

Since these withholdings may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

If you decide to appeal this decision, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

NSA FOIA/PA Appeal Authority (P132)
National Security Agency
9800 Savage Road STE 6932
Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612.
The appropriate e-mail address to submit an appeal is FOIA_PA_Appeals@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd. - OGIS
College Park, MD 20740
ogis@nara.gov
877-684-6448
(Fax) 202-741-5769

Sincerely,

SALLY A. NICHOLSON
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

(U) Report on the Audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act"

AU-13-0005

7 August 2013

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

7 August 2013
IG-11569-13

TO: DISTRIBUTION

SUBJECT: (U) Report on the Audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act" (AU-13-0005) — ACTION MEMORANDUM

1. (U) This report summarizes our audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act."

2. (U//~~FOUO~~) In accordance with NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General*, and IG-11358-12, *Follow-up Procedures for OIG Report Recommendation*, actions on OIG audit recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and forward a revised target completion date to [redacted] Follow-up Program Manager, at DL D1_Followup (ALIAS) D1.

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors throughout the review. For additional information, please contact [redacted] or via e-mail at [redacted] or [redacted] or via e-mail at [redacted]

George Ellard

(b)(3)-P.L. 86-36

DR. GEORGE ELLARD
Inspector General

AU-13-0005

(U//~~FOUO~~) DISTRIBUTION:
ADET
ADHR
ADPR
CFM
CoS
D4
OGC
SAE
SID
TD

cc: BF09 [redacted]
BMI [redacted]
DL BMI_Registry
DC06 [redacted]
DJ2 [redacted]
DL d_gc_tasker
DL D_DJ_Tasker (ALIAS) D
DL ADET_REGISTRY
DL ADHR_REG
DL SIDIGLIAISON
DL TD_REGISTRY
IG
D1 [redacted]
D11
D12
D13
D14

(b)(3)-P.L. 86-36

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) EXECUTIVE SUMMARY

(U) Overview

(U~~//FOUO~~) This is the first of two reports required by Public Law 111-258, the "Reducing Over-Classification Act," which mandates that the Inspector General of each agency with an officer or employee authorized to make original classifications:

- (U~~//FOUO~~) Assess whether classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered and
- (U~~//FOUO~~) Identify policies, procedures, rules, regulations, and management practices that might contribute to persistent misclassification.

(U) Highlights

- (U) **Information Security Program Management**
  (U~~//FOUO~~) The National Security Agency/Central Security Service's (NSA/CSS) Information Security Program is not compliant with E.O. 13526, *Classified National Security Information*, 5 January 2010, because of outdated program guidance, a flawed classification tool, lack of classification elements in personnel performance appraisals, and a deficient classification challenge process.
- (U) **Original Classification**
  (U~~//FOUO~~) Agency original classification guidance is sometimes conflicting and incomplete; this might cause inaccurate derivative classifications.
- (U) **Derivative Classification**
  (U~~//FOUO~~) Agency derivative classifications are sometimes incorrect because of unclear requirements, unsubstantiated classification decisions, and confusing lines of authority.
- (U) **Information Security Self-Inspection Program**
  (U~~//FOUO~~) The NSA/CSS Self-Inspection Program is incomplete because of missing report elements and a flawed program; this might impede the Associate Directorate for Policy and Records management from identifying and correcting problems in the program
- (U) **Information Security Training and Education**
  (U~~//FOUO~~) NSA/CSS mandatory classification training does not teach derivative classifiers how to classify information accurately. NSA/CSS employees are not compelled to complete mandatory training or classifications. As a result, some Agency derivative classifiers are making improper classifications.

(U) This page intentionally left blank.

I. (U) INTRODUCTION

(U) Requirements

(U) Objectives

(U~~//FOUO~~) This is the first of two reports required by the "Reducing Over-Classification Act," 6 U.S.C. §101 note, which mandates that the Inspector General of each agency with an officer or employee authorized to make original classifications, in consultation with the Information Security Oversight Office (ISOO)[1]:

- (U~~//FOUO~~) Assess whether classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered and
- (U~~//FOUO~~) Identify policies, procedures, rules, regulations, and management practices that might contribute to persistent misclassification.

(U) Methodology

(U~~//FOUO~~) The Department of Defense (DoD) Office of the Inspector General (OIG) coordinated this review to ensure comparable reports across DoD components. The DoD OIG issued *A Standard User's Guide for Inspector General Conducting Evaluations Under Public Law 111-258, the "Reducing Over-Classification Act,"* and a standard report template. Our report addresses the nine areas associated with classification and control marking:

1. (U) Effectiveness of Security Program Management
2. (U) Effectiveness of Original Classification Authorities
3. (U) Effectiveness of Original Classification and Dissemination Control Markings
4. (U) Effectiveness of Derivative Classification Decisions
5. (U) Effectiveness of Derivative Classification and Dissemination Control Marking Decisions
6. (U) Effectiveness of Security Self-Inspection Program
7. (U) Effectiveness of Security Reporting
8. (U) Effectiveness of Security Education and Training
9. (U) Intelligence Community (IC) Cross-Cutting Issues

(U~~//FOUO~~) We reviewed policies and documentation, interviewed Agency classifiers, and evaluated a judgmental sample of classified documents. Our

[1] (U) The ISOO is responsible to the President for policy and oversight of the government security classification system. The ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

sample review focused on classified information intended to be shared outside the Agency. Findings are reported in the areas of program management, original classification, derivative classification, self-inspections, and education and training.

(U~~//FOUO~~) Information security reporting is addressed in Finding One, and IC cross-cutting issues are addressed in Finding Two. Our review did not result in reportable findings in these areas.

(U) Background

(U) National Security Agency/Central Security Service (NSA/CSS) Information Security Program management

(U~~//FOUO~~) Federal organizations that create or hold classified information are responsible for its management. The Office of Information Security/Classification Policy (DJ2), which falls under the Associate Directorate for Policy and Records (DJ), administers NSA/CSS's classification management program. The Associate Director for Policy and Records is designated the Senior Agency Official (SAO) in NSA/CSS Policy 1-52, *Classified National Security Information*, 16 November 2012. DJ2 business lines include classification guide development, classification reviews, education and training programs, and the Agency's Information Security Self-Inspection Program.

(U) Executive Order (E.O.) 13526

(U~~//FOUO~~) E.O. 13526, *Classified National Security Information*, 5 January 2010, establishes policies and procedures for classification. The E.O. prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also expresses the President's belief that the nation's progress depends on the free flow of information within the government and to the American people.

(U) Levels of classification

(U~~//FOUO~~) Classified information - information requiring protection against unauthorized disclosure to prevent damage to national security - must be marked appropriately. E.O. 13526 defines three U.S. classification levels and the expected damage to U.S. security if information is disclosed inappropriately as:

1. (U~~//FOUO~~) Top Secret: information the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the Original Classification Authority (OCA) is able to identify or describe.
2. (U~~//FOUO~~) Secret: information the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the OCA is able to identify or describe.

3. (U~~//FOUO~~) Confidential: information the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the OCA is able to identify or describe.

(U~~//FOUO~~) E.O. 13526 mandates that, except as otherwise provided by statute, no other terms can be used to identify U.S. classified information. If significant doubt exists about the appropriate level of classification, information should be classified at the lower level.

(U) Original classification

(U~~//FOUO~~) Information may be originally classified only by OCAs, individuals authorized in writing by the President, the Vice President, agency heads, or other officials designated by the President to initially classify information. OCAs must receive training on proper classification before originally classifying information and at least once per calendar year thereafter. To make an original classification decision, an OCA must determine whether the information meets the following standards for classification:

- (U~~//FOUO~~) The information is owned, controlled, or produced by or for the U.S. government
- (U~~//FOUO~~) The information falls within one or more of the eight categories of information (reasons for classification) described in Section 1.4 of E.O. 13526 and
- (U~~//FOUO~~) The unauthorized disclosure of the information reasonably could be expected to result in damage to the national security that the OCA is able to identify or describe.

(U~~//FOUO~~) If significant doubt exists about the need to classify information, it should not be classified.

(U) Derivative classification

(U~~//FOUO~~) All personnel with active security clearances can perform derivative classification. Derivative classification is the incorporating, paraphrasing, restating, or regenerating of information that has already been classified and marking the newly developed material consistent with the classification markings that apply to the source information. All personnel who apply derivative classification markings must receive training on E.O. 13526 before derivatively classifying information and at least once every two years thereafter. Information may be derivatively classified from source documents or through classification guides.

(U) NSA/CSS Classification Advisory Officer (CAO) Program

(U~~//FOUO~~) The CAO Program, administered by DJ2, is unique to NSA. CAOs are responsible for ensuring that classified and sensitive information in their organizations is properly labeled and protected and that employees in their organizations understand and properly apply classification rules.

(U) Dissemination control and handling markings

(U//~~FOUO~~) Federal departments and agencies also have restrictive caveats that can be added to documents in the form of dissemination control and handling markings. These restrictions are not classifications; they identify the expansion or limitation on the distribution of the information. These markings are in addition to and separate from levels of classification. Only external dissemination control and handling markings approved by ISOO or, with respect to the IC, by the Director of National Intelligence may be used by agencies to control and handle the dissemination of classified information pursuant to agency policies issued under E.O. 13526.

II. (U) FINDING S AND RECOMMENDATIONS

(U) FINDING ONE: Information Security Program Management

(U//~~FOUO~~) The Agency's Information Security Program does not comply with E.O. 13526 because of outdated program guidance, a flawed classification tool, lack of classification elements in personnel performance appraisals, and a deficient classification challenge process.

(U) Outdated Program Guidance

(U) NSA/CSS Policy Manual 1-52

(U//~~FOUO~~) NSA/CSS Policy Manual 1-52, *NSA/CSS Classification Manual*, prescribes the policies and procedures critical for safeguarding NSA/CSS protected information. The manual, revised 8 January 2007, makes numerous references to the revoked E.O. 12958, *Classified National Security Information*, 17 April 1995, and has not been updated to conform to E.O. 13526. For example, the "Classified By" line required for derivative classification decisions is not included in the manual. In addition, the links in the manual do not work.

(U//~~FOUO~~) NSA's classification guidance lacks elements called for in E.O. 13526 and 32 C.F.R. Part 2001. The manual does not address statistical reporting to the ISOO, the accounting of costs associated with the implementation of E.O. 13526, and the actions to be taken for information declassified without proper authority.

(b) (3)-P.L. 86-36

(U) Classification guides

(U//~~FOUO~~) As of March 2013, the DJ2 web page for classification guides ("go classguides") listed 76 of the Agency's 177 classification guides currently in use, excluding guides that address [redacted]. The implementing directive, 32 C.F.R. Part 2001, requires that classification guidance be evaluated at least once every five years to ensure that it is current and to identify for declassification information that no longer requires protection. Updating classification guides is a collaborative process among DJ2, information owners, and CAOs and OCAs. Of the 76 classification guides listed, 13 were older than five years.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Update NSA/CSS Policy Manual 1-52 to comply with E.O. 13526. (ACTION: DJ2)
(U) Management Response (U//~~FOUO~~) **AGREE** NSA/CSS Policy Manual 1-52 is in coordination ; the target completion date is 30 September 2013. **(U) OIG Comment** (U) The planned action meets the intent of this recommendation .

(U//~~FOUO~~) Notify information owners, CAOs, and OCAs of the need to update outdated classification guides in compliance with E.O. 13526. (ACTION: DJ2)
(U) Management Response (U//~~FOUO~~) **AGREE** NSA/CSS Policy 1-52 identifies the roles and responsibilities for classifying, safeguarding, and declassifying NSA/CSS classified national security information. As DJ identifies outdated classification guides (older than 5 years) in the NSA Annual Security Classification Management Program Data Report (SF-311) response, DJ2 will notify information owners annually when formal guidance approaches the 5-year mark. This notification will occur no later than October of each year. **(U) OIG Comment** (U) The planned action meets the intent of our recommendation .

(U) Flawed Agency Classification Tools

(U//~~FOUO~~) NSA/CSS derivative classifiers do not adequately support classification levels in classified documents. The audit sample focused on two signals intelligence (SIGINT) reporting databases (Anchory and [redacted] because they contain information intended to be shared outside NSA. We analyzed [redacted] derivatively classified documents from these databases and determined [redacted]

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) E.O. 13526 requires that agencies that originate or handle classified information ensure that agency record systems optimize sharing and safeguarding of classified information and facilitate its declassification when it no longer meets the standards for continued classification. The Agency's classification tools [redacted] do not comply with E.O. 13526.

(U) **Identification of derivative classifier**

(U//~~FOUO~~) As shown in Figure 1, the Agency's classification tools [redacted] E.O. 13526 and the implementing directive, 32 C.F.R. Part 2001, require that the identity of the persons who apply derivative classification markings be apparent on each derivatively classified document; the derivative classifiers may be identified by name and position or by a personal identifier.

(U) **Derivative classification source**

(U//~~FOUO~~) NSA/CSS Policy Manual 1-52 provides explicit instructions on the requirements of a derivative classification block: the "Derived From" line must indicate the source of the classification determination. Each derivatively classified document must identify the documented original classification decision on which the derivative classification determination was based.

(U//~~FOUO~~) DJ2 permits Agency classifiers to classify documents derivatively [redacted] NSA/CSS Manual 1-52 was described by DJ2 as the Agency's overarching classification guide; however, it provides only general classification definitions and marking instructions with no specific guidance for classification.

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(U) Figure 1. Example of Incorrect NSA/CSS Classification Authority Block

(U//~~FOUO~~)

[redacted]

(U//~~FOUO~~)

(U//~~FOUO~~) The auto-populated classification authority block used for all documents in our review did not identify the appropriate classification guide or source documents that support the classification decisions. [redacted]

[redacted] From the information in the documents, we were unable to determine whether the classification markings were accurate.

(U//~~FOUO~~) We also noted that records printed from the [redacted] database do not include classification authority blocks, thereby impeding proper information sharing.

(U) **Derivative declassification date**

(U//~~FOUO~~) The Agency's classification tools automatically populate the declassification date [redacted] rather than carrying forward the declassification instructions of the original classification decision or source document as required by 32 C.F.R. Part 2001. This practice potentially allows the document to be declassified too soon or remain classified too long.

(U//~~FOUO~~) NSA/CSS Policy Manual 1-52 states that each derivatively classified document must include the date and identification of the documented original classification decision on which the derivative classification determination was based. In addition, the declassification instructions must be carried forward from the original classification decision.

(U//~~FOUO~~) Our review determined that the declassification dates for all [redacted] documents were based on the NSA/CSS Policy Manual 1-52 revised issue date, 8 January 2007, rather than the applicable classification guides' effective dates. As the example displayed in Figure 1 illustrates, [redacted]

(U//~~FOUO~~) We sent questionnaires to the point of contact (POC) aliases on [redacted] sampled reports; [redacted] POCs provided an applicable classification guide. For those [redacted] reports, we compared the declassification date listed in the "Declassify On" line and the declassification date that would have been used if the classification guide had been referenced.

(U//~~FOUO~~) As shown in Table 1, [redacted]

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(U) Table 1. Comparison of Anchory Report Declassification Dates Between NSA/CSS Policy Manual 1-52 and the Appropriate Classification Guide

(U//~~FOUO~~)

(U//~~FOUO~~)

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The information owners of Agency databases and systems potentially use different classification tools.

the classification tools must be updated to comply with E.O. 13526 and NSA/CSS Policy Manual 1-52.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Revise the requirements for the Agency's classification tools to include the following elements:

a. **(U//~~FOUO~~) Personal identifier of person who applied derivative classification markings,**
b. **(U//~~FOUO~~) Source document or the classification guide (drop-down menu of Agency guides), and**
c. **(U//~~FOUO~~) Declassification information carried forward from the source document or guide.**

(ACTION: DJ2)

(U) Management Response

(U//~~FOUO~~) **AGREE** The E.O. 13526 and 32 C.F.R. Part 2001 requirements for identification of persons who apply derivative classification markings by name and position or personal identifier, source documents used to derive classification markings, and date or event of declassification will be implemented through NSA/CSS Policy Manual 1-52. The revision of NSA/CSS Policy Manual 1-52 as the NSA Classification Guide as well as satisfaction of recommendations 4 and 5 will realize the intent of recommendation 3.

(U) OIG Comment

(U//~~FOUO~~) The planned action meets the intent of the recommendation.

(U//~~FOUO~~) Implement the Agency's classification tool revisions for Microsoft Office applications.

(ACTION: End User Solutions (T3)

(U) Management Response

(U//~~FOUO~~) **AGREE** TD agreed to implement the classification changes to the tool for Microsoft Office applications, upon DJ2 completion of Recommendation 3.

(U) OIG Comment

(U//~~FOUO~~) The planned action meets the intent of this recommendation.

(b) (3)-P.L. 86-36

[redacted]

a. (U//~~FOUO~~) [redacted]

b. (U//~~FOUO~~) **Ensure that all identified embedded classification tools are updated to comply with E.O. 13526 and NSA/CSS Policy Manual 1-52.**

(ACTION: T1)

(U) Management Response

(U//~~FOUO~~) **AGREE** TD concurs with the recommendation [redacted]

(U) OIG Comments

(U//~~FOUO~~) [redacted] TD agreed to determine the universe of embedded classification tools used in Agency databases and systems. The planned action meets the intent of the recommendation.

(U) Lacking Classification Element in Performance Evaluations

(U//~~FOUO~~) NSA/CSS Policy 1-52 designates the Associate Director for Policy and Records as the SAO responsible for directing NSA's information security program. E.O. 13526 requires that the SAO ensure that the performance contract or system used to rate civilian and military personnel includes the designation and management of classified information as a critical element in rating OCAs, security managers and specialists, and personnel who regularly apply derivative classification markings.

(U//~~FOUO~~) The uniform Defense Civilian Intelligence Personnel System requires that defense intelligence agencies develop performance management systems. NSA uses the Annual Contribution Evaluation (ACE) performance management system to satisfy this requirement.

(U//~~FOUO~~) NSA employees are evaluated according to six standard ACE performance elements: (1) accountability for results, (2) communication, (3) critical thinking, (4) engagement and collaboration, (5) personal leadership and integrity, and (6) technical expertise. These standards do not address classification management.

(U//~~FOUO~~) Because of the uniform ACE performance elements, DJ2 has been unable to satisfy E.O. 13526. Without the classification performance element, original and derivative classifiers are not held formally accountable for classification decisions.

(U//~~FOUO~~) Update NSA personnel performance objectives to include the designation and management of classified information as a critical performance element. **(ACTION: Management Gateway (MD2)**
(U) Management Response (U//~~FOUO~~) **AGREE** Effective 8 April 2013, MD incorporated changes to the ACE, performance element 6, for both supervisors and non-supervisors to comply with E.O. 13526. All documents created after 8 April 2013 contain the updated language. **(U) OIG Comment** (U) This recommendation is closed.

(U) Deficient Challenge Process

(U//~~FOUO~~) According to E.O. 13526, authorized holders of information who, in good faith, believe that its classification is improper are expected to challenge the classification. The E.O. directs the SAO to establish procedures through which authorized holders of information can challenge the classification of information they believe has been improperly classified. These procedures must ensure that:

- (U//~~FOUO~~) Individuals are not subject to retribution for bringing challenge s,
- (U//~~FOUO~~) An opportunity is provided for review by an impartial official or panel, and
- (U//~~FOUO~~) Individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel.

(U//~~FOUO~~) NSA/CSS Policy Manual 1-52 outlines the Agency's classification challenge process; however, the policy does not state that individuals may not be subject to retribution for challenging classifications.

(U//~~FOUO~~) According to interviewed Agency classifiers, derivative classifiers are unfamiliar with the classification challenge process or consider it intimidating. Derivative classifiers noted that classification is subjective, and they assume that experts, whom they would feel uncomfortable challenging, have classified classification guides and source documents. As a result, derivative classifiers might be unknowingly perpetuating misclassifications of source documents and guides and inhibiting information sharing.

(U) RECOMMENDATION 7
(U//~~FOUO~~) Update NSA/CSS Policy Manual 1-52 to declare that individuals who engage in the classification challenge process may not be subject to retribution. **(ACTION: DJ)**
(U) Management Response (U//~~FOUO~~) **AGREE** NSA/CSS Policy Memorandum 2013-02, Classification Challenges – Amendment to Policy Manual 1-52, was issued to document that no punitive action would be taken against an authorized holder who, in good faith, makes a classification challenge. This memorandum was issued on 3 May 2013. **(U) OIG Comment** (U) This recommendation is closed.

(U) RECOMMENDATION 8
(U//~~FOUO~~) Publicize the Agency's classification challenge process. **(ACTION: DJ)**
(U) Management Response (U//~~FOUO~~) **AGREE** NSA/CSS Policy Memorandum 2013-02 will be incorporated into NSA/CSS Policy Manual 1-52. An Agency-All message will be promulgated to the workforce upon the issuance of the updated NSA/CSS Policy Manual 1-52. A tailored message will be sent to the CAO population using the Electronic Subscription Service messaging system. **(U) OIG Comment** (U) The planned action meets the intent of our recommendation.

(U) This page intentionally left blank.

(U) FINDING TWO: Original Classification

(U//~~FOUO~~) Agency original classification guidance is sometimes conflicting and incomplete. As a result, derivative classifications might be inaccurate.

(U) Original Classification Authority

(b)(3)-P.L. 86-36

(U//~~FOUO~~) NSA/CSS has [redacted] OCAs authorized to exercise TOP SECRET original classification authority in accordance with E.O. 13526, as stated in the Deputy Secretary of Defense Memorandum, "Delegation of Top Secret Original Classification Authority," 5 May 2011. We interviewed a judgmental sample of [redacted] Agency OCAs and reviewed their 2012 original classification decisions. Table 2 provides the Agency's original classification decisions for FY2012.

(U) Table 2. NSA/CSS Original Classification Decisions

(U//~~FOUO~~)

2012	41	23	3	67

(U//~~FOUO~~)

(U//~~FOUO~~) According to 32 C.F.R. Part 2001, information for derivative classification shall be carried forward from the source document or taken from the appropriate classification guide. Therefore, original classification decisions provide the basis for derivative classifications. The majority of Agency original decisions take the form of published classification guides. Inaccurate OCA guidance leads to incorrect derivative classification decisions.

(U) Conflicting Classification Guidance

(U//~~FOUO~~) We selected the FY2012 Agency Financial Report (AFR) for review because it is shared throughout the IC. The AFR contains 43 classified paragraphs and 56 classified tables. The remainder of the report is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO).

(U//~~FOUO~~) The AFR has input from many Agency Directorates and information classified under many sources, including internal policy, the *Office of the Director of National Intelligence (ODNI) Classification Guide*, and the NSA *Finance Classification Guide 7-1*.

(U//~~FOUO~~) The AFR went through several classification reviews. Information was initially reviewed by CAOs from each contributing directorate; then the report was compiled and reviewed by the Office of Resource Management Policy (BFP1) (an organization that consists mostly of CAOs). Finally, the AFR was sent to DJ2 for a corporate classification review before it was published. DJ2 provided classification and marking

recommend ations that were not implemented; this resulted in the audit team finding marking discrepancies.

(U//~~FOUO~~) These discrepancies occurred because the NSA *Finance Classification Guide* is outdated and conflicts with the *ODNI Classification Guide*. The *Finance Classification Guide*, last updated in August 2007, was more than five years old when the AFR was written. The guide lacks the required declassification instructions on the front page and the reason for classification. E.O. 13526 requires a concise reason for classification that, at a minimum, cites the applicable classification categories in Section 1.4 of the Order. The POC for questions is an e-mail alias that is no longer used.

(U//~~FOUO~~) The NSA *Finance Classification Guide* and the *ODNI Classification Guide* also present conflicting guidance, which resulted in conflicting markings in the AFR.

(b)(3)-P.L. 86-36

(U) **AFR marking discrepancies**

(U//~~FOUO~~) We found derivative marking errors and discrepancies in the AFR, which we attribute to the conflicting original classification guidance. The report contained several marking discrepancies between the tables of financial data and the paragraphs that describe the data in the tables. The tables were marked S//NF, and the paragraphs S//REL TO USA, FVEY.

(U//~~FOUO~~) The AFR also contained marking discrepancies that could be described as misclassification. In two cases, financial data was marked S//NF and the paragraph describing this data was marked U//FOUO. Another section of the AFR marked the same dollar value at three levels: U//FOUO, S//REL TO USA, FVEY, and S//NF.

(U//~~FOUO~~) Potential over-classification was also found: a paragraph was marked S//REL TO USA, FVEY, yet, according to the NSA Finance and ODNI classification guides, it does not contain SECRET information. The paragraph refers to Office of Management and Budget Circulars A-136 and A-11, which are unclassified documents; therefore, the source and justification for the S//REL TO USA, FVEY classification level are questionable.

[redacted]

(U//~~FOUO~~) Coordinate with ODNI to ensure that the *Finance Classification Guide 7-1* and the *ODNI Classification Guide* agree.

(ACTION: DJ2)

(U) Management Response

(U//~~FOUO~~) **AGREE** DJ2 coordinated the *Finance Classification Guide* (7-1) with Resources Management Policy & Budget Structure Management (BFP) and ODNI IC CIO/Information and Data Management office personnel. This eliminated conflict between ODNI classification guidance and NSA/CSS specific classification guidance. The revised guide was signed by the OCA on 21 May 2013.

(U) OIG Comment

(U) This recommendation is closed.

(U) Incomplete Classification Guidance

(U//~~FOUO~~) The current NSA/CSS [redacted]

(b)(3)-P.L. 86-36

(U//~~FOUO~~) A team of FISA experts, including DJ leadership, the Office of General Counsel, and the Office of SIGINT Policy and Corporate Issues (S02), are reviewing FISA classifications. Because the Department of Justice (DoJ) and ODNI oversee Agency FISA reporting, their participation is necessary in developing a complete and non-conflicting guide. DJ has ruled that anything not covered in the guide must be handled case by case and OCA decisions should be drafted after coordination with DoJ and ODNI.

(U//~~FOUO~~) Since this determination by DJ, efforts commenced to develop a list of facts not included in the current FISA guide; the list includes [redacted] The facts were shared with DoJ. Despite progress toward a completed guide, the current process has been inefficient and consumed the resources of several senior officials by requiring individual decisions.

(U//~~FOUO~~) Coordinate with ODNI and DoJ to develop a classification guide that adequately addresses FAA §702. **(ACTION: DJ)**

(U) Management Response

(U//~~FOUO~~) **AGREE** NSA submitted a list of §702-related facts that may have been declassified to DNI for approval. A proposed revision to the NSA FISA guide will also require prior approval by ODNI and DoJ. Assuming this approval is received, the NSA FISA guide will be updated by 31 December 2014.

(U) OIG Comments

(U//~~FOUO~~) The planned action meets the intent of the recommendation. In addition to including the facts that may have been declassified, the current FISA guide does not fully address the classification of some FISA §702 facts. The OIG suggests that DJ also include the list of facts currently not included in the FISA guide, which is discussed in this finding under "Incomplete Classification Guidance."

(U) FINDING THREE: Derivative Classification

(U//~~FOUO~~) Agency derivative classifications are sometimes improper because of unclear requirements, unsubstantiated classification decisions, and confusing lines of authority. As a result, the Agency cannot ensure that classified information is protected and shared at the correct level.

(U) Unclear Derivative Classification Requirements

(U//~~FOUO~~) We used interviews and questionnaires to assess derivative classifier knowledge of classification management principles and procedures. Sampled derivative classifiers understand their classification role and the difference between original and derivative classification authority.[2]

(U//~~FOUO~~) Derivative classifiers understood the requirements of derivative classifications, such as banner and portion markings and classification authority blocks.

(U//~~FOUO~~) Derivative classifiers are required to take CLAS1000 annually. This course explains derivative classification requirements; yet, it does not adequately explain how to fulfill the requirements. (See Finding Five for an assessment of Agency classification training.)

(U//~~FOUO~~) The information provided to Agency derivative classifiers is unclear and contradictory. As a result, derivative classifiers sometimes do not make proper decisions.

(U) Improperly Substantiated Derivative Classification Decisions

(U//~~FOUO~~) Sampled derivative classifiers did not understand the difference between marking manuals and classification guides; they sometimes used outdated classification markings and did not consistently carry forward classification levels from one document to another.

(U//~~FOUO~~) As discussed in Finding One, our review of [redacted] sampled documents revealed that none referred to appropriate classification guides; all the documents referred to NSA/CSS Policy Manual 1-52. Of the [redacted] reports reviewed, we were able to identify POCs for [redacted]. We sent [redacted] questionnaires to these POCs, typically organizational e-mail addresses, and asked the derivative classifiers to provide the classification guides or source documents used to support the classification levels of the reports:

(b) (3)-P.L. 86-36

- (U) [redacted] derivative classifiers did not provide a classification guide, a source document, or a marking manual.
- (U) [redacted] derivative classifiers provided marking manuals.

(b) (3)-P.L. 86-36

[2] (U//~~FOUO~~) Sampled derivative classifiers included Anchory and financial report writers and CAOs.

- (U) [redacted] derivative classifiers provided classification guides.
- (U) [redacted] derivative classifiers provided marking manuals and classification guides.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Because [redacted] derivative classifiers provided classification guides, we were able to validate classification levels for [redacted] documents.

(U//~~FOUO~~) [redacted] respondents who provided marking manuals stated that their classifications were based on NSA/CSS Policy 123-2 (24 February 1998). However, NSA/CSS Policy Manual 1-52 superseded this manual in November 2004.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Additional training is needed for derivative classifiers to ensure that the classification of information and the declassification date are based on appropriate classification guides or source documents. Finding Five recommends including these topics in the Agency's mandatory classification training.

(U) **Control marking inconsistencies in reporting**

(U//~~FOUO~~) **Outdated markings** We reviewed [redacted] documents to determine whether derivative classifiers applied the correct banner and portion markings.

(U//~~FOUO~~) NSA/CSS Policy Manual 1-52 implemented the requirement from ODNI Controlled Access Program Coordination Office (CAPCO) to eliminate the communications intelligence (COMINT) code words UMBRA and SPOKE, effective October 1999. COMINT information formerly protected by these code words should now be protected as special intelligence (SI). The Agency announced at that time that certain software applications would continue to use the code words until software changes could be made and that all applications could not be changed simultaneously. However, 14 years later, [redacted] FY2012 reports used these outdated classification markings: [redacted] were marked "UMBRA" and [redacted] "SPOKE."

(U//~~FOUO~~) ODNI has requested that NSA eliminate the code words or obtain an exemption to continue using the obsolete markings. Currently, NSA does not have an exemption.

(b) (3)-P.L. 86-36

[redacted]

(U//~~FOUO~~) Comply with CAPCO guidance to eliminate the use of retired code words or obtain a waiver for non-compliant software applications.

(ACTION: S1S)

(U) Management Response

(U//~~FOUO~~) **REASSIGNED** DJ recommended designating the Information Sharing Services Group (S1S) as the lead for this action.

(U) OIG Comment

(U//~~FOUO~~) OIG coordinated with S1S to eliminate the use of retired code words or obtain a waiver for non-compliant software applications. The planned action meets the intent of the recommendation

(U) Confusion over Lines of Authority

(U//~~FOUO~~) NSA lacks a single corporate source for classification guidance. DJ oversees DJ2, which is the perceived source for classification reviews and guidance. However, [redacted] other offices also conduct classification reviews, depending on the document or topic to be reviewed. [redacted]

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(U//~~FOUO~~) DJ2 reviewed and provided classification guidance on the OIG Intelligence Oversight *Draft Report on Assessment of Management Controls Over SFAA 702* [redacted]

(U//~~FOUO~~) In our assessment of derivatively classified documents, we found evidence of [redacted]

[redacted]

(U//~~FOUO~~) Publicize the lines of authority for classification reviews on the DJ and DJ2 web sites to make users aware of the responsible organizations.

(ACTION: DJ)

(U) Management Response

(U~~//FOUO~~) **AGREE** The Office of Policy and Records will publicize the specific classification advisory officer (CAO) functions performed on behalf of agency personnel by DJ and DJ2. The target completion date is 30 September 2013.

(U) OIG Comment

(U~~//FOUO~~) DJ2 agreed to publish any CAO functions that they will not perform on their web site. The planned action meets the intent of the recommendation.

(U) FINDING FOUR: Information Security Self-Inspection Program

(U//~~FOUO~~) The NSA/CSS Self-Inspection Program is incomplete because of missing report elements and a flawed program focus. As a result, DJ management is unable to identify and correct problems in the program.

(U) Criteria

(U//~~FOUO~~) Section 5.4(d)(4) of E.O. 13526 and 32 C.F.R. Part 2001.60 require that designated SAOs establish self-inspection programs and report annually on them to the Director of the ISOO. The reports should provide information about the structure and implementation of the Agency's program.

(U//~~FOUO~~) NSA/CSS Policy 1-52 and Policy Manual 1-52 do not include the elements of self-inspections that E.O. 13526 and 32 C.F.R. Part 2001 require. NSA/CSS Policy Manual 1-52 includes a short annex stating that DJ, with assistance from CAOs, shall perform periodic agency self-inspections. A link is provided for additional information; however, the link directs readers to an error page.

(U) Missing Report Elements

(U//~~FOUO~~) The SAO's annual report to the Director of ISOO should include:

1. (U) A description of the Agency's self-inspection program,
2. (U) An assessment and summary of the findings,
3. (U) Specific information about the findings of the annual review of the Agency's original and derivative classification actions, including the volume of classified materials reviewed and the number and type of discrepancies identified,
4. (U) Actions that have been taken or are planned to correct deficiencies or misclassifications and to deter their recurrence, and
5. (U) Best practices.

(U//~~FOUO~~) **SAO involvement** Agency policy fails to explicitly assign responsibility to the SAO for the self-inspection program. The implementing directive, 32 C.F.R. Part 2001.60, states that the self-inspection program shall be structured to provide the SAO with information necessary to assess the effectiveness of the classified national security information program. The directive also requires that the SAO report annually to the Director of ISOO, who noted that *NSA's 2012 Self-Inspection Program Report* had not been endorsed with the SAO's signature.

(U//~~FOUO~~) **Program description** The self-inspection program report fails to sufficiently describe the Agency's program. The *NSA/CSS Information Security Self-Inspection Program Standard Operating Procedures* were included in the report; [redacted]

(U) Flawed Self-Inspection Program Focus

(U//~~FOUO~~) The Agency's self-inspection program should verify classification markings; however, the program does not evaluate a representative sample of Agency documents to ensure proper classification.

(U//~~FOUO~~) According to DJ2 and the 2011 and 2012 NSA/CSS Annual Self-Inspection Program Reports, the NSA/CSS self-inspection focuses on classification marking format (e.g., classification banners, portion markings). [redacted]

(b) (3)-P.L. 86-36

(U//~~FOUO~~) The 2012 NSA/CSS Self-Inspection Program Report fails to address deficiencies in the following required areas:

[redacted]

(U) RECOMMENDATION 13

(U//~~FOUO~~) Update NSA/CSS Policy Manual 1-52 to include the essential elements for self-inspections in accordance with E.O. 13526 and 32 C.F.R. Part 2001.

(ACTION: DJ2)

(U) Management Response

(U//~~FOUO~~) **AGREE** The NSA Annual Self-Inspection Program Report for FY2012 was fully compliant with ISOO requirements when provided to OUSD(I). The essential elements for self-inspections will be added to the draft NSA/CSS Policy Manual 1-52.

(U) OIG Comment

(U) The planned action meets the intent of the recommendation .

(U//~~FOUO~~) Include a review of classification levels in the NSA/CSS Information Security Self-Inspection Program. **(ACTION: DJ2)**
(U) Management Comments (U//~~FOUO~~) **AGREE** The Information Security Policy Self-Inspection SOP and related software templates were updated on 4 June 2013 to require DJ2 review of submitted material for appropriate use of classification. The self-inspection assessment will indicate instances of overclassification and provide recommendation(s) for corrective action. These changes will be implemented with the next scheduled self-inspection projected to commence between August and October 2013. **(U) OIG Comment** (U) The planned action meets the intent of the recommendation.

(U) This page intentionally left blank.

(U) FINDING FIVE: Information Security Education and Training

(U//~~FOUO~~) NSA/CSS mandatory classification training does not teach derivative classifiers how to accurately classify information. NSA/CSS employees are not compelled to complete mandatory training. As a result, some Agency derivative classifiers are making improper classifications.

(U) Lack of Essential Elements in Mandatory Derivative Classification Training

(U//~~FOUO~~) We evaluated NSA/CSS classification training courses to determine whether they met the requirement of E.O. 13526 and Intelligence Community Directive (ICD) 710, *Classification and Control Marking System*[3]. We also reviewed training records for a sample of NSA/CSS employees to determine whether they had completed the mandatory classification training.

(U//~~FOUO~~) DJ2 with the Associate Directorate for Education and Training (ADET) developed CLAS1000, "Elements of Classification and Marking," to satisfy the training requirements of E.O. 13526 and ICD 710 and to educate personnel on the basic principles of marking and safeguarding classified national security information.

(U//~~FOUO~~) We reviewed CLAS1000 training material and determined that the course met the minimum requirements of E.O. 13526 and ICD 710. However, the training course discusses only basic principles of information classification markings.

- (U//~~FOUO~~) The training did not prepare derivative classifiers to classify specific pieces of information accurately. [redacted]

(b) (3) -P.L. 86-36

(b) (3) -P.L. 86-36

- (U//~~FOUO~~) The training did not provide sufficient instruction on derivative classification. CLAS1000 discussed the classification authority block and stated that citations for the identification of source documentation should include the title, originating agency,

[3] Intelligence Community Directive 710, *Classification and Control Markings System* requires heads of IC elements to establish continuing training and education programs within their elements, including an annual workforce training requirement that ensures a complete and common understanding of the classification and control marking system.

and date of each source. In addition, when a document is classified derivatively based on more than one source, a complete list must appear or be attached to every copy of the document. Derivative classifiers are told to respect original classification decisions and carry forward all classification and control markings. Derivative classifiers must ensure that classified information is accurately traceable and mark documents properly to provide adequate protection from unauthorized disclosure.

(U//~~FOUO~~) Although CLAS1000 addresses proper application of E.O. 13526 and provides the NSA/CSS workforce with a basic framework to classify information , it does not provide specific guidance on the implementation of the framework . Furthermore, it does not provide sufficient explanations to ensure that OCA decisions are enforced and carried forward appropriately.

(U//~~FOUO~~) We evaluated other classification courses to determine whether additional material could be incorporated into CLAS1000 to provide derivative classifiers with more complete guidance. We identified three courses—CLAS1500, CLAS2000, and CLAS2200—that provide additional instruction on proper classifications and on identifying classification guides and using them to derive appropriate classification and control markings. These are critical skills needed by all derivative classifiers. Derivative classifiers could benefit from having this additional course material incorporated into the annual mandatory training. The material addresses the problems discussed in Findings One and Two of this report.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Update CLAS1000 to include additional coverage on proper classifications and on identifying classification guides and using them to derive appropriate classification control markings.

(ACTION: DJ2 with ADET)

(U) Management Comments

(U//~~FOUO~~) **AGREE** DJ submitted a New Learning Solution request for ADET to update and revise CLAS1000, with all modules undergoing update and/or revision as appropriate.

(U) OIG Comment

(U) The planned actions meet the intent of the recommendation.

[4] (U//~~FOUO~~) NSA/CSS databases (e.g., Anchory

(U) CLAS1000 Completion

(U//~~FOUO~~) NSA/CSS requires that all NSA/CSS civilian and military personnel take CLAS1000 annually. E.O. 13526 states that derivative classifiers who do not receive such training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received the training. DJ2 personnel stated that, to date, no one has been suspended for non-completion.

(U//~~FOUO~~) Under 32 C.F.R. Part 2001, persons who apply derivative classification markings must receive training on derivative classification principles before derivatively classifying information and at least once every two years. The C.F.R. also states that the Agency must provide refresher training at least annually for all personnel who handle or generate classified information.

(U//~~FOUO~~) According to NSA/CSS Policy 1-52, all NSA/CSS civilian and military personnel must complete annual information security training. Civilian, military, contractor, and integree personnel working within NSA/CSS spaces and performing NSA/CSS mission but not assigned to the Agency are encouraged but not required to receive this training. However, the policy also states that all authorized holders of NSA/CSS information must complete annual information security refresher training compliant with DoD and ODNI requirements.

(U//~~FOUO~~) We requested training histories for the [redacted] derivative classifiers whom we interviewed and to whom we had sent questionnaires to determine whether they had completed CLAS1000 in 2011 and 2012.[5] According to the training histories ADET provided, [redacted] NSA/CSS employees in our sample of [redacted] had not completed CLAS1000.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) We also asked ADET for the number of NSA/CSS employees who did not complete CLAS1000 in 2011 or 2012. The information is summarized in Table 3.

(U) Table 3. NSA/CSS Employees Who Did Not Complete CLAS1000

(U//~~FOUO~~)

Civilian	**13.2**	**18.1**
Military	**51.6**	**63.1**
Contractor	**82.7**	**44.7**
* (U//~~FOUO~~) The completion percentages might be skewed. The numbers are calculated as a running tally of personnel who enter and leave throughout the year. The totals, therefore, are higher than the number of personnel at the Agency at any single point in the year.		

(U//~~FOUO~~)

[5] (U//~~FOUO~~) Sampled employees included Anchory and AFR writers, CAOs, and OCAs.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Although the Agency's 2011 and 2012 ICD 710 reports stated that NSA/CSS requires and has established a continuing information security training and education program, there is no oversight to ensure that NSA/CSS employees complete mandatory classification training.

[redacted] Because this type of enforcement spans Directorates, it is outside of DJ's authority to enforce compliance; therefore, the OIG is referring this recommendation to the NSA/CSS Chief of Staff for resolution.

[redacted]

a. (U//~~FOUO~~) Develop measures to identify Agency personnel who are not compliant with the mandatory classification training.

b. (U//~~FOUO~~) Provide a list of non-compliant personnel to DJ2.

(ACTION: ADET)

(U) Management Comments

(U//~~FOUO~~) **AGREE** The ADET database of record, Enterprise Learning Management (ELM), sends automated reminder notifications to all personnel who have not completed mandatory training on a set monthly schedule. Each manager has access to ELM to view compliance for employees assigned to them in HRMS. Several reports display the status of the employees' mandatory training completion. Upon a request from DJ2, the ELM administrators can arrange for the list to be provided.

(U) OIG Comment

(U) The planned action meets the intent of the recommendation.

[redacted]

(U//~~FOUO~~) Document and implement measures to enforce compliance with the mandatory classification training.

(ACTION: DC)

(U) Management Comments

(U//~~FOUO~~) **AGREE** The NSA/CSS Chief of Staff has agreed to document and implement measures to enforce compliance with the mandatory training requirement .

(U) OIG Comment

(U) The planned action meets the intent of the recommendation.

III. (U) OBSERVATIONS

(U) Lack of CAO Program Oversight

(U//~~FOUO~~) NSA/CSS established a cadre of CAOs throughout the enterprise to interpret and assist derivative classifiers in the application of classification policy and guidance. NSA/CSS Policy 1-52 describes CAO responsibilities:

- (U//~~FOUO~~) Provide guidance on protecting and marking national security information and classification matters
- (U//~~FOUO~~) Assist in developing classification and declassification guides
- (U//~~FOUO~~) Perform initial classification review of NSA/CSS information intended for public dissemination
- (U//~~FOUO~~) Convey classification information and issues between their organizations and DJ2
- (U//~~FOUO~~) Assess the classification training needs of their organization
- (U//~~FOUO~~) Assist DJ2 with the NSA/CSS Self-Inspection Program
- (U//~~FOUO~~) Remain knowledgeable of NSA/CSS and higher level policies governing classification

(U//~~FOUO~~) DJ2 does not track the number of Agency CAOs. However, it provided an estimate of more than [redacted] We analyzed the CAO personnel lists on DJ2's CAO web page and determined that [redacted] CAOs were listed, as of April 2013.

(U//~~FOUO~~) We interviewed CAOs from [redacted] Agency Directorates to understand program responsibilities, time required for CAO duties, and the system used to track CAO reviews. Of the [redacted] CAOs interviewed, [redacted] stated that their CAO responsibilities are "additional duties as assigned" and that their management does not fully understand how much effort goes into performing this duty. The amount of time CAOs spent executing their CAO responsibilities varied greatly. For example, one CAO stated that he spends only five percent of his time performing CAO reviews, whereas another CAO stated that she spends approximately 75 percent of her time executing CAO responsibilities .

(U//~~FOUO~~) We requested a list of documents that the CAOs reviewed between 1 April and 30 September 2012 to select a sample for evaluation; however, DJ2 does not require CAOs to document their reviews. [redacted]

(b) (3) -P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Although CAOs feel comfortable asking DJ2 for guidance, we did not find evidence that DJ2 reviews documents for classification accuracy, unless the CAOs specifically requested that it do so. Requiring CAOs to track and maintain the reviewed documents would enable CAOs to monitor how much of their time is spent on CAO duties and provide that evidence to management. In addition, this would enable DJ2 to perform quality control by selecting a sample of CAO-reviewed documents during the annual self-inspections to ensure that classification decisions are accurate and in accordance with Agency policies.

(U) AUDIT SUGGESTION

(U//~~FOUO~~) Require CAOs to track the documents they review as part of their CAO duties.

(ACTION: DJ2)

(U) AUDIT SUGGESTION

(U//~~FOUO~~) During the annual information security program self-inspections, perform quality control of CAO-reviewed documents to ensure that classification decisions are accurate and in accordance with Agency policies.

(ACTION: DJ2)

(U) Inadequate CAO Training

(U//~~FOUO~~) The NSA/CSS Classification Advisory Officer Program Memorandum, 21 June 2010, requires that prospective CAOs successfully complete CLAS2200, "Principles of Classification and Information Security," before appointment as a CAO. Agency policy, however, does not require that CAOs receive continual or updated training thereafter.

(U//~~FOUO~~) We requested from ADET the training histories for [redacted] CAOs and determined that, although all [redacted] were compliant with the CLAS2200 training requirement, only one had taken the course more than once. Five of the [redacted] CAOs took the course in or before 2009; therefore, these five CAOs have not received training on E.O. 13526. In addition, according to ADET, CLAS1500, "Classification Marking Mechanics," is a mandatory prerequisite for CLAS2200 offerings that commence on or after 1 August 2012. Of the [redacted] CAOs reviewed, only two had completed that class.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Require CAOs to complete classification refresher training. (ACTION: DJ2)

(U) This page intentionally left blank.

IV. (U) SUMMARY OF RECOMMENDATIONS

(U) RECOMMENDATION 1

(U//~~FOUO~~) Update NSA/CSS Policy Manual 1-52 to comply with E.O. 13526.

(U) ACTION: DJ2
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 2

(U//~~FOUO~~) Notify information owners, CAOs, and OCAs of the need to update outdated classification guides in compliance with E.O. 13526.

(U) ACTION: DJ2
(U) Status: **OPEN**
(U) Target Completion Date: 31 October 2013

(U) RECOMMENDATION 3

(U//~~FOUO~~) Revise the requirements for the Agency's Classification tools to include the following elements:

a. **(U//~~FOUO~~) Personal identifier of person who applied derivative classification markings,**
b. **(U//~~FOUO~~) Source document or the classification guide (drop-down menu of Agency guides), and**
c. **(U//~~FOUO~~) Declassification information carried forward from the source document or guide.**

(U) ACTION: DJ2
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 4

(U//~~FOUO~~) Implement the Agency's classification tool revisions for Microsoft Office applications.

(U) ACTION: T3
(U) Status: **OPEN**
(U) Target Completion Date: 30 June 2014

(b)(3)-P.L. 86-36

(U) RECOMMENDATION 5

a. (U//~~FOUO~~)

b. (U//~~FOUO~~) **Ensure that all identified embedded classification tools are updated to comply with E.O. 13526 and NSA/CSS Policy Manual 1-52.**

(U) ACTION: **T1**
(U) Status: **OPEN**
(U) Target Completion Date: 30 June 2014

(U) RECOMMENDATION 6

(U//~~FOUO~~) **Update NSA personnel performance objectives to include the designation and management of classified information as a critical performance element.**

(U) ACTION: **MD2**
(U) Status: **CLOSED**

(U) RECOMMENDATION 7

(U//~~FOUO~~) **Update NSA/CSS Policy Manual 1-52 to declare that individuals who engage in the classification challenge process may not be subject to retribution.**

(U) ACTION: **DJ**
(U) Status: **CLOSED**

(U) RECOMMENDATION 8

(U//~~FOUO~~) **Publicize the Agency's classification challenge process.**

(U) ACTION: **DJ**
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 9

(U//~~FOUO~~) **Coordinate with ODNI to ensure that the *Finance Classification Guide 7-1* and the *ODNI Classification Guide* agree.**

(U) ACTION: **DJ2**
(U) Status: **CLOSED**

(U) RECOMMENDATION 10

(U//~~FOUO~~) **Coordinate with ODNI and DoJ to develop a classification guide that adequately addresses FAA §702.**

(U) ACTION: **DJ**

(U) Status: **OPEN**
(U) Target Completion Date: 31 December 2014

(U) RECOMMENDATION 11

(U//~~FOUO~~) Comply with CAPCO guidance to eliminate the use of retired code words or obtain a waiver for non-compliant software applications.

(U) ACTION: S1S
(U) Status: **OPEN**
(U) Target Completion Date: **TBD**

(U) RECOMMENDATION 12

(U//~~FOUO~~) Publicize the lines of authority for classification reviews on the DJ and DJ2 web sites to make users aware of the responsible organizations.

(U) ACTION: DJ
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 13

(U//~~FOUO~~) Update NSA/CSS Policy Manual 1-52 to include the essential elements for self-inspections in accordance with E.O. 13256 and 32 C.F.R. Part 2001.

(U) ACTION: DJ2
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 14

(U//~~FOUO~~) Include a review of classification levels in the NSA/CSS Information Security Self-Inspection Program.

(U) ACTION: DJ2
(U) Status: **OPEN**
(U) Target Completion Date: 31 October 2013

(U) RECOMMENDATION 15

(U//~~FOUO~~) Update CLAS1000 to include additional coverage on proper classifications and on identifying classification guides and using them to derive appropriate classification control markings.

(U) ACTION: DJ2 with ADET
(U) Status: **OPEN**
(U) Target Completion Date: 27 September 2013

(U) RECOMMENDATION 16

a. (U//~~FOUO~~) Develop measures to identify Agency personnel who are not compliant with the mandatory classification training.

b. (U//~~FOUO~~) Provide list of non-compliant personnel to DJ2.

(U) ACTION: ADET
(U) Status: **OPEN**
(U) Target Completion Date: 30 September 2013

(U) RECOMMENDATION 17

(U//~~FOUO~~) Document and implement measures to enforce compliance with the mandatory classification training.

(U) ACTION: DC
(U) Status: **OPEN**
(U) Target Completion Date: **TBD**

V. (U) ABBREVIATIONS AND ORGANIZATIONS

(U) ACE	Annual Contribution Evaluation
(U) ADET	Associate Directorate for Education and Training
(U) AFR	Agency Financial Report
(U) CAO	Classification Advisory Officer
(U) CAPCO	Controlled Access Program Coordination Office
(U) C.F.R.	Code of Federal Regulations
(U) COMINT	communications intelligence
(U) DJ	Associate Directorate for Policy and Records
(U) DJ2	Office of Information Security/Classification Policy
(U) DoD	Department of Defense
(U) DoJ	Department of Justice
(U) ELM	Enterprise Learning Management
(U) E.O.	Executive Order
(U) FAA	FISA Amendments Act
(U) FISA	Foreign Intelligence Surveillance Act
(U) IC	Intelligence Community
(U) ICD	Intelligence Community Directive
(U) ISOO	Information Security Oversight Office
(U) NSA/CSS	National Security Agency/Central Security Service
(U) OCA	Original Classification Authority
(U) ODNI	Office of the Director of National Intelligence
(U) OIG	Office of the Inspector General
(U) MD2	Management Gateway
(U) P.L.	Public Law
(U) POC	point of contact
(U) S02	Office of SIGINT Policy and Corporate Issues
(U) SAO	Senior Agency Official
(U) SI	special intelligence
(U) SIGINT	signals intelligence
(U) S//NF	SECRET//NOFORN
(U) S//REL TO USA, FVEY	SECRET//RELEAS ABLE TO USA AND FIVE EYES
(U) T314	End User Services
(U) TD	Technology Directorate
(U) U//FOUO	UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Audit

(U) This page intentionally left blank.

(U) ABOUT THE AUDIT

(U) Objective

(U//~~FOUO~~) The specific audit objectives were to assess whether classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within the National Security Agency/Central Security Service (NSA/CSS) and to identify policies, procedures, rules, regulations, or management practices that might be contributing to persistent over-classification of material within NSA.

(U) Scope and Methodology

(U) The audit fieldwork was conducted from January to April.

(U//~~FOUO~~) We met with personnel from the Information Security/Classification Policy Office (DJ2); in addition, we interviewed a judgmental sample of [redacted] Agency OCAs and reviewed their 2012 original classification decisions. We met with [redacted] of the Agency's Classification Advisory Officers, and sent classification questionnaires to [redacted] Anchory points of contact. We also sent surveys to [redacted] derivative classifiers and evaluated the [redacted] responses received. We reviewed Executive Orders, Public Laws, and Department of Defense (DoD) regulations and evaluated NSA/CSS guidance related to classification, including policies and training.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) We reviewed [redacted] reports from the Anchory and [redacted] databases because the databases are used for reporting signals intelligence (SIGINT) data. We obtained a download for all reports and records in the databases between 1 April and 30 September 2012 that were classified at or above the CONFIDENTIAL level. In addition, we reviewed the FY2012 Agency Financial Report (AFR). We then evaluated the Anchory reports, [redacted] records, and AFR against DoD Inspector General's *Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the "Reducing Over-Classification Act" Appendix C (Methodology for Determining the Appropriateness of a Derivative Classification Decision).*

(b) (3)-P.L. 86-36

(U//~~FOUO~~) We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U) Use of Computer-Processed Data

(U~~//FOUO~~) To achieve the audit objectives, we relied on computer-processed data from SIGINT reporting databases. The computer-processed data was used in aggregate to make random report selections. No conclusions were based on any single data entry record. Although we did not perform a formal reliability assessment of the computer-processed data, we did not find errors that would preclude use of the data to meet objectives or that would change the conclusions in the report, and Agency personnel did not identify errors.

(U) Prior Coverage

(U~~//FOUO~~) No audits have focused specifically on the classification of information. However, many audits have included reviews of the databases referenced in the report.

(U) Managers' Internal Control Program

(U~~//FOUO~~) As part of the audit, we assessed the organization's control environment pertaining to the audit objective, as set forth in NSA/CSS Policy 7-3, *Internal Control Program*, 14 February 2012. On 4 June 2012, the Associate Directorate for Policy and Records provided a qualified statement of reasonable assurance that the Office of Policy and Records internal controls met the objectives of the Federal Manager's Financial Integrity Act. The qualified statement was, in part, due to insufficient resources to meet responsibilities for declassification. E.O. 13526 mandates declassification activities to NSA/CSS. Problems that complicate completion of the task include recruiting and training a workforce with senior reviewers who have deep SIGINT and information assurance experience and who can keep pace with a high number of declassification referrals, mandatory 25-year reviews, and mandatory declassification reviews.

(U) APPENDIX B

(U) Full Text of Management Comments

(U) This page intentionally left blank.

(U) OFFICE OF POLICY AND RECORDS RESPONSE

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Office of Policy and Records
Revised Response to the
Office of the Inspector General
Draft Report

2 August, 2013

Subject: (U) Revised Response on the Audit of NSA's Compliance with PL 111-258, the "Reducing Over-Classification Act" (AU-13-0005)

(U//~~FOUO~~) The Office of Policy and Records (DJ) appreciated the opportunity to review and comment on the NSA/CSS Office of the Inspector General (OIG) Draft Report titled Audit of NSA's Compliance with PL 111-258, the "Reducing Over-Classification Act" (AU-13-0005). Responses on specific findings and recommendations assigned to DJ follow below, with revised responses to three (3) recommendations.

(U) Findings and Recommendations

(U) Finding One: (U) Information Security Program Management
(U) Recommendation 1 (DJ2): (U) Update NSA/CSS Policy Manual 1-52 to comply with E.O. 13526.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: NSA/CSS Policy Manual 1-52 is in coordination.

(U) Proposed Target Completion date: 30 September 2013.

(U) Finding One: (U) Information Security Program Management
(U) Recommendation 2 (DJ2): (U) Notify the Information owners, CAOs, and OCAs of the need to update outdated classification guides in compliance with E.O. 13526.

(U) Management's Response: CONCUR with comment.

(U) NSA/CSS Policy 1-52 identifies the roles and responsibilities for classifying, safeguarding, and declassifying NSA/CSS classified national security information. The current policy reflects a collaborative process whereby Original Classification Authorities are to "validate the information in, update, or cancel the classification and declassification guides under their purview at least once every 5 years or when directed as part of a fundamental classification guide review to ensure that guides are current and accurate" and the Associate Director for Policy and Records shall "manage the development of and maintain classification and declassification guides and…publish guides as necessary."

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Planned Corrective Action: As DJ currently identifies outdated classification guides (older than 5 years) in the NSA Annual Security Classification Management Program Data Report (SF-311) response, DJ2 will notify information owners on an annual basis when formal guidance approaches the 5 year mark.

(U) Proposed Target Completion date: No later than October of each year.

(U) Finding One: (U) Information Security Program Management
(U) Recommendation 3 (DJ2): (U) Revise the requirements for the Agency's Classification Tools to include the following elements:

a. (U) Personal identifier of person who applied derivative classification markings;
b. (U) Source document or the classification guide (drop down menu listing of Agency guides); and
c. (U) Declassification information carried forward from the source document or guide.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: E.O. 13526 and 32 CFR Part 2001 requirements for the identification of persons who apply derivative classification markings by name and position or personal identifier, source documents used to derive classification markings ("go classguides"), and date or event of declassification will be implemented through NSA/CSS Policy Manual 1-52. The revision of NSA/CSS Manual 1-52 as the NSA Classification Guide as well as satisfaction of recommendations 4 and 5 will realize the intent of recommendation 3.

(U) Proposed Target Completion date: 30 September 2013.

(U) Finding One: (U) Information Security Program Management
(U) Recommendation 7 (DJ): (U) Update NSA/CSS Policy Manual 1-52 to declare that individuals who engage in the classification challenge process may not be subject to retribution.

(U) Management's Response: CONCUR

(U) Corrective Action Completed: NSA/CSS Policy Memorandum 2013-02. *Classification Challenges – Amendment to Policy Manual 1-52*, was issued to document that no punitive action will be taken against an authorized holder who, in good faith, makes a classification challenge.

(U) Completed date: NSA/CSS Policy Memorandum 2013-02 was issued on 3 May 2013.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Finding One: (U) Information Security Program Management
(U) Recommendation 8 (DJ): (U) Publicize the Agency's classification challenge process.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: NSA/CSS Policy Memorandum 2013-02 will be incorporated into NSA/CSS Policy Manual 1-52 by the expiration date of 3 May 2014. An Agency-all message will be promulgated to the NSA/CSS workforce upon the issuance of NSA/CSS Policy Manual 1-52, and a tailored message will be sent to the CAO population using the Electronic Subscription Service messaging system.

(U) Proposed Target Completion date: 30 September 2013.

(U) Finding Two: (U) Original Classification
(U//~~FOUO~~) Recommendation 9 (DJ2): (U//~~FOUO~~) Coordinate with ODNI to ensure that the Finance Classification Guide (7-1) and the ODNI Classification Guide agree.

(U) Management's Response: CONCUR

(U//~~FOUO~~) Corrective Action Completed: Information Security Policy (DJ2), Resources Management Policy and Budget Structure Management (BFP), and ODNI IC CIO/Information and Data Management office personnel completed coordination on the revised Director of Finance Classification Guide (7-1) on 8 May 2013 to ensure there was no conflict between ODNI classification guidance and NSA/CSS-specific classification guidance.

(U) Completed date: NSA/CSS Classification Guide for the Directorate of Resources Management (7-1) was signed by the OCA on 21 May 2013.

(U) Finding Two: (U) Original Classification
(U) Recommendation 10 (DJ): (U//~~FOUO~~) Coordinate with ODNI and DoJ to develop a classification guide that adequately addresses FAA Section 702.

(U) Management's Response: CONCUR

(U//~~FOUO~~) Planned Corrective Action: NSA has submitted for DNI approval a list of 702-related facts that we believe have been declassified in recent weeks. The package going to the DNI requires agencies, upon DNI approval, to update their classification guides accordingly. A proposed revision to the NSA FISA guide will require prior approval by ODNI and DoJ.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) Proposed Target Completion date: NSA will have the FISA guide updated by 31 December 2014.

(U) Finding Three: (U) Derivative Classification
(U) Recommendation 11 (DJ): (U//~~FOUO~~) Comply with CAPCO guidance to eliminate the use of retired code words or obtain a waiver for non-compliant software applications.

(U) Management's Response: NON-CONCUR

(U) Reason for Disagreement (if management disagrees): The action to prepare the initial draft for a waiver or eliminate the use of retired code words resides with SID (Information Sharing Services Group (S1S)), as it is outside the control of the Office of Policy and Records. As documented in Section 8 of USSID CR1400, issued 29 December 2005 and revised 29 September 2011, the code words are still used in traditional text reports sent via CRITICOMM due to software limitations.

(U) Finding Three: (U) Derivative Classification
(U) Recommendation 12 (DJ): (U//~~FOUO~~) Publicize the lines of authority for classification reviews on the DJ and DJ2 web sites to make users aware of the responsible organizations.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: The Office of Policy and Records will publicize the specific classification advisory officer (CAO) functions performed on behalf of agency personnel by DJ and DJ2.

(U) Proposed Target Completion date: 30 September 2013.

(U) Finding Four: (U) Information Security Self-Inspection Program
(U) Recommendation 13 (DJ2): (U) Update NSA/CSS Policy Manual 1-52 to include the essential elements for self-inspections in accordance with EO 13526 and 32 CFR Part 2001.

(U) Management's Response: CONCUR with comments

(U) The NSA/CSS Annual Self-Inspection Program Report for FY 2012 was submitted to the Office of the Under Secretary of Defense for Intelligence as directed, with a cover letter signed by the NSA Senior Agency Official and the inclusion of the NSA Information Security Self-Inspection Program Standard Operating Procedures. The OUSD(I) provided a consolidated DoD report to ISOO that did not include the NSA cover letter and NSA SOP information. The NSA Annual Self-Inspection Program Report for FY 2012 was fully compliant with ISOO requirements when provided to OUSD(I).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Planned Corrective Action: Essential elements for self-inspections will be added to the draft NSA/CSS Policy Manual 1-52.

(U) Proposed Target Completion date: 30 September 2013.

(U) Finding Four: (U) Information Security Self-Inspection Program
(U) Recommendation 14 (DJ2): (U) Include a review of classification levels in the NSA/CSS Information Security Self-Inspection Program.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: The Information Security Policy Self-Inspection Standard Operating Procedures and related software templates were updated as of 4 June 2013 to require DJ2 review of submitted material for appropriate use of classification. The self-inspection assessment will indicate instances of over-classification and provide recommendation(s) for corrective action.

(U) Proposed Target Completion date: The changes in the NSA Information Security Self-Inspection Program to review classification levels will be implemented with the next scheduled self-inspection (BM1 organization), projected to commence between the August to October 2013 timeframe.

(U) Finding Five: (U) Information Security Education and Training
(U) Recommendation 15 (DJ2 with ADET): (U) Update CLAS-1000 to include additional coverage on proper classifications and on identifying classification guides and using them to derive appropriate classification control markings.

(U) Management's Response: CONCUR

(U) Planned Corrective Action: ADET has accepted a New Learning Solution (NLS 1122) request to update and revise CLAS-1000, with all modules undergoing update and/or revision as appropriate.

(U) Proposed Target Completion date: 27 September 2013.

(U) Finding Five: (U) Information Security Education and Training
(U) Recommendation 17 (DJ): (U) Document and implement measures to enforce compliance with the mandatory classification training.

(U) Management's Response: NON-CONCUR with comment.

(U) In the ISOO Annual Report to the President for 2012, statistics were provided on executive branch Agency and Department satisfaction of the security education and training requirements of E.O. 13526. NSA information security and education training

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//FOR OFFICIAL USE ONLY

completion rates are as good as or better than those reported by ISOO for the executive branch:

(U)

Training	ISOO Findings	NSA Compliance	Comments
OCA Training	81.2 % (ISOO) 47.4% (all)	100%	NSA OCA training was not identified in the audit as an area for improvement.
Derivative Classifier Training	87% (ISOO) 47.1% (all)	81.9% (CIV/FY12) 36.9% (MIL/FY12)	

(U)

(U) Reason for Disagreement (if management disagrees): The Office of Policy and Records has no enforcement authority. The Associate Director of Policy and Records as Senior Agency Official does have the authority to document and implement methods to improve compliance with mandatory training, to include: a focus on CLAS-1000 completion rates during an organizational self-inspection assessment; greater management accountability through the Annual Contribution Evaluation plan commensurate with the IC element change effective August 2013; consideration of policy language.

(U//~~FOUO~~) If you have further questions or require additional information on the DJ response to this working draft report, please contact [redacted]

(b)(3)-P.L. 86-36

David J. Sherman

DAVID J. SHERMAN
Associate Director for Policy and Records

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) ASSOCIATE DIRECTORATE OF HUMAN RESOURCES RESPONSE

UNCLASSIFIED

Office of the Associate Directorate of Human Resources
National Security Agency

TO: [redacted]
Office of the Inspector General-Audits

(b) (3)-P.L. 86-36

FROM: [redacted] Chief HR Customer Gateway

SUBJECT: Draft Report of the Audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act" (AU-13-0005)

(U) The Office of Human Resources Customer Gateway appreciates the opportunity to respond to Inspector General Draft Report entitled, Draft Report of the Audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act" (AU-13-0005)

(U) MD concurs with Recommendation 6, Update NSA personnel performance objectives to include the designation and management of classified information as a critical performance element. (ACTION: Management Gateway (MD2))

(U) MD incorporated compliance with EO13526 into the Annual Contribution Evaluation Performance Element 6 for both the Supervisory and Non Supervisory templates. The changes became effective 8 April 2013, therefore, all documents created after 8 April 2013 will contain the updated language for Element 6.

(U) Non-Supervisory Element 6 - Technical Expertise - [redacted]

[redacted]

(U) Supervisory Element 6 – Management Proficiency - [redacted]

[redacted]

(b) (3)-P.L. 86-36

[redacted]

[redacted]

Chief of Staff
Associate Directorate Human Resources

Chief, HR Customer Gateway

(b) (3)-P.L. 86-36
(b) (6)

UNCLASSIFIED

(U) ASSOCIATE DIRECTORATE FOR EDUCATION AND TRAINING RESPONSE

Number of Recommendation	15
Text of Recommendation	(U//~~FOUO~~) Update CLAS1000 to include additional coverage on proper classifications and on identifying classification guides and using them to derive appropriate classification control markings.
Action Element	DJ2 with ADET
ADET Response	(U//~~FOUO~~) DJ2 is the Office of Primary Interest (OPI) for implementing the Executive Orders and associated policies relating to NSA's Classification System. They are also responsible for initiating New Learning Solutions for start-up and/or updating existing courses related to NSA's classification policies. ADET/E9 would work to enable new courses, or incorporate changes as a result of an approved NLS.
Recommended Completion Date	(U//~~FOUO~~) ADET defers to the completion date as proposed by DJ2 as ADET will assist as appropriate in the updating of CLAS1000 within existing ADET frameworks.
ADET POC for Response	[redacted] ADET/E91, [redacted]

Number of Recommendation	16
Text of Recommendation	(U//~~FOUO~~) a. Develop measures to identify Agency personnel who are not compliant with the mandatory classification training. (U//~~FOUO~~) b. Provide list of non-compliant personnel to DJ2.
Action Element	ADET
ADET Response	(U//~~FOUO~~) a. ADET's Database of Record, ELM, does send automated reminder notifications to all personnel that have not completed mandatory training, on a set schedule (monthly). Each NSA manager has access to the Completion/Compliance reports for employees assigned to them in HRMS. (U//~~FOUO~~) b. There are several completion/compliance reports that all ELM Administrators, Group Training Authorities and Curriculum Managers have access to pull, which will display the status of the employees mandatory training completion and date. Upon a request from DJ2, as to when DJ2 would like the list of noncompliant employees, the ELM Administrators can arrange for the listing to be provided.
Recommended Completion Date (16.a.)	(U) Complete.
Recommended Completion Date (16.b.)	(U//~~FOUO~~) ADET's portion of the action is complete. DJ2 will need to notify ADET of the date or dates that they need the information (list of noncompliant employees).
ADET POC for Response	[redacted] ADET/E91, [redacted]

(b) (3)-P.L. 86-36

(U) TECHNOLOGY DIRECTORATE RESPONSE

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
Security Classification

NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE MEMORANDUM

DATE: 20130725

REPLY TO ATTN OF: DIRECTOR, Technology Directorate

SUBJECT: (U) Draft Report on the Audit of NSA's Compliance with Public Law 111-258, the "Reducing Over-Classification Act" (AU-13-0005)

TO: Office of the Inspector General

(U//~~FOUO~~) The Technology Directorate (TD) appreciates the opportunity to review the subject draft audit. In the draft report, the Office of the Inspector General (OIG) outlines several recommendations. Below are the TD responses for recommendations 4 and 5:

(U//~~FOUO~~) IG Recommendation 4: Implement the Agency's classification tool revisions for Microsoft Office applications.

(U//~~FOUO~~) TD Management Response: Concur. The Microsoft tools currently supported by TD and used across the Agency, invoke the Classify tool [redacted] which currently functions properly and needs no modifications. The tool provides the mechanism to classify a document according to the user's needs. The author of a document is ultimately responsible for ensuring the classification is correct. POC for Recommendation 4 is [redacted] T3, Classify Tool Government Team Lead.

(U//~~FOUO~~) IG Recommendation 5:

(U//~~FOUO~~) 5.a: [redacted]

(U//~~FOUO~~) 5.b. Ensure that all identified embedded classification tools are updated to comply with E.O. 13526 and NSA/CSS Policy Manual 1-52.

(U//~~FOUO~~) TD Management Response: Concur. TD does not agree that the recommendation should specify an "Agency-wide data call." TD offers the following to replace the current recommendation:

(U//~~FOUO~~) Determine the universe of embedded classification tools used in Agency databases and systems. Ensure that all identified embedded classification tools are updated to comply with E.O. 13526 and NSA/CSS Policy Manual 1-52. POC for recommendation 5 is [redacted] T1.

(b) (3) -P.L. 86-36

(U) Thank you for the opportunity to review and comment on the subject draft audit report. If you have further questions or require additional information on this response to the draft report, please contact the POC's listed above.

FORM A6796A JUN 2000 *(Supersedes Optional Form (OF) 10 which was cancelled by GSA 10/99)*

Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
Security Classification

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
Security Classification

(b)(3)-P.L. 86-36
(b)(6)

LONNY A. ANDERSON
Director, Technology Directorate

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
Security Classification