

Department of Health and Human Services

**OFFICE OF
INSPECTOR GENERAL**

**HHS ADOPTED, ADMINISTERED,
AND GENERALLY FOLLOWED
CLASSIFIED INFORMATION
POLICIES**



Daniel R. Levinson
Inspector General

May 2013
OEI-07-12-00400

EXECUTIVE SUMMARY: HHS ADOPTED, ADMINISTERED, AND GENERALLY FOLLOWED CLASSIFIED INFORMATION POLICIES OEI-07-12-00400

WHY WE DID THIS STUDY

The Reducing Over-Classification Act of 2010 mandates that the Inspector General of each agency of the United States with an officer or employee who is authorized to make original classification decisions conduct two evaluations. One evaluation is intended to (1) assess whether applicable classification policies have been adopted, effectively administered, and followed; and (2) identify practices that may contribute to misclassification of material. This evaluation must be completed by September 30, 2013. A second evaluation must be completed by September 30, 2016, and must review progress made pursuant to the results of the first. This report pertains to the first required evaluation and assesses whether the Department of Health and Human Services (HHS) has adopted, effectively administered, and followed policies regarding classified national security information (NSI). The second objective is addressed in the report entitled *Originally and Derivatively Classified Documents Met Most Federal Requirements* (OEI-07-12-00401).

HOW WE DID THIS STUDY

We identified and reviewed all of HHS's classified NSI guidance documents to determine their scope and content. We compared HHS's *National Security Information Handbook (Handbook)* to an Executive Order and its implementing Directive to determine whether it was consistent with Federal requirements. We interviewed officials responsible for ensuring that HHS's classified NSI policies are effectively administered and followed. Finally, we surveyed Classification Security Officers responsible for providing guidance and oversight to their operating or staff divisions.

WHAT WE FOUND

HHS has adopted policies for classified NSI that are consistent with Federal requirements. HHS used annual status reports and self-inspections to ensure that its classified NSI policies are effectively administered. Finally, HHS provided guidance and training to individuals who access classified NSI to ensure that classified NSI policies are followed; however, not all Classification Security Officers received guidance or training.

WHAT WE RECOMMEND

We recommend that the Office of Security and Strategic Information (OSSI), working on behalf of the Office of the Secretary, clarify who is responsible for ensuring that Classification Security Officers receive training and ensure that all Classification Security Officers receive guidance and training regarding classified NSI. OSSI concurred with both recommendations and described actions taken to address them.

TABLE OF CONTENTS

Objective	1
Background	1
Methodology	4
Findings.....	6
HHS has adopted policies for classified NSI that are consistent with Federal requirements.....	6
HHS used annual status reports and self-inspections to ensure that its classified NSI policies are effectively administered	7
HHS provided guidance and training to individuals who access classified NSI to ensure that its classified NSI policies are followed; however, not all Classification Security Officers received guidance and/or training	8
Conclusion and Recommendation	11
Agency Comments and Office of Inspector General Response.....	12
Appendix.....	13
A: Definition of Each Classification Level.....	13
B: Agency Comments	14
Acknowledgments.....	16

OBJECTIVE

To assess the extent to which the Department of Health and Human Services (HHS) has adopted, effectively administered, and followed applicable policies, procedures, rules, and regulations regarding classified national security information (NSI).

BACKGROUND

Classified NSI is information that requires protection against unauthorized disclosure and is marked to indicate its classified status.¹ The Reducing Over-Classification Act of 2010 (the Act) mandates that the Inspector General of each agency of the United States with an officer or employee who is authorized to make original classification decisions conduct two evaluations. One evaluation is intended to (1) assess whether applicable classification policies, procedures, rules, and regulations (policies) have been adopted, effectively administered, and followed; and (2) identify policies, procedures, rules, and regulations, or management practices (practices) that may contribute to misclassification of material.² This evaluation must be completed by September 30, 2013. A second evaluation must be completed by September 30, 2016, and must review progress made pursuant to the results of the first evaluation. This report assesses whether policies have been adopted, effectively administered, and followed. A companion report, entitled *Originally and Derivatively Classified Documents Met Most Federal Requirements* (OEI-07-12-00401), identifies practices that may contribute to misclassification of information. Both reports are being published concurrently.

In addition, the Information Security Oversight Office (ISOO) of the National Archives and Records Administration requested that Inspectors General review their agencies' classified documents to determine whether the information within them was classified in accordance with Federal requirements.³ For information regarding ISOO's request, see *Originally and Derivatively Classified Documents Met Most Federal Requirements* (OEI-07-12-00401).

Federal Requirements

Executive Order No. 13526, its implementing Directive,⁴ and the Act have all directed Federal agencies to reduce unnecessary information classification or information classification at a higher and more restrictive level than necessary.

¹ Executive Order No. 13526, published at 75 Fed. Reg. 707 (Jan. 5, 2010).

² P.L. 111-258, § 6.

³ ISOO is responsible to the President for policy and oversight of the Governmentwide security classification system and the National Industrial Security Program. ISOO receives policy and program guidance from the National Security Council.

⁴ 32 CFR pt. 2001.

These initiatives are intended to promote information sharing across agencies; with State, local, and tribal governments; and with the public.⁵

Executive Order No. 13526. In 2009, the President issued Executive Order No. 13526, entitled *Classified National Security Information*.⁶ This Executive Order sets forth a uniform system for classifying, safeguarding, and declassifying NSI and outlines the method of implementation.

Implementing Directive: *Classified National Security Information*. Pursuant to Executive Order No. 13526, ISOO issued a Directive^{7, 8} to provide guidance to agencies regarding the classification system set forth in the order, including guidance on:

- original classification,⁹
- derivative classification,¹⁰
- declassification and downgrading,¹¹
- the safeguarding of classified NSI,
- standards for establishing and maintaining an ongoing agency self-inspection program, and
- standards for agency security education and training programs.¹²

Agency Self-Inspections. Each agency must establish and maintain ongoing self-inspection programs that include reviews of representative samples of the agency's original and derivative classification actions.^{13, 14} The self-inspections should determine whether the agency has adhered to the requirements for original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight of the

⁵ S. Rept. No. 111-200, at 1-2 (2010).

⁶ Executive Order No. 13526, published at 75 Fed. Reg. 707 (Jan. 5, 2010).

⁷ The Executive Order requires ISOO to issue directives as necessary to implement the uniform system for classifying, safeguarding, and declassifying NSI.

⁸ 32 CFR pt. 2001, published at 75 Fed. Reg. 37254 (June 28, 2010).

⁹ "Original classification" is defined as an initial determination, in the interest of national security, that information requires protection from unauthorized disclosure. Executive Order No. 13526 § 6.1(ff).

¹⁰ "Derivative classification" is defined as incorporating, paraphrasing, restating, or generating information that is already classified and marking the material consistent with the classifications that apply to the original information. Individuals who apply derivative classification markings need not have original classification authority, but must indicate their identity in a manner that is immediately apparent for each derivative classification action. Executive Order No. 13526 § 6.1(o).

¹¹ When information no longer meets the standards for classification, it must be declassified or downgraded by the official who authorized the original classification, the original classifier's current successor, a supervisory official, or an official delegated declassification authority. Executive Order No. 13526 § 3.1.

¹² 75 Fed. Reg. 37254-37275 (June 28, 2010).

¹³ The ongoing agency self-inspections are separate from the mandated evaluations required to be conducted by Inspectors General.

¹⁴ 32 CFR § 2001.60; Executive Order No. 13526 § 5.4.

Executive Order and the Directive.¹⁵ Each year, the agency must report the findings of its self-inspection program to the Director of ISOO.¹⁶

Agency Security Education and Training. Each agency must establish security education and training programs that ensure that all employees who create, process, or handle classified information understand the classification, safeguarding, and declassification policies and procedures.¹⁷ These employees include Classification Security Officers and other individuals who have access to classified NSI and the appropriate security clearance. Although these employees need not have original classification authority, they may derivatively classify information.¹⁸ Guidance and training provided to these employees is intended to reduce instances of overclassification and ensure that practices regarding classification, safeguarding, and declassification are followed.

HHS's Classified NSI Program

On January 9, 2012, the Office of Security and Strategic Information (OSSI) released HHS's Classified National Security Information Policy. The purpose of the policy is to ensure that all HHS agencies are aware of and compliant with Federal requirements related to the sharing, handling, and safeguarding of classified NSI.¹⁹ This policy clarifies the responsibilities of HHS and division officials tasked with implementing HHS's NSI program as set forth in Executive Order No. 13526 and Federal regulations. Specifically, this policy indicates that the Secretary of HHS (Secretary) serves as the original classification authority (OCA)²⁰ for HHS and may classify documents up to the "Secret" classification level.^{21, 22} This policy also charges the OSSI director with developing departmentwide policy and managing and overseeing the classified NSI program.²³ In addition, the policy requires that each HHS operating division and staff division designate a Classification Security Officer. The Classification Security Officer is responsible for providing his or her division with guidance and oversight on the handling and safeguarding of classified NSI. The Classification Security Officer is also responsible for conducting an initial review of his or her division's classified documents and coordinating this review with OSSI.²⁴

¹⁵ 32 CFR § 2001.60(c).

¹⁶ 32 CFR § 2001.60(f).

¹⁷ 32 CFR Part 2001, Subpart G; Executive Order No. 13526 § 4.1(a).

¹⁸ Executive Order No. 13526 § 6.1(o).

¹⁹ *Ibid.*, p. 3.

²⁰ An OCA is an individual authorized in writing, by the President, the Vice President, agency heads (such as the Secretary), or other officials designated by the President, to classify information in the first instance. Executive Order No. 13526 § 6.1(gg).

²¹ OSSI, Classified National Security Information Policy, January 9, 2012.

²² Information may be classified at one of three levels: (1) "Top Secret," (2) "Secret," or (3) "Confidential." See Appendix A for a description of each classification level.

²³ OSSI, Classified National Security Information Policy, January 9, 2012.

²⁴ *Ibid.*, § 6.4.

HHS has implemented the requirements of Executive Order No. 13526 and its Directive in greater detail in its *National Security Handbook (Handbook)*, which was released on February 17, 2012. It provides procedural guidance to HHS employees and contractors who have access to classified NSI and describes responsibilities for the handling and safeguarding of NSI. The *Handbook* indicates that the Secretary has delegated to the Deputy Secretary, the Director of OSSI, and the Associate Director of OSSI the authority to originally classify and declassify information.

Related Reports

In 2011, the Environmental Protection Agency (EPA) Office of Inspector General (OIG) was the first to issue its mandated evaluation.²⁵ Although other OIGs are reportedly undertaking evaluations, they had not issued reports as of May 2013.

METHODOLOGY

We identified and reviewed all of HHS's classified NSI guidance documents to determine their scope and content, including HHS's policy and *Handbook*.²⁶ We compared the *Handbook* to Executive Order No. 13526 and the Directive to determine whether it was consistent with Federal requirements. We conducted structured interviews with OSSI officials responsible for ensuring that HHS's classified NSI policies are effectively administered and followed. We also surveyed Classification Security Officers responsible for providing guidance and oversight regarding classified NSI to their divisions.

We verified that OCAs and Classification Security Officers who have access to classified NSI and who derivatively classified information received the required guidance and training. However, we did not determine whether other individuals who have access to classified NSI and derivatively classify information received guidance and training.²⁷ We determined which methods (e.g., self-inspections, training) HHS uses to ensure that its classified NSI policies are effectively administered and followed. We did not assess the implementation of those methods.

Data Collection and Analysis

Identification of NSI Policies. We asked OSSI to provide all of HHS's classified NSI guidance, including the current policy and *Handbook*. Once we identified all of HHS's classified NSI guidance, we reviewed each document to determine its scope and content. Specifically, we reviewed the *Handbook* to ensure that

²⁵ EPA OIG, *EPA Should Prepare and Distribute Security Classification Guides*, Report No. 11-P-0722, September 2011.

²⁶ In this report we collectively refer to HHS's policy and *Handbook* as policies.

²⁷ We chose to limit our review to those individuals responsible for providing the Department and divisions with guidance and oversight on the handling and safeguarding of classified NSI. These individuals included the OCAs and the Classification Security Officers.

guidance regarding the following information was included: (1) original classification, (2) derivative classification, (3) declassification and downgrading, (4) safeguarding of classified NSI, (5) standards for establishing and maintaining an ongoing agency self-inspection program, and (6) standards for agency security education and training programs.

Interviews With OSSI Officials. We conducted structured interviews with the Director and Associate Director of OSSI to gather information about how OSSI ensures that HHS's adopted policies are effectively administered. Specifically, we asked about (1) administration of HHS's self-inspection program and (2) procedures for reviewing the Department's classification actions. Lastly, we asked about OSSI's processes and procedures for annually reporting the findings regarding the Department's self-inspection program to ISOO.

We also gathered information from these officials regarding how OSSI ensures that the Department's adopted policies are followed. Specifically, we asked questions regarding the (1) dissemination of classified NSI guidance to employees who create, process, or handle classified information; (2) identification of staff who are required to complete training; (3) training content; and (4) frequency with which the training is provided. After conducting the interviews, we analyzed the responses of each official. We compared the responses to identify patterns across the various interviews.

Interviews With Classification Security Officers. We requested from OSSI the names and contact information of all of the designated Classification Security Officers at the time of our review. OSSI provided a roster of 16 primary Classification Security Officers for each division required to have such an officer. We asked each to confirm his or her status as a Classification Security Officer and to complete a survey regarding guidance and training that the Classification Security Officer may have received and/or provided regarding classified information. We received and analyzed responses from all 16 Classification Security Officers and compared the responses to identify patterns across the various surveys.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

HHS has adopted policies for classified NSI that are consistent with Federal requirements

HHS has adopted policies regarding classified NSI and developed additional guidance related to specific division programs and interagency information sharing. HHS's policies regarding classified NSI follow Federal requirements outlined in Executive Order No. 13526 and its Directive. Certain HHS divisions have developed guidance that further defines policies regarding classified NSI for specific programs. HHS has also developed a draft policy on interagency information sharing across Federal agencies within the national security community.

Adopted policies follow Federal requirements

HHS has adopted a policy entitled Classified National Security Information Policy which references Federal requirements on classified NSI and outlines the purpose, applicability, and scope of the policy. It also defines the responsibilities of individuals charged with handling and safeguarding classified NSI. HHS has also issued the *Handbook*, which provides specific instructions for implementing Executive Order No. 13526 and its Directive. The *Handbook* contains guidance on the following topics, which were included in the Executive Order: (1) original classification, (2) derivative classification, (3) declassification and downgrading, (4) safeguarding of classified NSI, (5) standards for establishing and maintaining an ongoing agency self-inspection program, and (6) standards for agency security education and training programs. HHS's *Handbook* provides information that would assist an individual in completing each of these actions in accordance with Federal requirements.

Additional guidance has been developed for specific programs and interagency information sharing

According to HHS's policy, divisions should establish additional written procedures, when necessary, to implement the Department's classified NSI policy. As a result, certain divisions have established division-specific policies regarding classified NSI. For example, OSSI and the Food and Drug Administration (FDA) have developed a classification guide for FDA's Center for Food Safety and Applied Nutrition.²⁸ This guide outlines standard operating procedures regarding classified NSI. The Centers for Disease Control and Prevention (CDC) has also developed guidance regarding classified NSI. For example, CDC issued guidance

²⁸ FDA, Center for Food Safety and Applied Nutrition Standard Operating Procedures: National Security Classification of Vulnerability Assessments, April 2007.

to its staff specifically addressing classification and marking of classified NSI.²⁹ HHS has also developed a policy for interagency information sharing entitled HHS Policy for Engagement With the National Security Community via the Information Sharing Environment. This policy designates OSSI, “which reports directly to the Deputy Secretary on intelligence and counterintelligence issues, as the Department’s lead on sharing and safeguarding national security information.” The policy establishes the responsibilities of HHS employees, contractors, and divisions related to sharing and safeguarding homeland security information, terrorism-related information, law enforcement information related to terrorism, or intelligence-related information.³⁰

HHS used annual status reports and self-inspections to ensure that its classified NSI policies are effectively administered

HHS has adopted methods to ensure that its classified NSI policies are effectively administered through various methods. For example, Classification Security Officers are required to complete annual status reports that document how their divisions handle and safeguard classified NSI.³¹ OSSI officials also conduct periodic self-inspections to determine whether derivatively classified documents were classified in accordance with Federal requirements. Finally, the findings from the Classification Security Officers’ annual status reports and OSSI’s self-inspections are used to complete required reporting forms and develop HHS’s annual self-inspection report, which is provided to the Director of ISOO.

Classification Security Officers completed required annual status reports

To ensure that HHS’s policies related to classified NSI are effectively administered, OSSI officials reported that each Classification Security Officer completed the required *Annual Status Report on Classified Information* (annual status report).³² The report is a self-assessment tool that Classification Security Officers complete to report how classified documents are being handled and safeguarded throughout HHS. The annual status report requires Classification Security Officers to provide specific information about their divisions’

²⁹ CDC, National Security Information Classification & Control Markings, 2012; CDC, Document Marking Briefing, 2012.

³⁰ OSSI, Policy for Engagement With the National Security Community via the Information Sharing Environment (ISE), November 29, 2012.

³¹ Classification Security Officers are required to conduct security inspections of all offices in their divisions that store or handle classified information to ensure that individuals responsible for classified information comply with classified NSI policies. Further, these officers are required to audit their divisions’ classified documents. The results of the security inspections and the audits are reported on the HHS “Annual Status Report on Classified Information” forms, also referred to as “annual status reports.”

³² Classification Security Officers serving in divisions that did not develop and/or maintain classified NSI did not complete the annual status report.

classification management programs. This information includes the location, number, and classification level of the classified documents; and the number of derivative classification decisions. OSSI officials reported that they use these annual status reports to determine which divisions may need additional training.

OSSI conducted annual self-inspections

OSSI officials also reported that they conducted annual self-inspections to ensure that HHS's classified NSI policies were effectively administered. The self-inspections included reviewing a sample of derivatively classified documents and conducting informal site visits to determine whether documents are classified in accordance with Executive Order No. 13526. One OCA stated that, during a self-inspection, she would "review the [derivative] classification decision with the individual making the classification and talk about any issues." OSSI officials reported that they conducted periodic informal site visits to the divisions to ensure that classified documents were being handled and safeguarded in accordance with HHS policy and Federal requirements.

Findings from the Classification Security Officers' annual status reports and the self-inspections were reported to ISOO

HHS's self-inspection report included descriptions of the Department's self-inspection program and findings, which included information from the Classification Security Officers' annual status reports. HHS's self-inspection report addressed all topics required by Executive Order No. 13526 (original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight). OSSI officials reported that they are required to complete both the "Agency Security Classification Management Program Data" form, also referred to as "Standard Form 311," and the self-inspection report annually and submit them to the Director of ISOO by November. The Associate Director of OSSI provided copies of both Standard Form 311 and the self-inspection report for 2011; both of these documents were submitted to ISOO by the November 2011 deadline.

HHS provided guidance and training to individuals who access classified NSI to ensure that its classified NSI policies are followed; however, not all Classification Security Officers received guidance and/or training

HHS adopted various methods to ensure that its policies regarding classified NSI are followed. For example, guidance and training regarding HHS's classified NSI policy and *Handbook* are disseminated to individuals who develop and access classified information. These individuals include the four OCAs (the Secretary, Deputy Secretary, Director of OSSI, and Associate Director of OSSI), Classification Security Officers, and individuals who possess security clearances.

Guidance regarding HHS's policy and Handbook was reportedly disseminated to administrative leads, Classification Security Officers, and other individuals who access classified NSI; however, not all Classification Security Officers received guidance

To ensure that HHS's policies related to classified NSI are followed, OSSI officials reported that they disseminated guidance to lead administrators, OCAs, Classification Security Officers, and other individuals who access classified NSI. OSSI officials reported that HHS's Classified National Security Information Policy was disseminated directly to the lead administrators of the divisions. OSSI officials reported that the *Handbook* was also disseminated directly to the Classification Security Officers, who are responsible for ensuring that their divisions adhere to policies for handling classified NSI. OSSI officials further reported that the classified NSI policy and *Handbook* were disseminated to the four OCAs.³³ Policies related to classified NSI and the *Handbook* are updated each time a relevant Executive Order is issued.

Of the 16 Classification Security Officers surveyed, 13 indicated that they had received guidance regarding HHS's policies for handling and classifying information since becoming Classification Security Officers. Four specifically reported receiving HHS's *Handbook*. Of the nine Classification Security Officers who did not report receiving the *Handbook*, eight reported receiving HHS's policy or general guidance from OSSI concerning classified information; one reported receiving information but could not recall the content. Of the three Classification Security Officers who indicated that they did not receive guidance, two reported that their divisions did not develop or maintain classified information. The third reported that he had not received guidance since joining HHS in 2010. However, he reported receiving training related to classified NSI from his former Federal employer.

Training was reportedly provided to OCAs, Classification Security Officers, and other individuals who accessed classified NSI; however, not all Classification Security Officers received training

OSSI officials reported that HHS has established required training for individuals who develop and access classified NSI (OCAs, Classification Security Officers, and individuals with security clearances). The four OCAs are required to complete annual training on making original classification decisions. The OCAs are also required to complete annual refresher training. OSSI officials reported that all four OCAs had completed their annual training for 2012.

OSSI officials indicated that Classification Security Officers are also required to receive training. Of the 16 Classification Security Officers surveyed, 14 indicated that they had received some type of training since becoming Classification

³³ OSSI officials confirmed that all four OCAs received HHS's policy and *Handbook*.

Security Officers for their divisions. These 14 Classification Security Officers reported receiving training on a number of topics, including handling and safeguarding classified information, transmitting classified information, original classification, derivative classification, downgrading and declassification, marking of classified materials, and storage of classified information. The two who did not receive training reported that their divisions do not develop or maintain classified information.

In addition to OCAs and Classification Security Officers, other individuals with access to classified NSI are required to receive training. OSSI officials reported that these individuals received training on topics such as handling, safeguarding, identifying, and marking classified NSI.

CONCLUSION AND RECOMMENDATION

As mandated by the Reducing Over-Classification Act, we assessed whether HHS has adopted, followed, and effectively administered policies regarding classified NSI. HHS's policies for classified NSI are consistent with Federal requirements outlined in Executive Order No. 13526 and its implementing Directive. Some HHS divisions have established additional procedures to implement the Department's classified NSI policy, such as FDA's classification guide for the Center for Food Safety and Applied Nutrition, CDC's guidance on classification and marking of classified NSI, and a draft policy on interagency information sharing across Federal agencies. Additionally, to ensure that its classified NSI policies are effectively administered, HHS requires annual status reports and self-inspections. HHS uses the findings from the annual status reports and self-inspections to provide ISOO with information regarding HHS's classified NSI program. Finally, HHS provides guidance and training to individuals who access classified NSI to ensure that its policies are followed. However, not all of the Classification Security Officers received the guidance or training.

We conclude that HHS has adopted policies regarding classified NSI and methods to ensure that the adopted policies are effectively administered and followed. However, the methods that HHS uses to ensure that Classification Security Officers receive appropriate guidance and training may not be effective. Therefore, we recommend OSSI, working on behalf of the Office of the Secretary:

Clarify Who Is Responsible for Ensuring That Classification Security Officers Receive Training

HHS's Classified National Security Information Policy does not specify who is responsible for ensuring that Classification Security Officers receive training. OSSI should revise this policy to clarify who is responsible for ensuring that designated Classification Security Officers receive training regarding the handling and safeguarding of classified information.

Ensure That All Classification Security Officers Receive Guidance and Training Regarding Classified NSI

OSSI should ensure that all Classification Security Officers are aware of their responsibility to provide their divisions with guidance and oversight on the handling and safeguarding of classified NSI. OSSI should also ensure that all Classification Security Officers receive guidance concerning HHS's classified NSI program, including HHS's *Handbook*.

Although some divisions may not develop or maintain classified information, their Classification Security Officers have access to and may receive classified information. Therefore, OSSI should ensure that all Classification Security Officers receive training concerning HHS's classified NSI program. Further, OSSI should inform HHS divisions that, regardless of whether the divisions

develop or maintain classified information, division heads and Classification Security Officers are responsible for ensuring that divisions follow HHS policies regarding classified NSI.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

OSSI concurred with both recommendations. In response to the first recommendation, OSSI indicated that it is revising the HHS *Handbook* to ensure that HHS division heads are aware of their responsibility to provide their divisions with guidance and oversight on the handling and safeguarding of classified NSI. OSSI also stated that it reissued the classified NSI policy and *Handbook* to all Classification Security Officers in mid-December 2012, to ensure that they all had their own copies, regardless of whether their divisions develop or maintain classified information.

In response to the second recommendation, OSSI said that it communicated with all Classification Security Officers to ensure that they are properly trained and have received appropriate guidance. Further, OSSI stated that it would start providing semiannual training for all Classification Security Officers in the spring of 2013 to ensure that established standards are acknowledged and maintained.

We did not make any changes to the report based on OSSI's comments.

APPENDIX A

Definition of Each Classification Level

Information may be classified at one of three levels: “Top Secret,” “Secret,” and “Confidential.” Below is a definition of each classification level.

Top Secret is “applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.”³⁴

Secret is “applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.”³⁵

Confidential is “applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.”³⁶

³⁴ Executive Order No. 13526 § 1.2.

³⁵ Ibid.

³⁶ Ibid.

APPENDIX B

Agency Comments



DEPARTMENT OF HEALTH & HUMAN SERVICES
Office Security and Strategic Information

February 22, 2012

To: Daniel R. Levinson
Inspector General for Evaluation and Inspections
Department of Health & Human Services

From: Dr. Joy Miller */S/*
Deputy Assistant Secretary for Security
Office of Security and Strategic Information (OSSI)
Secretary's Senior Intelligence Official

Subject: OSSI Response to Draft Final OIG Reports, dated 29 January 2013.

References:

OIG Report OEI-07-12-00400 (Draft) HHS Adopted, Administered, and Generally Followed Classified Information Policies, (OEI-07-12-00400)

OIG Report OEI-07-12-00401 (Draft) Originality and Derivatively Classified Documents Met Most Federal Requirements, (OEI-07-12-00401)

1. **Purpose.** To provide responses to OIG recommendations as noted in the reference reports.
2. **Background.** The Reducing Over-Classification Act of 2010 mandated that the Inspector General for each federal government agency or department who have employees authorized to make original classification decisions conduct two evaluations. One evaluation is intended to assess whether applicable classification policies have been adopted, effectively administered, and followed; and the other to identify practices that may contribute to misclassification of material. These evaluations will be completed by 30 September, 2013. Then, a second evaluation, to be completed by 30 September, 2016 must review progress made pursuant to the results of the first evaluation. The HHS Special Security Officer (SSO) serves as lead for coordinating Department wide implementation of the HHS Classified National Security Information (NSI) Policy.
3. **OIG Report OEI-07-12-00400 (Draft).** This OIG report addressed the first required evaluation and assessed whether HHS had adopted, effectively administered, and followed policies regarding Classified NSI.
 - A. **OIG Recommendation.** Clarify who is responsible for ensuring that Classification Security Officers (CSO) receive training.
 - B. **OSSI Response.** Concur. OSSI is in the process of revising the HHS Classified National Security Information Handbook, dated 17 February 2012 to ensure OP/STAFF DIV CSOs are aware of their responsibility to provide their divisions with guidance and oversight on the handling and safeguarding of classified NSI. Additionally, OSSI reissued the Classified NSI Policy and Handbook to all OP/STAFF DIV CSOs in mid-December 2012, to ensure each had their own copy of the handbook, regardless of whether their divisions develop or maintain classified information.
 - C. **OIG Recommendation.** Ensure that all Classification Security Officers receive guidance and training regarding Classified National Security Information.

D. OSSI Response. Concur. The HHS SSO communicated with each OP/STAFF DIV CSO to ensure they are properly trained and have received appropriate guidance and documents regarding their collateral duty responsibilities. Additionally, beginning in the second quarter of CY13, the HHS SSO will conduct semiannual training with all CSOs, to ensure established standards are acknowledged and maintained.

4. OIG Report OEI-07-12-00401 (Draft). The Information Security Oversight Office (ISOO) requested that Inspectors General conduct reviews of their agencies' classified documents to determine whether the information within the documents was classified in accordance with Federal requirements. This OIG report addressed that request.

- A. OIG Recommendation. Ensure that Original Classification Officers (OCAs) and individuals who derivatively classify NSI receive guidance and training regarding the required portion markings.
- B. OSSI Response. Concur. All individuals who handle classified information have attended mandatory initial, and when appropriate, annual refresher training in marking Classified NSI. The DAS Security provided OCA training for the HHS Secretary and Deputy Secretary. The HHS SSO and Primary Alternate SSO conducted derivative marking training for OS personnel and the CSOs, the same for their respective OP/STAFF DIV personnel.
- C. OIG Recommendation. Take appropriate action to apply the required portion markings to reviewed classified documents.
- D. OSSI Response. Concur. The HHS SSO and the OSSI Associate Director for Strategic Information reviewed and corrected the errors found by the OIG auditor during his review of the originally and derivatively classified documents.

Attachments:

- HHS Adopted, Administered, and Generally Followed Classified Information Policies, (OEI-07-12-00400) (Draft)
- Originally and Derivatively Classified Documents Met Most Federal Requirements, (OEI-07-12-00401) (Draft)

Note: The Office of Security and Strategic Information did not include any editorial or technical comments in the attachments referenced in its response.

ACKNOWLEDGMENTS

This report was prepared under the direction of Brian T. Pattison, Regional Inspector General for Evaluation and Inspections in the Kansas City regional office, and Brian T. Whitley, Deputy Regional Inspector General.

Rae Hutchison served as the project leader for this study. Other Office of Evaluation and Inspections staff from the Kansas City regional office who conducted the study include Michael J. Brown and Jordan R. Clementi. Central office staff who provided support include Althea Hosein, Debra Roush, and Talisha Searcy.

Office of Inspector General

<http://oig.hhs.gov>

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.