Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ORIGINALLY AND DERIVATIVELY CLASSIFIED DOCUMENTS MET MOST FEDERAL REQUIREMENTS

Daniel R. Levinson
Inspector General

May 2013
OEI-07-12-00401

EXECUTIVE SUMMARY: ORIGINALLY AND DERIVATIVELY CLASSIFIED DOCUMENTS MET MOST FEDERAL REQUIREMENTS
OEI-07-12-00401

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 assess whether applicable classification policies have been adopted, followed, and effectively administered; identify practices that may contribute to misclassification of material; and review progress made pursuant to these assessments. In addition, the Information Security Oversight Office (ISOO) requested that Inspectors General review their agencies' classified documents to determine whether the information within them was classified in accordance with Federal requirements. This report addresses ISOO's request and identifies practices that may contribute to the misclassification of material.

HOW WE DID THIS STUDY

We reviewed all documents the Department of Health and Human Services (HHS) had originally classified as of August 2012 and a purposive sample of derivatively classified documents to determine whether the information within them was classified in accordance with Federal requirements.

WHAT WE FOUND

Of the 43 classified documents reviewed, 36 met all Federal requirements regarding classified National Security Information (NSI). Seven of the reviewed documents (four of the originally and three of the derivatively classified documents) lacked the required markings.

WHAT WE RECOMMEND

We recommend that the Office of Security and Strategic Information (OSSI), working on behalf of the Office of the Secretary, ensure that original classification authorities and individuals who derivatively classify NSI receive guidance and training pertaining to the required portion markings. We also recommend that OSSI take appropriate action to apply the required portion markings to reviewed classified documents. OSSI concurred with both recommendations and described actions to address them.

TABLE OF CONTENTS

OBJECTIVE

To assess the extent to which the Department of Health and Human Services (HHS) maintains classified information in accordance with applicable Federal requirements 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, 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.[3] The report entitled *HHS Has Adopted, Administered, and Generally Followed Classified Information Policies* (OEI-07-12-00400) assessed whether polices have been adopted, effectively administered, and followed. This report identifies practices that may contribute to misclassification of information.[4]

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.[5] This report also addresses ISOO's request.

Federal Requirements

Executive Order No. 13526, its implementing Directive,[6] 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. This initiative is intended to promote information sharing across agencies; with State, local, and tribal governments; and with the public.[7]

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

[2] P.L. 111-258, § 6.

[3] Ibid.

[4] Both reports are being published concurrently.

[5] 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.

[6] 32 CFR pt. 2001, promulgated at 75 Fed. Reg. 37254 (June 28, 2010).

[7] S. Rept. No. 111-200, at 1-2 (2010).

Executive Order No. 13526. In 2009, the President issued Executive Order No. 13526, entitled *Classified National Security Information*.[8] 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[9, 10] to provide guidance to agencies regarding the classification system set forth in the Order, including guidance on:

- original classification,
- derivative classification, and
- declassification and downgrading.[11, 12]

Original Classification

"Original classification'' is defined as an initial determination, in the interest of national security, that information requires protection from unauthorized disclosure.[13] The Directive provides guidance to agencies for the following:

- classification standards,
- classification levels,
- classification authority,
- classification categories,
- duration of classification,
- identification and markings,
- classification prohibitions and limitations, and
- classification challenges.

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

[9] Executive Order No. 13526 requires ISOO to issue directives as necessary to implement the uniform system for classifying, safeguarding, and declassifying NSI.

[10] 32 CFR pt. 2001, published at 75 Fed. Reg. 37254 (June 28, 2010).

[11] Ibid. at 37274–37275.

[12] The Directive also provides guidance regarding the (1) safeguarding of classified NSI, (2) standards for establishing and maintaining an ongoing agency self-inspection program, and (3) standards for agency security education and training programs.

[13] Executive Order No. 13526 § 6.1(ff).

Classification Standards. Information may be originally classified if all of the following conditions are met:

an original classification authority (OCA) (i.e., an individual authorized to classify information in the first instance) is classifying the information;[14]

- the information is owned by, produced by or for, or is under the control of the Federal Government;
- the information falls within one or more of the classification categories noted in Table 1; and
- the OCA determines that unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security.[15]

Classification Levels. If the information meets all of the conditions above, then the OCA must determine the level at which the information should be classified. Information may be classified at one of three levels: (1) "Top Secret," (2) "Secret," or (3) "Confidential."[16]

Classification Authority. The authority to originally classify information may be carried out by (1) the President and the Vice President, (2) agency heads and other officials designated by the President, and (3) Government officials delegated the authority to classify information.[17] Officials authorized to classify information at a specified classification level are also authorized to classify information at a lower level.[18]

Classification Categories. Information may be originally classified if, in addition to meeting the classification standards, it falls within one or more of the categories in Table 1.

[14] "Original classification authority" means 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).

[15] 32 CFR § 2001.10; Executive Order No. 13526 § 1.1(a).

[16] Executive Order No. 13526 § 1.2(a).

[17] Executive Order No. 13526 § 1.3(a). Agency heads are responsible for ensuring that subordinate officials delegated responsibility have a demonstrable and continuing need to carry out this original classification authority.

[18] Executive Order No. 13526 § 1.3(b).

Table 1: Codes and Categories for Classification

Code	Category
A	Military plans, weapons systems, or operations
B	Foreign government information
C	Intelligence activities (including covert action), intelligence sources or methods, or cryptology
D	Foreign relations or foreign activities of the United States, including confidential sources
E	Scientific, technological, or economic matters relating to the national security
F	U.S. Government programs for safeguarding nuclear materials or facilities
G	Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
H	Development, production, or use of weapons of mass destruction

Source: Executive Order No. 13526 § 1.4 and 32 CFR § 2001.21.

Duration of Classification. Mandatory automatic declassification[19] standards apply to all agencies that have original classification authority, previously had original classification authority, or maintain NSI.[20] At the time of original classification, the OCA must establish a date or event for declassification based on the duration of the national security sensitivity of the classified information. Upon reaching the stated date or event, the information must be declassified automatically.[21] See Appendix A for a summary regarding the determination of the duration of classification.

Identification and Markings. Standard markings or other indicia must be applied to classified information at the time of original classification.[22] The identification and markings must include (1) the name and position, or personal identifier, of the OCA; (2) the agency and office of origin; (3) the reason(s) for the classification; and (4) declassification instructions (e.g., the declassification date). The OCA must identify the reason(s) for the decision to classify as well as the corresponding code indicating the classification category as listed in Table 1. Markings must be uniformly and conspicuously applied so as to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification. The agency originating the classified document

[19] "Automatic declassification" means the declassification of information solely on the basis of the occurrence of a specific date or event as determined by the OCA, or the expiration of a maximum timeframe for duration of classification established under the Executive Order. Executive Order No. 13526 § 6.1(e).

[20] 32 CFR § 2001.30; Executive Order No. 13526 § 3.3.

[21] Executive Order No. 13526 § 1.5; 32 CFR § 2001.12.

[22] Executive Order No. 13526 § 1.6; 32 CFR § 2001.21.

must indicate which portions (e.g., paragraphs) of the document are classified.[23] Specifically:

> Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets and other portions within slide presentations, and the like, shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies.[24]

Classification Prohibitions and Limitations. Information may not be classified or continue to be maintained as classified for the purpose of:

- concealing violations of law, inefficiency, or administrative error;
- preventing embarrassment to a person, organization, or agency;
- restraining competition; or
- preventing or delaying the release of information that does not require protection in the interest of the national security.[25]

After information is declassified and properly released to the public, the information may not be reclassified unless certain exceptions are met.[26] Conversely, information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of Executive Order No. 13526.[27]

Classification Challenges. Authorized holders of information who, in good faith, believe that the information's classification status is improper are encouraged and expected to challenge the classification status in accordance with agency procedures. Agencies must establish procedures to ensure that (1) individuals are not subject to retribution for challenging classification status, (2) an opportunity is provided for review by an impartial official or panel, and (3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established under Executive Order No. 13526.[28]

---

[23] Executive Order No. 13526 § 1.6(5)(c).

[24] 32 CFR § 2001.21(c).

[25] Executive Order No. 13526 § 1.7.

[26] Executive Order No. 13526 § 1.7(c). When reclassifying information, the OCA must include the following: (1) level of classification; (2) identity, by name and position or by personal identifier, of the OCA; (3) declassification instructions; (4) a concise reason for classification, including reference to the applicable classification category; and (5) date the reclassification action was taken. 32 CFR § 2001.24(l).

[27] Executive Order No. 13526 § 1.7(d).

[28] Executive Order No. 13526 § 1.8; 32 CFR § 2001.14.

Derivative Classification

''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.[29] 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. Individuals who apply derivative classification markings must transfer the pertinent classification markings to any newly created documents.[30]

Declassification and Downgrading

OCAs must attempt to assign a date or event upon which classified information will be declassified. Generally, the duration is not to exceed 25 years, except when the information relates to a confidential informant or weapons of mass destruction.[31] See Appendix A for a summary regarding the determination of the duration of classification. 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 as a declassification authority.[32] Information that continues to meet the classification requirements requires continued protection. However, in exceptional cases in which agencies determine that the need to protect classified information is outweighed by the public interest in disclosure, the information should be declassified. Questions concerning these exceptional cases must be referred to the agency head or senior agency officials.[33]

Automatic Declassification. Regardless of whether they have been reviewed, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value must be automatically declassified.[34] Documents may be exempted from automatic declassification if the ultimate release of the information would clearly and demonstrably be expected to seriously impair national security at the end of the 25-year classification period.[35] See Appendix B for a summary regarding the exceptions to automatic declassification.

---

[29] Executive Order No. 13526 § 6.1(o).

[30] Executive Order No. 13526 § 2.1(b); 32 CFR § 2001.22.

[31] Executive Order No. 13526 § 1.5; 32 CFR § 2001.12(a).

[32] Executive Order No. 13526 § 3.1.

[33] Executive Order No. 13526 § 3.1(d).

[34] Executive Order No. 13526 § 3.3; see also 32 CFR § 2001.30, which states, "All departments and agencies that have original classification authority or previously had original classification authority, or maintain records determined to be permanently valuable that contain classified national security information, shall comply with the automatic declassification provisions of the Order."

[35] Executive Order No. 13526 § 3.3; 32 CFR § 2001.26.

HHS's Classified NSI Program

The Secretary of HHS (Secretary) serves as OCA for HHS and may classify documents up to the "Secret" classification level.[36, 37] The Secretary has delegated to the Deputy Secretary, the Director of HHS's Office of Security and Strategic Information (OSSI), and the Associate Director of OSSI the authority to originally classify and declassify information.[38, 39] The Director of OSSI is responsible for departmentwide policy development, management, and oversight of the classified NSI program.[40]

HHS's Maintenance of Classified Documents

Originally and derivatively classified documents may be either retained in hardcopy or stored electronically. HHS's electronic documents are accessed on either of two classified information technology (IT) systems owned by the Department of Homeland Security (DHS) or the Department of Defense (DOD). All originally classified documents are retained in hardcopy format. Although some derivatively classified documents are retained in hardcopy format (e.g., briefing slides, Daily Intelligence Readbook),[41] the majority are stored electronically on the IT systems owned by DHS or DOD.

METHODOLOGY

We reviewed all documents HHS had originally classified as of August 2012 and a purposive sample of derivatively classified documents to determine whether the information within them was classified in accordance with Federal requirements.

[36] Executive Order 13526 § 6.1(gg).

[37] See Appendix C for a description of each classification level.

[38] The Director of OSSI is also known as and has the official title of Deputy Assistant Secretary for Security within HHS and is the Senior Intelligence Officer.

[39] OSSI, *HHS National Security Handbook*, February 17, 2012.

[40] OSSI, *Classified National Security Information Policy*, January 9, 2012.

[41] OSSI officials indicated that HHS produces three types of derivatively classified documents; each type of document is stored differently. These three types are: (1) briefing slides, (2) Daily Intelligence Readbook documents (Readbook), and (3) emails. Briefing slides are generally produced for the Deputy Secretary of HHS and other HHS leadership; these documents may be maintained in hardcopy format. The Readbook is produced to brief OSSI leadership; these documents are maintained in hardcopy format. Derivatively classified emails are produced as responses to original classification decisions made by other Federal agencies. These emails are stored electronically on the IT systems owned by DHS and DOD.

Population and Sample Selection

At the time of our review, the population of classified documents included 13 originally classified documents[42] and approximately 700 derivatively classified documents. We reviewed all 13 originally classified documents and a purposive sample of 30 derivatively classified documents. See Table 2 for an illustration of the population and sample sizes.

Table 2: Originally and Derivatively Classified Documents

Document Type	Population	Sample Size
Originally Classified	13	13
Derivatively Classified	700	30
Total	**713**	**43**

Source: Office of Inspector General (OIG) analysis of HHS's originally and derivatively classified documents, 2012.

With the assistance of OSSI, we chose a purposive sample that would enable us to determine whether the information within these documents was classified in accordance with Federal requirements.[43] In selecting this sample, we did not intend to project the results of our review of derivatively classified documents. Rather, we intended for our review to provide a general representation of whether derivatively classified documents were classified in accordance with Federal requirements. The derivatively classified documents included 12 hardcopy documents (8 briefing slides and 4 Readbook documents) and 18 printed emails.[44] See Appendix D for a description of the sample selection.

Document Review

For each sampled document, we completed a structured review instrument to determine whether the classification of original and derivative information complied with Federal requirements.

Originally classified documents were determined to have been classified in accordance with Federal regulations if all of the requirements listed below were met:

[42] During preinspection discussions, OSSI indicated that there were 15 originally classified documents for review. Once we began our review, we learned that 2 of the 15 documents had been declassified in May 2011. As a result, only 13 of the originally classified documents were pertinent to our review.

[43] The majority of derivatively classified documents are stored on IT systems owned by DHS and DOD and cannot be accessed by individuals who have not been granted access by the owners of the systems. OSSI officials have access to these IT systems and assisted us in selecting the sample.

[44] OSSI officials selected 22 derivatively classified emails for review. Four of these emails were directly related to four Readbook documents selected for review. As a result, these four emails were combined with their respective Readbook documents to make a single derivatively classified document. Thus, the sample of derivatively classified documents consisted of 12 hardcopy documents and 18 printed emails.

- the decision to classify the information was exercised by an individual possessing original classification authority;
- the information was owned by, produced by or for, or under the control of the Federal Government;
- the information fell within one or more of the classification categories noted in Table 1;
- when asked, the OCA described damage to national security that could be expected in the event of the information's unauthorized disclosure;[45]
- the information was not prohibited or limited from receiving classification (e.g., the information was not classified to conceal violations of the law, inefficiency, or administrative error);
- the OCA established a specific date or event for declassification; and
- the following identification and markings were included: portion marking; overall classification; the name and position, or personal identifier, of the original classification authority; the agency and office of origin; the reason(s) for the classification; and declassification instructions (e.g., the declassification date).

Derivatively classified documents were determined to have been classified in accordance with Federal regulations if all of the requirements listed below were met:

- the information was related to the reproduction, extraction, or summation of information that was already classified;
- the person who applied the derivative classification was identified on the document by name and position or personal identifier;
- the information was marked consistently with the classification markings that apply to the original information (i.e., the derivative classification includes the pertinent classification markings that were included on the originally classified document);
- the information was owned by, produced by or for, or under the control of the Federal Government;
- the information fell within one or more of the classification categories noted in Table 1;

[45] OCAs are not required to provide in writing a description of the damage to national security that could be expected in the event of the information's unauthorized disclosure. To determine whether this requirement was met, we asked the OCA who classified the information to describe the damage to national security that could be expected in the event of the information's unauthorized disclosure.

- the information was not prohibited or limited from receiving classification (e.g., the information was not classified to conceal violations of the law, inefficiency, or administrative error); and
- the following identification and markings were included: portion marking; overall classification; the name and position, or personal identifier, of the person applying the derivative classification; and declassification instructions (e.g., the declassification date).

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.

FINDING

Most classified documents reviewed adhered to all Federal requirements regarding classified NSI; four originally classified documents and three derivatively classified documents failed to meet Federal requirements regarding portion markings

Of the 43 HHS classified documents reviewed, 36 met all Federal requirements regarding classified NSI (see Table 3).

Table 3: Classified Documents That Met Federal Requirements

Type	Sample Size	Number That Met All Federal Requirements
Originally Classified	13	9
Derivatively Classified	30	27
Total	**43**	**36**

Source: OIG analysis of HHS's classified documents, 2012.

OCAs must originally classify NSI in accordance with Federal requirements. Nine of the originally classified documents met all Federal requirements; however, four lacked portion markings on various pages and paragraphs. Specifically, two documents were missing the required paragraph markings, one was missing the required page markings, and one was missing both. Portion markings indicate which portions are classified and which are unclassified within the same document. These different portions are marked separately in order to avoid overclassification. See Table 4 for the number of originally classified documents that met each Federal requirement.

Table 4: Originally Classified Documents That Met Federal Requirements

Requirement	Documents (n=13)
Decision to classify the information was exercised by an OCA	13
Information was owned by, produced by or for, or under the control of the Federal Government	13
Information fell within one or more of the classification categories	13
The OCA described damage to national security that could be expected in the event of the information's unauthorized disclosure	13
Classification of the information was not prohibited or limited	13
The OCA established a specific date or event for declassification	13
Portion markings were present	9
Overall classification level was present	13
"Classified by" line was present	13
Reason for classification was present	13
"Declassify on" line was present	13
Total That Met All Requirements	**9**

Source: OIG analysis of originally classified documents, 2012.

Individuals who derivatively classify NSI must do so in accordance with Federal requirements. Twenty-seven of the thirty derivatively classified documents sampled for review met all of these requirements. Three derivatively classified documents lacked the required portion markings, but met all other Federal requirements. Specifically, all three documents were missing required paragraph markings. See Table 5 for the number of sampled derivatively classified documents that met the Federal requirements.

Table 5: Derivatively Classified Documents That Met Federal Requirements

Requirement	Documents (n=30)
Information was related to the reproduction, extraction, or summation of information that was already classified	30
Person who applied the derivative classification was identified on the document by name and position or personal identifier	30
Information was marked consistently with the classification markings that apply to the original information	30
Information was owned by, produced by or for, or under the control of the Federal Government	30
Information fell within one or more of the classification categories	30
Classification of the information was not prohibited or limited	30
Portion markings were present	27
Overall classification level was present	30
“Classified by” line was present	30
“Declassify on” line was present	30
Total That Met All Requirements	**27**

Source: OIG analysis of derivatively classified documents, 2012.

CONCLUSION AND RECOMMENDATIONS

Of the 43 HHS classified documents reviewed, 36 met all Federal requirements regarding classified NSI. Seven of the documents (four of the originally and three of the derivatively classified documents) lacked the required portion markings. Portion markings indicate which portions are classified and which are unclassified within the same document. These different portions are marked separately to avoid overclassification. Therefore, we recommend that OSSI, working on behalf of the Office of the Secretary:

Ensure That OCAs and Individuals Who Derivatively Classify NSI Receive Guidance and Training Regarding the Required Portion Markings

OSSI should ensure that OCAs and individuals who derivatively classify information are aware of their responsibility to include required portion markings on all classified documents. OSSI should also provide guidance and training on the required portion markings to avoid overclassification of information.

Take Appropriate Action To Apply the Required Portion Markings to Reviewed Classified Documents

We will provide information regarding the classified documents that did not include the required portion markings. OSSI should apply the required portion markings to these documents.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

OSSI concurred with both recommendations. In response to the first recommendation, OSSI stated that it ensures that all individuals who handle classified information have attended initial mandatory training and, when appropriate, annual refresher training in marking classified NSI. OSSI also stated that it ensures that OCA training is provided to the HHS Secretary and Deputy Secretary. Further, OSSI stated that it conducted derivative marking training for Classification Security Officers and personnel.

In response to the second recommendation, OSSI indicated that it would review and correct the errors found by OIG during its review of the originally and derivatively classified documents.

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

APPENDIX A

Determination of the Duration of Classification

Pursuant to Executive Order No. 13526, the Information Security Oversight Office (ISOO) issued a Directive.[46, 47] According to this Directive, the original classification authority (OCA) is required to attempt to determine a date or event that is less than 10 years from the date of original classification and that coincides with the lapse of the information's national security sensitivity and to assign such date or event as the declassification instruction. If the OCA is unable to determine a date less than 10 years after the original classification, he or she must assign a declassification date of exactly 10 years. If the OCA is unable to assign a 10-year declassification date, he or she must assign a declassification date not to exceed 25 years from the date of the original classification decision.[48]

Exceptions to this timeline apply to special categories of information, such as information that should clearly and demonstrably be expected to reveal the identity of a confidential source of intelligence or key design concepts of weapons of mass destruction. These special categories may be assigned a declassification date up to 75 years from the date of the original classification.[49]

[46] Executive Order No. 13526 requires ISOO to issue directives as necessary to implement the uniform system for classifying, safeguarding, and declassifying national security information.
[47] 32 CFR pt. 2001; 75 Fed. Reg. 37254 (June 28, 2010).
[48] 32 CFR § 2001.12(a)(1).
[49] 32 CFR § 2001.12(a)(2).

APPENDIX B

Exceptions to Automatic Declassification[50]

An agency head may exempt information from automatic declassification if the release of the information is clearly and demonstrably expected to:

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

[50] This information is taken directly from Executive Order No. 13526 § 3.3(b); 32 CFR § 2001.26.

APPENDIX C

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."[51]

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."[52]

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."[53]

[51] Executive Order No. 13526 § 1.2.
[52] Ibid.
[53] Ibid.

APPENDIX D

Sample Selection for Derivatively Classified Documents

The Office of Security and Strategic Information (OSSI) assisted us in selecting a purposive sample of 30 derivatively classified documents for review.[54] Below is a description of the process that OSSI used to select the purposive sample.

Hardcopy derivatively classified documents. According to the Associate Director for the Strategic Intelligence Division of OSSI, few derivatively classified documents are retained in hardcopy format. He indicated that the hardcopy documents chosen for review were not randomly selected. Rather, he made copies of the hardcopy derivatively classified documents that he possessed and provided them for our review. This resulted in a total of 12 hardcopy documents—8 briefing slides and 4 Readbook documents.

Electronic derivatively classified documents. The majority of derivatively classified documents were stored electronically as email responses to original classification decisions made by other Federal agencies. These emails were stored electronically on information technology (IT) systems owned by the Department of Homeland Security and the Department of Defense. Below is a description of OSSI's process for selecting the derivatively classified emails included in our review.

(1) The Associate Director for the Strategic Intelligence Division of OSSI numbered pieces of paper 1 through 30.

(2) Four OSSI employees were instructed to select five of the numbered pieces of paper each.

(3) The four employees were then instructed to access their "sent" folders in their email accounts and choose the emails that corresponded to the first number that they had randomly selected (e.g., if the number selected was 25, the employee scrolled down his/her "sent" folder to the 25th email).[55]

(4) The email was printed for review.

[54] OSSI officials indicated that HHS produces three types of derivatively classified documents; each type is stored differently. These three types are: (1) briefing slides, (2) Daily Intelligence Readbook documents (Readbook), and (3) emails. Briefing slides are generally produced for the Deputy Secretary of HHS and other HHS leadership; these documents may be maintained in hardcopy format. The Readbook is produced to brief OSSI leadership; these documents are maintained in hardcopy format. Derivatively classified emails are produced as responses to original classification decisions made by other Federal agencies. These emails are stored electronically on the IT systems owned by the Department of Homeland Security and the Department of Defense.

[55] If a selected number corresponded to an email that was unclassified, the employee was instructed to move to the next email in succession.

(5) Steps 3 and 4 were repeated until each of the four employees had selected 5 emails, for a total of 20.

Two additional emails were selected by the Associate Director for the Strategic Intelligence Division using the same process, resulting in a total of 22 derivatively classified emails selected for review. However, 4 of the 22 emails were directly related to four Readbook documents selected for review. As a result, these four emails were combined with their respective Readbook documents to create a single, derivatively classified document. Thus, the sample of derivatively classified documents consisted of 12 hardcopy documents and 18 printed emails. See Table D-1 for the types of derivatively classified documents included in our review and sample sizes.

Table D-1: Derivatively Classified Documents Selected for Review

Type of Document	Number of Documents Selected	Sample Size
Briefing slide	8	8
Readbook document	4	4
Email	22*	18
Total	**34**	**30**

*Four of the twenty-two emails were directly related to the four Readbook documents selected for review. These 4 emails were attached to the respective Readbook documents to make up a single derivatively classified Readbook document, resulting in 18 emails.

Source: Office of Inspector General analysis of derivatively classified documents, 2012.

APPENDIX E

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) Originally 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 polices 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.

1

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 Investigations staff who provided support include Asher Shapiro.

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.