



OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

OIG-16-A-17

June 8, 2016



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**

June 8, 2016

MEMORANDUM TO: Victor M. McCree **/R/**
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-16-A-17)

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 June 2, 2016, 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 (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated



Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-16-A-17

June 8, 2016

Results in Brief

Why We Did This Review

The Reducing Over-Classification Act of 2010 mandated that the inspectors general of all Federal agencies with original classification authority perform at least two evaluations over proper use of classified information.

The act found that over-classification of information negatively affects dissemination of information within the government, increases information security costs, and needlessly limits stakeholder and public access to information.

NRC OIG issued the first mandatory audit report in 2013. The report's recommendations have been implemented by NRC. This report represents the results of OIG's second mandatory review.

The audit objective was to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed and effectively administered, and identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

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

What We Found

NRC's implementation of Federal classified information laws and policies protects classified information. Document reviews of NRC classification actions reported from April 2013 through January 2016 revealed no systematic misclassification. However, there are opportunities for improvement of records management of classified information within NRC.

Currently, the lack of records management of classified information within NRC has prevented timely disposition and declassification. NRC has not reviewed classified records for disposition and declassification as required and is not prepared for mandatory reviews.

Federal guidance requires agencies to implement a schedule for proper disposition. Effective records management supports timely review of classified information for exemption from automatic declassification and for disposition. However, NRC lacks a cohesive approach to records management of classified information which fosters inadequate understanding of and preparation for records management of classified information.

What We Recommend

This report makes recommendations to complete and fully implement current agency initiatives and to develop procedures and guidance to ensure effective records management and timely disposition and declassification of classified records at NRC. Management stated their agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

<u>ABBREVIATIONS AND ACRONYMS</u>	i
I. <u>BACKGROUND</u>	1
II. <u>OBJECTIVE</u>	5
III. <u>FINDING</u>	5
Lack of Records Management Has Prevented Timely Disposition and Declassification	5
Recommendations	12
IV. <u>AGENCY COMMENTS</u>	13
 APPENDIX	
<u>OBJECTIVE, SCOPE, AND METHODOLOGY</u>	14
 <u>TO REPORT FRAUD, WASTE, OR ABUSE</u>	17
<u>COMMENTS AND SUGGESTIONS</u>	17

ABBREVIATIONS AND ACRONYMS

MD	Management Directive
NRC	U.S. Nuclear Regulatory Commission
OIG	Office of Inspector General

I. BACKGROUND

Legislative Basis for the Audit

The Reducing Over-Classification Act of 2010¹ found 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 asserted that overclassification negatively affects dissemination of information within the Federal Government; with State, local, and Tribal entities; and with the private sector. Lastly, the act stated that Federal agencies that perform classification are responsible for developing, implementing, and administering policies, procedures, and programs that promote compliance with applicable laws, executive orders, and other authorities pertaining to the proper use of classification. The act required the inspector general of each agency authorized to make original classifications to perform at least two evaluations to assess whether the agency has implemented Federal laws, orders, and other authorities for proper use of classified information.

Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) published the first mandatory audit report in 2013.² The report made several recommendations for program updates and improvements, including revise Management Directive (MD) 12.2, *NRC Classified Information Security Program*; update regular training for original and derivative classifiers, and make it available electronically; and develop and implement a self-inspection process. The recommendations were all closed.

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

² [OIG-13-A-21, Audit of NRC's Implementation of Federal Classified Information Laws and Policies, September 12, 2013.](#)

Classified Information Within NRC

NRC possesses two primary categories of classified information:

- National Security Information: Information classified by an Executive Order, whose compromise would cause some degree of damage to the national security.
- Restricted Data: Information classified by the Atomic Energy Act,³ concerning the production of special nuclear materials⁴ or the use of special nuclear material in the production of energy.

There are three levels of classification used by the Federal government, including NRC, for the protection of classified information:

- Top Secret: Unauthorized disclosure could result in “exceptionally” grave damage to national security.
- Secret: Unauthorized disclosure could result in “serious damage” to national security.
- Confidential: Unauthorized disclosure could result in “damage” to national security.

Only these three classification designators may be used to identify the level of classification assigned to information.

Authorized Classifiers

A classification determination regarding NRC information, regardless of form, must be made solely by an NRC authorized classifier who has been delegated that authority and trained to exercise the authority.

An authorized classifier is delegated either original or derivative classification authority. An authorized classifier with original classification authority may classify information, on the basis of his or her knowledge, authority, and expertise, and if it meets specific Federal criteria. An

³ The [Atomic Energy Act of 1954, as amended](#), created the Atomic Energy Commission, predecessor organization to the NRC and Department of Energy.

⁴ Special nuclear materials consist of uranium-233 or uranium-235, enriched uranium, or plutonium.

authorized classifier with derivative classification authority may only classify information on the basis of classification determinations made by an original classification authority, a source document, or other classification guidance (e.g., a classification guide, a bulletin, or a notice).

NRC staff employ multiple electronic classified information systems to communicate classified information internally and with other agencies. The emails and documents they create and receive constitute classification activity. Therefore, at NRC, any user of an electronic classified information system must be trained and authorized for derivative classification.

NRC Classification Activity in 2015

In 2015, NRC reported that staff made no original classification decisions and 5,479 derivative classification decisions. Only 710 of these decisions were Confidential. The remainder were almost evenly split between Secret and Top Secret. The majority of the classification activity was in electronic form.

Declassification

Federal laws and authorities limit the time for which National Security Information can be classified. Exemptions for National Security Information meeting specific requirements can be established at original classification or through timely review before declassification. If classified information derives from another agency's original classification, the originating agency has equity in the information and makes the final declassification decision. There are three categories of declassification:

- *Automatic* occurs 25 years after the date of classification if no other date is specified.
- *Systematic* occurs after review of permanent records of historical value that are exempted from automatic declassification determines that the record no longer meets the standards for classification under Executive Order 13526.

- *Mandatory* occurs after a review triggered by a request for specific classified information determines that the information no longer meets the standards for classification under Executive Order 13526.

Restricted Data must be reviewed by the Department of Energy and is excluded from declassification by NRC.

Records Retention Schedules

Classified documents are also Federal records. Permanent and temporary records, regardless of medium or form, must be identified and assigned a records retention schedule. The schedule defines the life cycle of the record from creation to disposition. Disposition may range from destruction to temporary storage to transfer to the National Archives and Records Administration for permanent retention. Most Federal records are temporary and may be disposed after a designated retention period. Permanent records are determined to have historical or other value to warrant preservation beyond the time they are needed for administrative, legal, or fiscal purposes. Working files, such as draft documents, or transitory files of short-term interest can be destroyed and do not require retention schedules. Records retention schedules apply to classified as well as unclassified records.

Responsible NRC Offices

Several NRC offices have roles in NRC's classified information program, primarily

- Office of Nuclear Security and Incident Response, Division of Security Operations plans, develops, establishes, and administers policies, standards, and procedures for the NRC classified information security program, and manages the security classification program.
- Office of Administration, Division of Facilities and Security plans, develops, establishes, and administers policies, standards, and procedures for NRC facilities for handling and storing classified and sensitive unclassified information.

- Office of the Chief Information Officer, IT/IM Portfolio Management and Planning Division develops Information and Records Management policy and implements records operations and the records retention schedule.

II. OBJECTIVE

The audit's dual objectives derive from the Reducing Over-Classification Act:

- A. Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and
- B. Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

III. FINDING

NRC's implementation of Federal classified information laws and policies protects classified information. Document reviews of NRC classification actions reported from April 2013 through January 2016 revealed no systematic misclassification. However, there are opportunities for improvement related to the records management of classified information.

Lack of Records Management Has Prevented Timely Disposition and Declassification

Managing classified information through its life cycle ensures required reviews for declassification or other disposition occur. NRC has not reviewed classified records for disposition, as required, and is not

prepared for mandatory reviews. This stems from a lack of a cohesive approach to records management of classified information. Misclassification, uncontrolled release, inefficient use of resources, and reduction of transparency may result.

What Is Required

Records Management Should Facilitate Declassification

Federal and NRC policies emphasize planning for the disposition of a document at its creation.

Federal Guidance

Agencies must identify, schedule, and describe all records, and implement the schedule for proper disposition. Agencies must also have policies in place to identify, manage, and disposition emails that are Federal records.

Handling classified information over its entire life cycle is a subset of this government records management activity. Executive Order 13526, "Classified National Security Information,"⁵ underscored previously existing requirements for declassification reviews and tied declassification to records management, stating:

[Agencies shall] ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification.

The Executive Order allows for exemption from declassification using a process based on good records management. All classified records that are more than 25 years old and have been determined to have permanent historical value shall be automatically declassified whether or not the records have been reviewed. A review identifying one of several permitted reasons can exempt records from automatic declassification, but any exempted records should be described, either by reference to

⁵ [Executive Order 13526, "Classified National Security Information," December 29, 2009.](#)

information in specific records or in the form of a declassification guide, with an explanation of why the information is exempt. Information exempted from automatic declassification remains subject to the separate mandatory and systematic declassification review provisions of the order. Good records management prepares for disposition of classified information that includes automatic declassification or exemption from automatic declassification by identifying and describing classified records and implementing their associated retention schedules.

The U.S. Government Accountability Office *Standards for Internal Control in the Federal Government*⁶ states that having integrated policies, plans, and activities contributes to internal control processes providing reasonable assurance that objectives are met – in this case compliance with required review and declassification or other disposition of classified information.

NRC Guidance

NRC records management policy and guidance emphasize that, within constraints for protecting classified information, the same records management requirements should be followed.

What We Found

NRC Does Not Meet All Requirements for Disposition of Classified Information

NRC has not reviewed classified records for disposition and declassification, as required, and is not prepared for mandatory reviews.

Accumulated Backlog of Unprocessed Classified Information

NRC staff has a backlog of hard copy classified information that requires processing.⁷ The agency has approximately 1,500 cubic feet of classified

⁶ [*Standards for Internal Control in the Federal Government*](#), September 2014

⁷ Processing includes organizing the information and identifying applicable records series to determine the retention schedule. Records schedules apply regardless of classification level or status of records. Documents that are approaching or that have reached their declassification dates must undergo review for declassification or exemption.

holdings in General Services Administration-approved containers issued across the agency and in security areas approved for the open storage of classified information. Some of the classified material relates to Atomic Energy Commission activities dating to the 1950s. Some material is Restricted Data, which is not automatically declassified but which, like all records, must be reviewed for proper disposition. Disposition may necessitate transfer to the Department of Energy, which has equity in and makes final determinations about all Restricted Data.⁸

NRC Not Prepared for Mandatory Review

NRC lacks specific procedures to conduct declassification reviews, in particular mandatory declassification reviews. A recent citizen request for declassification of approximately 200 pages met Federal standards for specificity and completeness. Staff must plan a review of these materials to consider whether declassification is feasible both individually and in compilation. Any exemptions must be justified, according to Federal requirements. However, to complete this task, NRC must first develop instructions for staff conducting the review.

Classifiers Uncertain About Records Management

Classifiers are uncertain what is an agency record and do not understand how to manage their hardcopy and electronic files. For example, related to hardcopy documents,

- One classifier stated that he keeps drafts because he is not sure whether any one of them is a temporary or permanent record rather than just a working document.
- Another classifier keeps copies of classified documents for reference because the originals are “owned by” a different office.

⁸ NRC also holds some Formerly Restricted Data onsite that has been provided by other agencies and is not the result of NRC derivative classification activity. Formerly Restricted Data is classified information related primarily to the military utilization of atomic weapons that has been removed from the Restricted Data category after the Department of Energy and U.S. Department of Defense have jointly determined that the information can be adequately protected in a manner similar to National Security Information. Like Restricted Data, Formerly Restricted Data is not subject to automatic declassification, and the Department of Energy makes final determinations about its disposition.

These occurrences are reflected in NRC's 2015 self-inspection report, which noted that keeping drafts and duplicates after a classified document is completed is a "prevalent issue."

Further, records management within classified electronic information systems relies on individual approaches to file management. For example, one system user described careful organization of classified email and personal drive contents but noted system owners do not limit storage volume or push users to cull their account files. File management is not a priority for most users. Individual approaches do not systematically capture classified electronic records and identify them for a scheduled review.

Why This Occurred

Lack of Cohesive Approach to Records Management for Classified Information

Lack of a cohesive approach to records management of classified information fosters inadequate understanding of and preparation for records management of classified information.

NRC Policy Does Not Provide for Routine Declassification Activity

NRC policy in MD 12.2, *NRC Classified Information Security*, spells out requirements for many aspects of classification and classified information security. The MD addresses classification, controlling, handling, and marking, and discusses automatic declassification and exemptions. However, the policy guidance describes declassification review as a reactive process rather than as an ongoing responsibility. Further, the MD says that the Office of Nuclear Security and Incident Response will designate authorized declassifiers, provide guidance, and coordinate with other agencies, yet the MD does not provide for routine, annual reviews for declassification or other disposition.

NRC Lacks Classified Record Review Procedures

Procedures for the automatic, systematic, discretionary, and mandatory declassification review of documents have not been fully established and

implemented. Further, there is no systematic procedure for NRC's classified electronic system users to manage emails and documents for future review.

Classifier Training Overlooks Records Management

Classifier training explains principles of derivative classification, classification levels, duration of classification, classification guides, and identification and markings. Training also discusses classification prohibitions and limitations, sanctions, classification challenges, and security. Individual classifiers are properly trained and are aware of penalties to individuals for spills of classified information as spelled out in guidance.

However, training for classifiers does not mention records management for disposition and review for declassification. Without policy guidance or training on disposition and declassification, users are "better at classification than declassification." They default to what they know well – protected storage – rather than ensuring proper records management of classified documents.

Current NRC Initiatives

NRC recognizes the lack of procedures and declassification training and has several current initiatives. However, these initiatives are not mature. Efforts include

- Records management training under development to guide classifiers on the life cycle of classified documents and to emphasize proper marking supports effective maintenance and disposition of records.
- Inventory and cleanup of safe contents to support efforts to schedule, review, and disposition documents.
- Regular training of authorized declassifiers to ensure subject matter experts are available to support declassification reviews.

- Development of an updated declassification guide to support declassification reviews.
- Processing the material currently in secure storage to determine declassification status and schedule disposition.
- Developing an Office Instruction covering the process for receiving, planning, conducting, and providing results of a mandatory declassification review.

Challenges will persist until these efforts are completed.

Why This Is Important

Potential for Misclassification, Uncontrolled Release, Inefficiency, Reduced Transparency

Misclassification, uncontrolled release, inefficiency, and reduced transparency may result from lack of a cohesive records management approach.

- Lack of understanding of the document life cycle could result in incorrect or inconsistent use of declassification markings, which is a form of misclassification.
- Automatic declassification reviews have not been completed, which increases the potential risk of an uncontrolled release.
- Storing and securing a backlog of unreviewed classified material is an ineffective use of resources.
- Delay of declassification by a lack of timely review could decrease transparency.
- Lack of preparation for a mandatory review slows the response and creates an additional burden that competes with planned work.

Recommendations

OIG recommends that the Executive Director for Operations

1. Complete and fully implement current initiatives:
 - a. Finalize and provide records management training for authorized classifiers.
 - b. Complete the current inventories of classified information in safes and secure storage areas.
 - c. Develop declassification training to prepare and authorize declassifiers.
 - d. Develop an updated declassification guide.
 - e. Identify classified records requiring transfer to National Archives and Records Administration and complete the transfers.
 - f. Complete the Office Instruction for performing mandatory declassification reviews.
2. Develop procedures for how to disposition NRC classified records that other agencies have equity in.
3. Develop guidance for derivative classifiers to apply records management principles to documents created and stored electronically.

IV. AGENCY COMMENTS

An exit conference was held with the agency on June 2, 2016. Prior to this meeting, after reviewing a discussion draft, agency management provided comments that have been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objectives were to:

- A. Assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered, and
- B. Identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

Scope

This audit focused on the implementation of Federal classified laws and policies by NRC offices responsible for classified information security, and whether the classified information program prevents systematic misclassification.

Audit scope included verification of the effectiveness of program changes implemented in response to recommendations from the 2013 NRC OIG audit, such as

- Training and authorization records.
- Training content.
- Self-inspection procedures and reports.
- Classified information duties reflected in position descriptions and/or performance evaluation criteria.

The scope of the document review included National Security Information and Restricted Data classified at NRC since the 2013 audit, but did not include licensee or contractor information.

OIG conducted this performance audit from December 2015 to April 2016 at NRC headquarters (Rockville, MD), Region II (Atlanta, GA), and Region IV (Arlington, TX). Internal controls related to the audit objectives were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility of fraud, waste and abuse in the program.

Methodology

OIG reviewed relevant laws, regulations, and policies; conducted approximately 40 interviews of NRC staff and management; and reviewed Secret and Confidential classified documents representing about 87 percent of hardcopy classification activity since the 2013 audit.

OIG reviewed applicable Federal requirements, including

- Executive Order 13526, Classified National Security Information, December 29, 2009.
- PL 111-258, The Reducing Over-Classification Act, October 7, 2010.
- 32 CFR Part 2001, Classified National Security Information, July 28, 2010.
- 10 CFR Part 1045, Nuclear Classification and Declassification, December 31, 1997.
- Atomic Energy Act of 1954, as amended.

We reviewed NRC requirements, including

- Management Directive (MD) 12.1, "NRC Facility Security Program."
- MD 12.2, "NRC Classified Information Program."

- MD 12.5, "NRC Cybersecurity Program."
- MD 3.53, "NRC Records and Document Management Program."
- Office Instructions.

OIG interviewed derivative classifiers and others in Office of Nuclear Security and Incident Response, Office of the Chief Information Officer, Office of Administration, Office of Nuclear Reactor Regulation, Office of Nuclear Material Safety and Security, and Regions II and IV. OIG viewed storage areas in headquarters and the regions.

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 was conducted by Beth Serepca, Team Leader; Kristen Lipuma, Audit Manager; Amy Hardin, Audit Manager; and Felicia Silver, Auditor.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: [Online Form](#)

Telephone: 1-800-233-3497

TDD 1-800-270-2787

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this [link](#).

In addition, if you have suggestions for future OIG audits, please provide them using this [link](#).