AUDIT REPORT

Audit of NRC's Implementation of Federal Classified Information Laws and Policies

OIG-13-A-21-September 12, 2013

All publicly available OIG reports (including this report) are accessible through NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

September 12, 2013

MEMORANDUM TO: Mark A. Satorius
Executive Director for Operations

FROM: Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S IMPLEMENTATION OF FEDERAL CLASSIFIED INFORMATION LAWS AND POLICIES (OIG-13-A-21)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Implementation of Federal Classified Information Laws and Policies.*

The report presents the results of the subject audit. Following the September 3, 2013, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

EXECUTIVE SUMMARY

BACKGROUND

Legislative Basis for Audit

The Reducing Over-Classification Act[1] (the Act) states that over-classification of information interferes with information sharing, increases information security costs, and needlessly limits stakeholder and public access to information. Further, the Act asserts that over-classification negatively affects dissemination of information within the Federal Government; with State, local, and tribal entities; and with the private sector.[2] Lastly, the Act states that Federal agencies that perform classification are responsible for promoting compliance with applicable laws, executive orders, and other authorities pertaining to classification.

Classified Information Security at NRC

The U.S. Nuclear Regulatory Commission (NRC) must protect classified information related to Federal Government programs for securing nuclear materials and facilities. Classification is the process of identifying information that must be protected against unauthorized disclosure in the interest of national security.

NRC's Office of Nuclear Security and Incident Response has overall responsibility for the agency's information security program and develops policies and procedures for classified information security. Agency policy, which is based on higher-level Federal Government standards, is expressed in Management Directive 12.2, *NRC Classified Information Security Program*.

Classification may be performed only by personnel who have been delegated special authority and undergone required training. Specifically, Original Classifiers can make an initial determination, in the interest of national security, that information requires protection from unauthorized disclosure. In contrast, Derivative Classifiers may only restate or paraphrase information that has already been classified.

[1] Public Law 111-258/H.R. 553, "Reducing Over-Classification Act," October 7, 2010.

[2] Public Law 111-258, Section 2, "Findings."

Federal Classification Policies

On December 29, 2009, the President of the United States signed Executive Order 13526, "Classified National Security Information" (the Order), which establishes current principles, policies, and procedures for classification. The Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The Order also places equal emphasis on protecting information critical to national security while fostering Government transparency through accurate and accountable implementation of classified information management policies.

On June 25, 2010, the National Archives and Records Administration's Information Security Oversight Office issued a directive (the Directive) in the Code of Federal Regulations (CFR)[3] that included guidance to be used by Federal agencies in implementing the Order.

OBJECTIVES

In accordance with the Act's requirements, the audit objectives were to:

(a) Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component.

(b) Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

RESULTS IN BRIEF

Office of the Inspector General (OIG) auditors reviewed NRC policies and procedures for its classified information security program and developed five findings with corresponding recommendations to improve agency compliance with current Federal Government standards. Specifically, these findings address:

1. Original Classifier training.
2. Documentation of training certification.

[3] 32 CFR Parts 2001 and 2003.

3. Scope of self-inspections.
4. Staff position descriptions and performance evaluation criteria.
5. NRC policy guidance (Management Directive 12.2).

Auditors also reviewed a non-statistical sample of classified documents produced by NRC staff and found a limited number of marking errors but no evidence of systemic misclassification. Consequently, this report includes no findings or recommendations pertaining to misclassification.

RECOMMENDATIONS

This report makes recommendations to improve NRC's implementation of Federal classified information laws and policies.

AGENCY COMMENTS

An exit conference was held with the agency on September 3, 2013. Agency staff generally agreed with the report findings and recommendations, and provided technical comments on a draft version of the report. OIG has incorporated these comments, as appropriate, into the final version of the report.

ABBREVIATIONS AND ACRONYMS

C	Confidential
CFR	Code of Federal Regulations
E.O.	Executive Order
FY	Fiscal Year
ISSO	Information Security Oversight Office
MD	Management Directive
NARA	National Archives and Records Administration
NRC	Nuclear Regulatory Commission
NSI	National Security Information
NSIR	Office of Nuclear Security and Incident Response
OIG	Office of the Inspector General
P.L.	Public Law
RD	Restricted Data
S	Secret
TS	Top Secret

TABLE OF CONTENTS

I. BACKGROUND

Legislative Basis for Audit

The Reducing Over-Classification Act[4] (the Act) states that over-classification of information interferes with information sharing, increases information security costs, and needlessly limits stakeholder and public access to information. Further, the Act asserts that over-classification negatively affects dissemination of information within the Federal Government; with State, local, and tribal entities; and with the private sector.[5] Lastly, the Act states that Federal agencies that perform classification are responsible for promoting compliance with applicable laws, executive orders, and other authorities pertaining to classification.

Reflecting the Congress's concerns regarding over-classification in Federal agencies, the Act requires that Inspectors General perform at least two evaluations to determine whether their respective agencies have effectively implemented appropriate classification policies and procedures, and to identify policies, procedures, and management practices that may be contributing to persistent misclassification within these agencies.[6] The first evaluation is to be completed no later than September 30, 2013, and the second evaluation no later than September 30, 2016. The NRC Office of the Inspector General (OIG) conducted this audit to comply with the Act's 2013 reporting requirement.

Classified Information Security at NRC

The U.S. Nuclear Regulatory Commission (NRC) must protect classified information related to Federal Government programs for securing nuclear materials and facilities. Classification is the process of identifying information that must be protected against unauthorized disclosure in the interest of national security.

[4] Public Law 111-258/H.R. 553, "Reducing Over-Classification Act," October 7, 2010.

[5] Public Law 111-258, Section 2, "Findings."

[6] Public Law 111-258, Section 6, "Promotion of Accurate Classification of Information."

NRC staff work primarily with two types of classified information:

- **National Security Information (NSI):** Information classified by an Executive Order, whose compromise would cause some degree of damage to the national security.

- **Restricted Data (RD):** Information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.[7]

The lowest level of classified information is Confidential (C). The next higher level is Secret (S), and the highest level is Top Secret (TS). Thus, National Security Information documents may be marked C-NSI, S-NSI, or TS-NSI. Similarly, Restricted Data documents may be marked C-RD, S-RD, or TS-RD.[8]

NRC's Office of Nuclear Security and Incident Response (NSIR) has overall responsibility for the agency's information security program and develops policies and procedures for classified information security. Agency policy, which is based on higher-level Federal Government standards, is expressed in Management Directive 12.2, *NRC Classified Information Security Program*.

Classification may be performed only by personnel who have been delegated special authority and undergone required training. Specifically, Original Classifiers can make an initial determination, in the interest of national security, that information requires protection from unauthorized disclosure. In contrast, Derivative Classifiers may only restate or paraphrase information that has already been classified. To that end, Derivative Classifiers must transfer all pertinent classification markings from their sources to newly created documents. In addition, Derivative Classifiers may base their decisions on source documents or classification guides.[9] At the time of this audit, NRC had 11 Original Classifiers and

[7] More specifically, Restricted Data is all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142.

[8] NSI and RD can be combined in a document. Following the "Precedence Rule," for example, a document containing TS-NSI and C-RD would have an overall classification of TS-RD.

[9] In accordance with Executive Order 13526 and 32 CFR 2001, NRC performed a fundamental classification guidance review during 2011 and 2012.

approximately 100 Derivative Classifiers. In FY 2012, NRC reported no decisions by Original Classifiers, and approximately 2,459 decisions by Derivative Classifiers.[10]

Federal Classification Policies

On December 29, 2009, the President of the United States signed Executive Order (E.O.) 13526, "Classified National Security Information" (the Order), which establishes current principles, policies, and procedures for classification. The Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The Order also places equal emphasis on protecting information critical to national security while fostering Government transparency through accurate and accountable implementation of classified information management policies.

On June 25, 2010, the National Archives and Records Administration's Information Security Oversight Office (NARA/ISOO) issued a directive (the Directive) in the Code of Federal Regulations (CFR)[11] that included guidance to be used by Federal agencies in implementing the Order. Topics covered in this guidance include classification standards, classification challenges, declassification, information security, and agency reporting requirements.[12]

II. OBJECTIVES

In accordance with the Act's requirements, the audit objectives were to:

a) Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component.

[10] NRC's annual classification reports to the National Archives and Records Administration (NARA) include all classifications, regardless of media. For electronic classifications such as e-mail, NRC uses a NARA-approved sampling estimate methodology to count the number of classifications. The standardized reporting template does not disaggregate classifications by media type.

[11] 32 CFR Parts 2001 and 2003.

[12] Per 32 CFR 2001.90-91, NRC and other agencies are required to report annually to NARA/ISOO on matters such as delegation of classification authority, program costs and statistics, and self-inspections. As needed, agencies must also report events such as unauthorized declassification, reclassifications, and violations of the Order.

b) Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

The report appendix contains information on the audit scope and methodology.

III. FINDINGS

OIG auditors reviewed NRC policies and procedures for its classified information security program and developed five findings with corresponding recommendations to improve agency compliance with current Federal Government standards. Specifically, these findings address:

1. Original Classifier training.
2. Documentation of training certification.
3. Scope of self-inspections.
4. Staff position descriptions and performance evaluation criteria.
5. NRC policy guidance (Management Directive 12.2).

Auditors also reviewed a non-statistical sample of classified documents produced by NRC staff and found a limited number of marking errors but no evidence of systemic misclassification. Consequently, this report includes no findings or recommendations pertaining to misclassification.

A. Original Classifiers Do Not Receive Required Annual Training

Annual Training Requirement

The Order and the Directive require Original Classifiers to undergo annual training.[13] This training is to cover classification and declassification, as well as administrative matters such as classification appeals, managing information security breaches, and sanctions for unauthorized release of classified material. Further, Original Classifiers who do not undergo annual training are to have their authority suspended.[14]

[13] E.O. 13526, Section 1.3(d) and 32 CFR 2001.71(c).

[14] Original Classifiers may receive a waiver if they are unable to take required training because of unavoidable circumstances.

Required Training Not Taken

Original Classifiers had not taken required annual training during the time of this audit.[15] Through interviews with 3 of 11 NRC personnel who have Original Classification authority, auditors learned that these personnel had not taken required training. Auditors later confirmed with cognizant NRC staff that training had not been provided to Original Classifiers. However, staff said that a training program was being prepared at the time of the audit, and that the training would be delivered at some point in 2013.

Management Directive Does Not Convey Training Requirement

Required Original Classifier training has not occurred because NRC's Management Directive 12.2 does not prescribe training in accordance with current Federal standards. Although NRC's internal guidance requires Original Classifier training in general terms, it does not address periodicity (annual) or specify consequences for failure to satisfy Original Classifier training requirements.

Classifiers Need Training To Carry Out Their Duties

NRC's Original Classifiers who fail to meet their training requirements cannot perform classification work in an emergency, or in other unexpected circumstances that might require them to exercise their authority. Further, this training is intended to cover relevant administrative duties in addition to classification that Original Classifiers may need to perform as part of their work.

Recommendations:

OIG recommends that the Executive Director for Operations:

1. Update Management Directive 12.2 to reflect Original Classifier training standards expressed in Public Law 111-258, E.O.13526, and 32 CFR 2001.

2. Train Original Classifiers as directed by Public Law 111-258, E.O. 13526, and 32 CFR 2001.

[15] January 2013 through June 2013.

B. Training Certification Is Not Documented as Required

Training Documentation Requirement

Federal law requires documentation of training for Original and Derivative Classifiers. Public Law 111-258 specifically states that training for Original and Derivative Classifiers is a prerequisite, "as evidenced by an appropriate certificate or other record" for obtaining original classification authority or derivatively classifying information, and for maintaining such authority.[16] In addition, Government Accountability Office standards for Federal Government training recommend centralization of employee training records for efficiency and better management oversight, while maintaining a decentralized approach to training content and delivery.[17]

NRC Does Not Issue Documentation of Completed Training

NRC Classifiers are not issued training certificates or other documentation after completing required training. Auditors observed a training session for Derivative Classifiers and reviewed documentation of a previous Derivative Classifier training session. However, some classifiers interviewed by auditors could not accurately recall recent training dates, nor could they produce documentation of their training.

Training Information Managed by E-Mail

NRC staff explained that individual classifiers' training information is managed by e-mail correspondence, and that cognizant staff maintain a record of this activity. However, staff acknowledged that classifiers do not receive e-mail confirmation or other documentation after successfully completing required training. In contrast, other programs at NRC use the agency's automated training system, iLearn, to track training dates and validate credentials that require specific training.

[16] Public Law 111-258, Section 7(a)(2).

[17] United States General Accounting Office, Human Capital: *A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G, Washington, D.C.: March 2004.

Centralized Management Would Help Meet Documentation Requirement

Managing classifier training requirements and credentials centrally in NRC's iLearn system would provide classifiers and their supervisors better visibility over training obligations, and would facilitate compliance with Public Law 111-258 criteria. In addition, this would mitigate risk associated with reliance on a single person to manage training requirements and records through e-mail correspondence and computer desktop files.

Recommendation:

OIG recommends that the Executive Director for Operations:

3. Use iLearn to document classifier training, to include certifications and notification of suspended classification authority.

C. NRC Conducts Self-Inspections with Limited Scope

Self-Inspection Requirement

Federal standards require agencies to conduct routine self-inspections of classified information security programs. Specifically, the Order and the Directive state that self-inspections are to include regular reviews of representative samples of original and derivative classifications, and misclassifications are to be corrected.[18]

NRC Self-Inspections Have Limited Scope

NRC conducts self-inspections of its classified information security program.[19] However, these self-inspections do not include representative samples of classifications insofar as NSIR (the NRC office responsible for classified information security) does not review work produced by classifiers from other offices. Although NSIR produces nearly half of the classified NRC documents recorded in the agency's Form 790[20] tracking database, at least two other offices are known to produce classified documents. A fourth office reported producing no hard copy classified documents even though the office has 13 staff on NRC's roster of active Derivative Classifiers.

NRC Guidance Does Not Reflect Current Standard

Management Directive 12.2 calls for a self-inspection program, but does not reflect current Federal standards. Specifically, NRC's guidance does not call for representative sampling of agency classifications and correction of misclassifications. Although NSIR is responsible for NRC's classified information security program, the wording of Management Directive 12.2 in its current form does not provide NSIR leverage to conduct broader scoped self-inspections as called for in higher level Federal guidance.

[18] E.O. 13526 Section 5.4(d)(4), and 32 CFR 2001.60.

[19] NRC reported having conducted two self-inspections in FY 2012.

[20] NRC staff are supposed to complete Form 790 to document classifications, and submit each Form 790 to NSIR.

Expanded Self-Inspections Would Enhance Program Oversight

Expanded self-inspections would improve NRC's oversight of classification activity. In their current limited form, NRC's self-inspections do not cover the breadth of classification activity at NRC and, thus, provide limited ability to identify and correct errors and identify documents that might be eligible for declassification. Further, expanded inspections would improve classified document tracking and allow NRC to report classification activity to NARA/ISOO with greater accuracy.

Recommendations:

OIG recommends that the Executive Director for Operations:

4. Revise Management Directive 12.2 to require self-inspections in accordance with standards prescribed by E.O.13526 and 32 CFR 2001, to include representative sampling of original and derivative classifications as well as correction of misclassifications.

5. Conduct self-inspections in accordance with standards prescribed by E.O. 13526 and 32 CFR 2001, to include representative sampling of original and derivative classifications as well as correction of misclassifications.

D. NRC Does Not Include Classification Duties in Staff Position Descriptions and Performance Evaluations

Performance Management Requirements

Current Federal standards require NRC and other agencies to include classification duties in staff performance management. Specifically, the Order[21] requires management of classified information as a critical element for rating staff whose duties significantly involve handling of classified information. In addition, Public Law 111-258 states that agencies may consider proper and consistent classification of information in awarding cash incentives to authorized classifiers.[22]

Position Descriptions Do Not Include Classification Duties

Most Derivative Classifiers at NRC do not have classification duties in their position descriptions and are not rated on these tasks. Among nine Derivative Classifiers interviewed by auditors, six reportedly do not have classification duties in their position descriptions, and seven indicated that they are not evaluated on classification duties.[23] Some noted that they have been evaluated on classification duties in the past at NRC and/or other Federal agencies, and some cautioned that it is difficult to weigh classification duties proportionally to other core job tasks and responsibilities.

NRC Seeks To Resolve Issue

Cognizant NRC staff are aware of this requirement but face labor negotiation challenges in meeting it. NSIR staff confirmed that classification duties are not included in staff performance management. However, NSIR is working with the Office of the Chief Human Capital Officer to reach a solution that takes into consideration NRC's contractual obligations to bargaining unit (i.e., unionized) employees.

[21] E.O. 13526 Section 5.4(d)(7).

[22] Public Law 11-258, Section 6(a).

[23] One additional interviewee had recently changed jobs and was not sure if the current position's description and performance criteria address classification.

Solution Would Enhance Accountability and Performance Management

Developing a solution would benefit NRC because Federal policy emphasizes the importance of classification duties as well as employees' roles in promoting classified information security. NRC staff who routinely process and/or handle classified information cannot be held accountable and incentivized for this work if it is not considered as part of their formal position description used for performance evaluations.

Recommendation:

OIG recommends that the Executive Director for Operations:

6. Revise staff position descriptions and evaluation criteria, as practicable, to reflect classified information duties.

E. Management Directive 12.2 Needs Comprehensive Update

Management Directive Update Policy

NRC's internal policy requires the agency's management directives to be updated under specific circumstances. Management Directive 1.1[24] requires directive and handbook revisions to reflect changes in Federal law and regulation. Management Directive 1.1 also requires revisions every 5 years following a management directive's last complete revision.[25]

Management Directive 12.2 Is Not Up-to-Date

NRC has not updated Management Directive 12.2 to reflect current Federal policy and some agency practices. Examples of issues that need updates include:

- Federal policy references (e.g., Executive Orders).
- Classification categories and declassification exemptions.
- Third Agency Rule.[26]
- Classifier training requirements.
- Secure system for submitting allegations and complaints about misclassification within the agency.
- Specific requirements for reporting to NARA/ISOO.
- Form 790 reporting process.[27]

NRC issued a Yellow Announcement in January 2012 to address Federal policy references, classification categories and declassification exemptions, and the Third Agency Rule. However, Yellow Announcements are intended only as an interim policy measure preceding full revision of agency directives. Management Directive 12.2 was last approved in

[24] Management Directive 1.1, *NRC Management Directives System*, Section VI (A)(2).

[25] Management Directive 1.1, *NRC Management Directives System*, Section VII (A)(2).

[26] According to the current interpretation of the Third Agency Rule, staff no longer need authorization from a different originating agency to share classified information with third-party agencies if recipients have appropriate clearance and "need to know." Previously, agencies that created classified information and shared it with a second-party agency had to authorize its dissemination to third-party agencies.

[27] Management Directive 12.2 incorrectly references use of a dedicated data system to be used in Form 790 submissions. NRC retired this data system in 2011 to save money on system maintenance and now has different procedures for Form 790 submissions.

July 2006, while one page from its handbook was updated in August 2007; both of these actions thus occurred outside NRC's prescribed 5-year cycle for management directive revision.

NRC Has Postponed Update

NRC's process for revising management directives has deferred revision of Management Directive 12.2 until 2014. Although NSIR is responsible for this guidance, cognizant staff told auditors that they cannot initiate revision of a management directive and that such efforts must be coordinated with other offices.

Updating Directive Will Ensure Staff Have Accurate Guidance

NRC should comply with internal standards for management directive revision to ensure staff have current and accurate guidance to support their work. Indeed, Management Directive 1.1 explicitly states that it is agency policy "to communicate to employees NRC policies, requirements, and procedures necessary for the agency to comply with Executive Orders, pertinent laws, regulations, and the circulars and directives of other Federal agencies." Beyond the practical importance of timely management directive revisions, alignment between NRC guidance and higher level Federal guidance is important for positioning NRC as a responsive, transparent regulatory organization.

Recommendation:

OIG recommends that the Executive Director for Operations:

7. Update Management Directive 12.2 to align with E.O. 13526, Public Law 111-258, and 32 CFR 2001, and to reflect current NRC policy and procedures.

IV. CONCLUSION

Recent changes in Federal laws, policies, and regulations governing classification underscore the importance of maintaining a robust and transparent classified information security program. OIG auditors evaluated NRC's classification policies and procedures, including a review of classified documents created by agency staff. Based on this work, OIG identified several opportunities for NRC to align its policies and procedures with Federal standards. However, auditors did not find evidence of systemic misclassification at the agency and therefore have no findings or recommendations pertaining to misclassification.

V. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Update Management Directive 12.2 to reflect Original Classifier training standards expressed in Public Law 111-258, E.O.13526, and 32 CFR 2001.

2. Train Original Classifiers as directed by Public Law 111-258, E.O. 13526, and 32 CFR 2001.

3. Use iLearn to document classifier training, to include certifications and notification of suspended classification authority.

4. Revise Management Directive 12.2 to require self-inspections in accordance with standards prescribed by E.O.13526 and 32 CFR 2001, to include representative sampling of original and derivative classifications as well as correction of misclassifications.

5. Conduct self-inspections in accordance with standards prescribed by E.O. 13526 and 32 CFR 2001, to include representative sampling of original and derivative classifications as well as correction of misclassifications.

6. Revise staff position descriptions and evaluation criteria, as practicable, to reflect classified information duties.

7. Update Management Directive 12.2 to align with E.O. 13526, Public Law 111-258, and 32 CFR 2001, and to reflect current NRC policy and procedures.

VI. AGENCY COMMENTS

An exit conference was held with the agency on September 3, 2013. Agency staff generally agreed with the report findings and recommendations, and provided technical comments on a draft version of the report. OIG has incorporated these comments as appropriate into the final version of the report.

Appendix

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

OIG conducted this audit in accordance with Public Law 111-258 to:

(a) Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component.

(b) Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

Scope

OIG performed this work from January 2013 through June 2013. Auditors conducted interviews and document reviews at NRC headquarters in Rockville, MD, with cooperation from staff representing NSIR, the Office of Nuclear Material Safety and Safeguards, the Office of Nuclear Reactor Regulation, the Office of International Programs, the Office of the Commission, and the Office of the Executive Director for Operations. Auditors also conducted interviews and document reviews at two NRC regional offices. Internal controls related to the audit objectives were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program.

Methodology

OIG conducted this audit using guidance developed by the Council of Inspectors General for Integrity and Efficiency specifically to provide Federal Inspectors General a common framework for conducting evaluations in accordance with Public Law 111-258. To understand background and contextual issues, auditors reviewed reports by the Government Accountability Office, Environmental Protection Agency Office of the Inspector General, and the Department of Health and Human Services Office of the Inspector General. To assess NRC's classification policies and procedures, auditors reviewed requirements in Public Law 111-258, E.O. 13526, and 32 CFR 2001 and compared these standards to information obtained from NRC documents and interviews with NRC staff. To

assess classifiers' training and understanding of classification policies and procedures, auditors interviewed Derivative and Original Classifiers who, together, represented nine different NRC offices. Auditors also attended a training session for Derivative Classifiers and analyzed instruction materials provided to trainees.

To assess classification actions, auditors drew a non-statistical sample of hard copy classified documents produced and/or maintained by staff representing four NRC offices. Auditors reviewed 18 of 34 classified documents identified by analysis of NRC's Form 790 database and by direct observation.[28] This sample focused on documents produced between June 30, 2010, and May 1, 2013.[29] Selected documents included National Security Information and Restricted Data classification categories, as well as Confidential and Secret classification levels. Auditors analyzed these documents using a checklist of questions to determine whether each document had proper markings, such as classification reason codes, information source identification, and classifier identification. Auditors reviewed document contents to ensure classification was justified based on classification reason codes, and examined each document to ensure that no prohibited caveats were used.[30] During this review, auditors, found two documents with marking errors: one missing a classification reason code and one missing a classified information category stamp. Based on this document review, auditors concluded that there was no evidence in this document sample of systemic misclassification at NRC.

We conducted this performance 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 based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit work was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; and Larry Vaught, Senior Auditor.

[28] Auditors found several documents during their reviews that had not been registered in NRC's Form 790 database, which the agency uses to track classifications.

[29] 32 CFR 2001 took effect on June 25, 2010; therefore, auditors assessed documents produced subsequently to check for compliance with current standards. In short, auditors did not retroactively apply current standards to documents produced in accordance with different policies.

[30] E.O. 13526 Section 1.7 explicitly prohibits use of classification to conceal malfeasance or information that would embarrass individuals or an organization.