U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Inspection Report

Review of Controls Over the Department's Classification of National Security Information

DOE/IG-0904 March 2014

Department of Energy
Washington, DC 20585

March 27, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Review of Controls Over the Department's Classification of National Security Information"

BACKGROUND

The Department of Energy handles and manages a broad spectrum of classified information, including National Security Information (NSI). NSI relates to national defense and foreign relations information and is classified in accordance with Executive Order 13526 and 32 Code of Federal Regulations Part 2001, each entitled *Classified National Security Information*. Federal requirements for NSI stress the need for the flow of information without compromising its protection, and prescribe a uniform system for classifying, safeguarding and declassifying NSI.

The Office of Health, Safety and Security's Office of Classification, manages the Department-wide classification program and establishes policies to conform with Federal classification requirements. Implementation of classification requirements is shared among various organizations within the Department. In addition, the Department's Office of Intelligence and Counterintelligence (Headquarters Intelligence) is required to follow NSI policies and procedures instituted by the Office of the Director of National Intelligence. Similarly, the Department's National Nuclear Security Administration (NNSA) separately develops and implements policies and procedures, in coordination with the Office of Classification, for the protection and security of classified information at NNSA sites.

Due to the importance of adequately protecting and sharing classified NSI and in conjunction with a Government-wide review of such material conducted by a number of other offices of Inspector General, we initiated this inspection to assess the status of the Department's classified NSI program. The vast majority of the Department's classified information is Restricted Data and Formerly Restricted Data, which concerns nuclear weapons-related data.[1] Classification of this information was not assessed during this review.

RESULTS OF INSPECTION

Our inspection revealed that the Department had established and implemented critical elements of its classified NSI program. However, our review revealed that certain aspects of the NSI program could be improved. Our inspection determined that:

[1] Classified Restricted Data and Formerly Restricted Data are protected in accordance with the *Atomic Energy Act of 1954*, as amended, which provides different classification requirements from NSI, including exclusion from portion marking and automatic declassification. Further, dissemination of Restricted Data and Formerly Restricted Data is limited to individuals with special access.

- Of the 231 documents and emails we reviewed, 65 percent had classification marking errors that could adversely impact efforts to protect classified NSI against loss or unauthorized disclosure and impede information sharing. These errors included: (1) over or under classification; (2) improper annotations regarding duration and source of protection; and, (3) missing information on the origin and level of protection.

- A classification marking tool embedded in the classified email system at an NNSA site automatically marked emails as Secret//Restricted Data, regardless of content. We observed and senior program officials confirmed that this automatic feature could potentially result in over classifying and improperly marking classified NSI; however, we did not identify any instances in which this actually occurred.

- Headquarters Intelligence officials had not fully implemented required biennial self-assessments and annual classification decision reviews at Headquarters and field intelligence elements to identify and correct classification errors.

- Some of the derivative classifiers we interviewed who were responsible for ensuring the protection of classified information were not familiar with the requirements for making a formal challenge to external entities when they believed that information could be misclassified. However, they were aware of their responsibility to reach out internally to their respective classification officers.

The issues identified in this report are based on a judgmentally selected sample. Yet, when considered in conjunction with deficiencies identified by separate compliance reviews completed by the Office of Classification, they may reflect lessons learns which apply to the broader NSI classification processes at Department and NNSA elements. A summary of the requirements and the results of our review are detailed in Appendix 1, *Inspectors General Community-Wide Focus Areas* and Appendix 2, *Document Review Results*.

The classification related issues we observed occurred, in part, because of ineffective oversight of classification activities and inadequate training and guidance. We were told by a classification program official that oversight activities such as self-assessments and document decision reviews had not been completed at Headquarters Intelligence and field intelligence elements because Headquarters Intelligence had not allocated resources to do so. Also, Headquarters Intelligence officials had not granted proper security clearances to allow local classification officers to assess and review the classified NSI program at field intelligence elements. Further, interviews revealed, and we confirmed, that performance standards regarding classification duties had not been established for the majority of the Federal derivative classifiers we interviewed, although required by Executive Order 13526.

With regard to the sufficiency of training and guidance on classification, we found that derivative classifiers' initial and refresher training materials focused on marking documents, but not emails. We also found that this training had not provided sufficient emphasis on marking working papers that contained classified NSI. Further, we noted that although the Department offers training covering the topic of marking classified working papers at Headquarters, derivative classifiers were not required to complete the training.

In addition, the Department and NNSA guidance pertaining to marking classified emails was not consistent with Federal requirements. In particular, the Federal guidance required marking emails in the electronic environment while Department and NNSA guidance only required that emails be marked when printed. Also, interviewed derivative classifiers were not familiar with all requirements for making a formal challenge regarding information that could be misclassified because the Department had not developed comprehensive training and guidance on that subject.

Striking a balance between protecting NSI and appropriate information sharing is difficult even in optimal circumstances. But, it became clear that effective oversight, training and well-developed guidance for those involved with the classification of NSI are imperative if the Department is to be successful in this effort. We made a number of recommendations to assist the Department with improving program management and execution of its classified NSI program.

MANAGEMENT REACTION

While management concurred with the recommendations in the report, concerns were raised on the impact our recommendations would have on established processes for classifying and protecting Restricted Data and Formerly Restricted Data, and on the costs associated with implementing corrective actions resulting from the recommendations. As more fully discussed in the body of the report, alternative marking procedures that are compliant with Federal NSI requirements are available and could address management's concerns. Overall, we found management's comments and planned corrective actions to be generally responsive to our report findings and recommendations. Management's formal comments are included in Appendix 6.

Attachment

cc: Deputy Secretary
Chief of Staff
Acting Administrator, National Nuclear Security Administration
Chief, Health, Safety and Security Officer
Director, Office of Intelligence and Counterintelligence
Chief Information Officer

REPORT ON REVIEW OF CONTROLS OVER THE DEPARTMENT'S CLASSIFICATION OF NATIONAL SECURITY INFORMATION

TABLE OF CONTENTS

Classification of National Security Information

Appendices

PROTECTING NATIONAL SECURITY INFORMATION

Our inspection revealed that the Department of Energy's (Department) Office of Health, Safety and Security, Office of Classification had taken steps to establish policies and procedures to protect National Security Information (NSI) within the Department. While we observed that some improvements to training were necessary, we determined that, in general, individuals authorized to originally or derivatively classify information had received fundamental training and possessed the basic knowledge necessary to execute their classification duties.[3] The training covers familiarization with the system of classification, derivative review process and use of classification guides, and marking mechanisms. However, opportunities for improvement exist for certain aspects of the Department's classified NSI program for the three Department elements we reviewed.

Classification Marking Errors

Requirements in 32 Code of Federal Regulations (CFR) Part 2001, *Classified National Security Information,* indicate that classification markings, such as elements of a classification block as well as portion and banner markings, are essential to leave no doubt about the classified status of information, level of protection required and duration of classification.[4] Appendix 3, *Sample of a Classified Document,* provides an illustration for marking classified information. Further, Department Order 471.6 and National Nuclear Security Administration (NNSA) Policy Letter 70.4, both entitled *Information Security*, specifies Departmental marking requirements for classified working papers and emails to ensure that information is adequately classified and protected.[5]

In spite of the specific information contained in these authorities, we found that a number of items we examined were not properly marked by derivative classifiers. Of the 231 documents and emails we reviewed, 65 percent had classification marking errors that could adversely impact efforts to protect and share classified NSI, as presented in Appendix 2, *Document Review Results*.[6] Notably, we found classification marking errors including: (1) over or under classification; (2) improper annotations regarding duration and source of protection; and (3) missing information on the origin and level of protection.

Over or Under Classification

We determined that four emails and one document were over or under classified. For example, one email was marked classified even though the email did not contain classified information and three transmittal emails were marked unclassified but contained classified attachments. We

[3] Individuals with original classification authority classify information in the first instance (originally). Individuals with derivative classification authority incorporate, paraphrase, restate, or generate, in new form, information that is already classified and also apply markings in accordance with classification guidance and source documents.
[4] Classification block consists of the "Classified by," "Derived from," and "Declassify on" lines.
[5] Working papers are documents or materials that are expected to be revised prior to the preparation of a finished product for dissemination or retention.
[6] A single document or email may include multiple marking errors.

found that the Department and NNSA guidance did not provide information on marking emails with classified attachments. A senior program official also stated that the practice of marking unclassified transmittal emails with classified attachments was adequate provided that appropriate warnings were noted in the emails. However, we noted that this practice was contrary to 32 CFR Part 2001, which indicates that the overall classification of an email should account for the classification level of any attached files, including the transmittal message.

In addition to emails, we noted one document was improperly marked Secret NSI even though it contained classified Formerly Restricted Data, information that requires special access. Such marking resulted in the document being subject to a premature release due to NSI automatic declassification provisions, which is contrary to the *Atomic Energy Act of 1954,* as amended (Atomic Energy Act).[7] Unlike NSI, documents classified as Restricted Data or Formerly Restricted Data do not have declassification instructions. We noted that the document was part of a classified file that was updated on a frequent basis. Such updates could potentially change the classification status of the documents contained in the file. Even though this classified document appeared to have characteristics of a "Draft" or "Working Paper," it was not annotated to convey the working draft status of the file, contrary to Department Order 471.6 and NNSA Policy Letter 70.4.

Improper Annotation Regarding Duration and Source of Protection

We identified 37 documents that contained improper instructions on when to declassify information. Although required, 17 of the 37 documents we reviewed did not include the appropriate and more restrictive declassification instructions. The documents specified automatic declassification dates within 25 years instead of correctly indicating that the information was exempt from automatic declassification. According to a senior program official, the absence of declassification exemption markings may present a risk of prematurely disclosing classified information, even if documents include a control marking indicating that information requires a review by an authorized individual prior to declassification. Other program officials opined that there is little risk of improper disclosure because a review is specifically required prior to declassification. We could not reconcile these disparate views, but noted that compliance with marking requirements generally improves accountability and helps protect against improper disclosure.

Additionally, we identified two documents from field intelligence elements in which marking guidance was incorrectly applied. One of these documents was marked with a specific declassification date within 25 years and another marked with 25X1. Both documents, however, appeared to contain information meeting the criteria of 50X1-HUM declassification exemption.[8]

[7] Classified NSI is subject to automatic declassification, which permits information to be declassified without review, if the document is more than 25 years old and has been determined to have permanent historical value under Title 44, United States Code. However, classified NSI requiring continued protection beyond 25 years can be exempted from automatic declassification, when the information has been determined to satisfy one or more of the exemption categories as indicated on the classification guides used.

[8] Both 25x1 and 50x1 are automatic declassification exemptions indicating that the document shall be protected beyond 25 and 50 years, respectively. 50X1 is applied to information that could reveal the identity of a confidential human source, whereas 25X1 pertains to human and non-human sources and methods.

The respective derivative classifiers interviewed indicated that they were unaware of a policy change issued by Information Security Oversight Office, *Notice 2012-02: Classification Marking Instructions on the Use of "50X1-HUM" vs "25X1-human" as a Declassification Instruction*, in December 2011. This policy specified that the declassification instruction of 50X1-HUM should be applied if information could reveal specific sources. Further, based on a separate document review performed by a senior program official and an Office of Intelligence and Counterintelligence (Headquarters Intelligence) derivative classifier, the information contained in the two documents came from multiple sources, even though the documents did not include a source list. This treatment is contrary to 32 CFR Part 2001, which indicates that a listing of source materials should be indicated or attached to a derivatively classified document if multiple sources were used to classify the information. Accordingly, proper declassification instructions could not be determined because the source list information was not available.

We further identified improper instructions in 32 emails regarding the duration of protection. Half of these emails originated from Headquarters Intelligence and field intelligence elements. Headquarters Intelligence derivative classifiers stated that a classification marking tool embedded in the email system allowed users to set-up default declassification instructions. However, we found that instructions were not always modified to ensure consistency with the classification guide being used. Further, we determined that the Headquarters Intelligence classification marking tool had not been deployed in the classified email systems at two field intelligence elements. Thus, field intelligence elements derivative classifiers applied classification markings manually and also, in the majority of the cases we reviewed, markings that were inconsistent with requirements.

Missing Information on the Origin and Level of Protection

We determined that classification blocks and portion markings, which describe the origin, duration and level of protection, were not always properly annotated on the documents reviewed. We identified 20 documents that were marked as classified by derivative classifiers in which the blocks were missing information. According to a local classification officer, derivative classifiers were not required to mark the documents until the documents were considered final. Further, the local classification officer told us that draft documents or working papers were not required to be marked by derivative classifiers until after 180 days of creation or prior to being released outside the organization. However, we noted that these documents, which were hard copies, were not marked as "Draft" or "Working Papers" to clearly convey the status of classified information as required by Department Order 471.6 and NNSA Policy Letter 70.4. Furthermore, contrary to 32 CFR Part 2001, we identified 57 documents and emails that lacked portion markings on the subject line and main body of documents and emails; 42 of the 57 documents and emails were attributable to emails that originated from Headquarters Intelligence and field intelligence elements. Without adequate information on the origin and level of protection, traceability to the origin of classification decisions and protection of classified information could negatively impact efforts to safeguard and share classified NSI.

Classified Email System

We observed that a classification marking tool embedded in the classified email system at one NNSA site automatically marked emails as Secret//Restricted Data , the highest level of protection authorized for that system, regardless of content. In contrast, the classified email system at another NNSA site did not include a marking tool, and required users to manually mark emails. We did not assess the appropriateness of email markings from the two NNSA sites' classified email systems; however, we observed and senior officials confirmed that the classification marking tool's automatic feature at one NNSA site could result in improperly marking emails and potentially over classifying NSI. The requirements in 32 CFR Part 2001 indicate that emails containing classified NSI should be marked with proper classification markings while in the electronic environment, or if not practicable, a warning should be annotated to provide further guidance on the limited use of classified information contained in the email. Contrary to 32 CFR Part 2001, we noted that Department guidance, Department Order 471.6 and NNSA Policy Letter 70.4, did not specify that classified NSI emails required proper markings while in electronic format, but did when printed.

Senior officials told us that the Department faces a unique challenge of effectively protecting and implementing classification requirements for Restricted Data, Formerly Restricted Data and NSI in the electronic environment. The challenge is attributable to the differing requirements for protecting Restricted Data and NSI. NSI requires provisions, such as portion markings and automatic declassification, whereas RD is excluded from these provisions because it is classified under the Atomic Energy Act. As the Department deals with Restricted Data the majority of the time, certain classified email systems at the Department and NNSA sites were designed to protect such information. Despite the challenges, a senior program official indicated that emails should be marked appropriately while in the original electronic format, as information could be shared outside the organization. The senior program official also acknowledged that the process for marking emails could be improved.

Self-Inspection Program

We determined that the Department's Office of Classification had completed on-site evaluations, an element of its self-inspection program. However, responsible Headquarters Intelligence officials had not conducted the required classification biennial self-assessments and annual classification decision reviews. We noted that there are three elements of the self-inspection program – on-site evaluations, self-assessments and classification decision reviews. These elements are required to appropriately assess the effectiveness of the NSI program, including distribution of classification authorities, actions taken to correct previous assessment findings, and to identify and correct misclassification actions, as specified in Department Order 475.2A, *Identifying Classified Information*.

On-Site Evaluations

We determined that the Office of Classification had conducted the required on-site evaluations to independently assess the NSI program within individual Department and NNSA sites. In fact,

the on-site evaluation report for one NNSA site reviewed noted deficiencies concerning the site's insufficient sample of documents reviewed during the annual classification decision reviews. In particular, the Office of Classification found that the site only reviewed unclassified documents to ensure that such documents did not contain classified information, but did not include a sample of classified documents as required by Department Order 475.2A. Since that review, we noted that the site had taken corrective actions to incorporate a sample of classified documents during its annual reviews.

Self-Assessments

We noted that Headquarters Intelligence had used Assistance Visits conducted by the Office of Classification in July 2008 and November 2010, in lieu of completing the required biennial self-assessments. According to a senior program official, an Assistance Visit can be used as a form of self-assessment to assist Headquarters Intelligence in developing corrective actions to address concerns found during the review. However, we determined from the *Assistance Visit to the Department of Energy, Office of Intelligence and Counterintelligence* report, dated November 2010, and interviews with Headquarters officials that Headquarters Intelligence had not: (1) implemented corrective actions addressing the need to conduct biennial self-assessments noted during the previous July 2008 Assistance Visit; or (2) established oversight responsibilities, such as the performance of self-assessments and classification decision reviews at field intelligence elements. The assessment also identified classification marking errors in 27 percent of the classified documents reviewed. Such errors included improper annotation on the duration of protection, missing advisement on origin, and inadequate information on the sources used to make classification determinations.

When asked about the failure to perform self-assessments, a senior Headquarters Intelligence official told us that integrating quality control into its classification program through the use of technical subject matter experts and reviews of finished intelligence products containing authoritative analysis disseminated to Intelligence Community elements are forms of self-assessment. Although the quality assurance review of finished intelligence products appears to be a sound practice, we believe that Headquarters Intelligence officials are missing an opportunity to identify and correct deficiencies and strengthen processes necessary to protect NSI through the performance of the required assessments.

Classification Decision Reviews

Headquarters Intelligence had not conducted comprehensive classification decision reviews that encompassed a representative sample of classified NSI at Department Headquarters, as required by Department Order 475.2A. Specifically, we determined that Headquarters Intelligence classification officials only reviewed approximately 140 finished intelligence products during Fiscal Year (FY) 2012. We found that Headquarters Intelligence classification officials did not review emails and internal documents, despite the fact that 90 percent of the 5,737 derivative classifier decisions reported to the Information Security Oversight Office were attributable to emails.

In addition, we determined that annual classification decision reviews excluded field intelligence element activities. According to a Headquarters Intelligence program official, a classification decision review was conducted at one of two field intelligence sites that we reviewed, in conjunction with an Office of Classification on-site evaluation in March 2012. We also noted that this review was last performed in March 2012 even though it is required on an annual basis. Further, we found that as of March 2014, Headquarters Intelligence had not conducted a classification decision review at the other site that we reviewed, but had tentatively scheduled the review for FY 2015. The lack of annual classification decision reviews may have contributed to the classification marking errors identified during our review.

Classification Challenges

While we did not find instances in which formal challenges were handled inappropriately, we determined that 12 of 37 interviewed derivative classifiers responsible for ensuring the integrity and protection of classified information were not familiar with the requirements for making a formal challenge to external entities when they believe that information could be misclassified. [9] However, they were aware of their responsibility to reach out internally to their respective classification officers. In addition to derivative classifiers, individuals with security clearances may not be aware of the requirements for making a formal challenge. Executive Order 13526, *Classified National Security Information*, specifies that the Department must establish procedures to allow and encourage authorized holders of information to challenge the classification of information that is believed to be misclassified. These procedures ensure that, among other things, individuals are advised of their appeal rights outside the agency. Also, 32 CFR Part 2001 specifies that formal challenges must be made in writing and established response timeframes shall be met. Classification officials told us that even though the Department lacks procedures on formal challenges, informal challenges are generally encouraged in the Department to facilitate timely resolution.

During interviews, senior program officials stated that classification challenges occur infrequently at the Department. However, the senior official acknowledged that there is a need to clarify the process for making classification challenges and provide information on appeal rights to create an environment where people have the knowledge to raise concerns about information that could be misclassified.

CONTRIBUTING FACTORS AND POTENTIAL IMPACT

The classification related issues we observed occurred, in part, because of ineffective oversight of classification activities and inadequate training and guidance. We were told by a classification program official that oversight activities such as self-assessments and document decision reviews had not been completed at Headquarters Intelligence and field intelligence elements because Headquarters Intelligence officials had not allocated resources to do so.

[9] Formal challenges are those that are submitted in writing to the Office of Classification or Associate Administrator for Defense Nuclear Security, if submitted by NNSA personnel. Informal challenges, which are generally encouraged in the Department, rise up to the level of formal challenges when differences in views are not resolved at the program/field classification officer level.

Further, Headquarters Intelligence had not granted proper security clearances to local classification officers to allow accessibility to field intelligence element information enabling the performance of self-assessments and classification decision reviews. Further, interviews revealed and we confirmed that performance standards regarding classification duties had not been established for the majority of interviewed Federal derivative classifiers, although required by Executive Order 13526. Such performance standards could help ensure that operational and security requirements pertaining to classified NSI are satisfied.

Sufficiency of training and guidance on classification may have also contributed to the marking errors and other issues. We found that derivative classifiers' initial and refresher training materials at Headquarters and at the two sites reviewed focused on marking documents but not emails. We also found that the same derivative classifiers' training did not provide sufficient emphasis on marking working papers that contained classified NSI. Further, we noted that although the Department offers training covering the topic of marking classified working papers at Headquarters, derivative classifiers were not required to complete the training. We also found that while initial security briefings provided to individuals who are granted security clearances covered marking classified working papers, annual refresher security briefings did not.

In addition, Department and NNSA guidance pertaining to marking classified emails were not consistent with Federal requirements. In particular, the Federal guidance provides for marking emails in the electronic environment while the Department guidance only specifies the requirement for marking emails when printed. Additionally, derivative classifiers we interviewed were not familiar with all requirements for making a formal challenge regarding information that could be misclassified because the Department had not developed comprehensive training and guidance on that subject. For example, our review of training materials for derivative classifiers at one site specified the need to contact the local classification officer about challenges, but did not describe the process for making formal challenges outside the local classification office. In addition, we noted that reference materials available to other individuals with security clearances, such as annual security briefings and policies at Headquarters and the two NNSA sites, were not comprehensive. For instance, the procedures for making formal classification challenges, including appeal rights and established timeframes were not specified in the Department Order 475.2A and local policies at the two NNSA sites. Further, security briefings did not provide procedures or information regarding appeal rights outside of the Office of Classification or the local classification office.

Protecting NSI while sharing information as widely as possible presents a difficult challenge. Strikingly, the balance between these very important national priorities is difficult without effective oversight, training and well-developed guidance for those involved with classification of NSI. While the issues identified in this report are based on a judgmentally selected sample, they may, when considered in conjunction with deficiencies identified by the Office of Classification during its evaluations, be indicative of issues impacting NSI classification processes at Department and NNSA elements we did not specifically test. We have made a number of recommendations intended to assist the Department with improving program management and execution of its classified NSI program.

RECOMMENDATIONS

To address the challenges we identified in this report, we recommend that the Chief Health, Safety and Security Officer:

1. Update Department Order 475.2A to incorporate guidance on the process for formal classification challenges.

We also recommend that the Chief Health Safety and Security Officer, in coordination with the National Nuclear Security Administration, Office of the Chief Information Officer, Office of Intelligence and Counterintelligence, and Field Elements:

2. Ensure that the Department guidance is updated to make certain that emails containing classified NSI are properly marked while in the original electronic format;

3. Provide appropriate training and guidance on classification marking for working papers to assist derivative classifiers and others with security clearances in more effectively marking classified information;

4. Ensure that individuals with security clearances, including derivative classifiers, are trained and made aware of their responsibilities to make formal challenges;

5. Ensure that emails containing classified NSI are appropriately marked while in the original electronic format; and

6. Implement a process to hold derivative classifiers accountable for implementing NSI classification requirements, including marking of classified NSI documents and emails.

Further, we recommend that the Director, Office of Intelligence and Counterintelligence:

7. Ensure that self-assessments and document decision reviews are conducted at Headquarters Intelligence and field intelligence elements, as required.

MANAGEMENT AND INSPECTOR COMMENTS

Management concurred with the recommendations in the report, but raised concerns regarding the impact our recommendation would have on established processes for classifying and protecting Restricted Data and Formerly Restricted Data, and on the costs associated with implementing corrective actions resulting from the recommendations. Specifically, management expressed concerns with classified emails containing NSI in which the Federal requirement to fully mark the classification of each email is problematic because not all email users are derivative classifiers authorized to make final classification determinations. Management cited possible solutions of permitting all email users to be NSI derivative classifiers to ensure classified NSI emails are properly marked while in the original electronic format.

While we concur that corrective actions resulting from our recommendations should take into consideration impacts to existing processes, including those related to protecting Restricted Data and Formerly Restricted Data, appropriate guidance specific to classified NSI, including emails, should be provided to ensure consistent application of Federal NSI classification requirements. Also, in recognition of the implementation costs of properly marking classified NSI emails, Federal requirements permit classified NSI emails to exclude proper classification markings while in the electronic environment, provided that a warning on the limited use of the information is annotated on the email. Such option could potentially alleviate issues related to the possible management solution of permitting all email users to be derivative classifiers.

Overall, we found management's comments and planned corrective actions to be responsive to our report findings and recommendations. Management's formal comments were included in Appendix 6.

Appendix 1

INSPECTORS GENERAL COMMUNITY-WIDE FOCUS AREAS

	Inspection Focus Area	Disposition
1.	General Program Management	Program Management and Execution. We found that the Department of Energy (Department), in general, had established and implemented certain elements of the Federal classification requirements, including an annual process for validating special access programs to limit its number, as required by Executive Order 13526, *Classified National Security Information*. However, we found derivative classifiers were not familiar with the requirements for making a formal challenge for information that could be misclassified.
2.	Original Classification Authority	Program Execution. We found 14 individuals with Original Classification Authority (OCA), 5 with Top Secret OCA and 9 with Secret OCA, were appropriately delegated and reported to Information Security Oversight Office (ISOO).
3.	Original Classification and Marking	Program Execution. We determined that the last original classification determination, made in Fiscal Year (FY) 2008, was completed in accordance with Federal classification requirements.
4.	Derivative Classification and Marking	Program Execution. We determined that derivative classifiers appeared to have basic knowledge on classification. However, we noted that the derivative classifiers did not always appropriately apply classification marking requirements. Specifically, 65 percent of documents and emails reviewed contained classification marking errors.
5.	Self-Inspection	Program Management and Execution. As part of the Department's self-inspection program, we found that the Department's Office of Health, Safety and Security, Office of Classification had conducted an on-site evaluation at one of the reviewed National Nuclear Security Administration sites, to independently assess the effectiveness of the classification program. We noted that deficiencies were identified during the evaluation and that the site had taken corrective actions to address those deficiencies. However, we found that elements of the self-inspection program had not been fully implemented by responsible Office of Intelligence and Counterintelligence (Headquarters Intelligence) officials at Headquarters Intelligence and field intelligence elements.

	Inspection Focus Area	**Disposition**
6.	Reporting to ISOO	Program Execution. We found that the required reporting to ISOO such as delegations of OCA, statistical reports, accounting for costs, and self-inspections were submitted to ISOO. Further, we noted that the Department had no reportable incidents of security violations and improper declassification of information, as described in the self-inspection reports submitted to ISOO for FY 2012 and 2011. Also, we noted that the estimated total of derivative classifier decisions reported to ISOO was projected. We noted that ISOO permits the submission of these estimates.
7.	Security Education and Training	Program Management and Execution. We noted that the Department's policy incorporated the essential elements for establishing a formal security education and training program for individuals with security clearance, including derivative classifier training on familiarization to system of classification, derivative review process and use of classification guides, and marking mechanisms. The policy also provided for suspending OCA and derivative classifiers who fail to meet training requirements. Based on our review of training records, we determined that original classifiers and derivative classifiers had met the required training.
8.	Intelligence Component	Program Management and Execution. We found that the Intelligence Community-wide guidance and directives related to classification, such as Controlled Access Program Coordination Office Register and Manual, were incorporated in Headquarters Intelligence's derivative classifier training materials. We also noted that 20 of 21 derivative classifiers from Headquarters Intelligence and field intelligence elements had access to updated Intelligence-related policies and procedures. Based on interviews with derivative classifiers, we did not find common issues or concerns related to the Office of the Director of National Intelligence policies on controlled access information.

DOCUMENT REVIEW RESULTS

Table 1: Classification Error by Category

Department Element	Sample Size	Identified Classification Errors				Total Errors	Errors %
		Misclassified	Improper Declassification Instructions	Lack of Portion Markings	No Classification Block		
A	118	1	40	47	0	88	75%
		[Errors found in 29 documents and 59 emails]					
B	47	3	10	8	5	26	55%
		[Errors found in 7 documents and 19 emails]					
C	66	1	19	2	15	37	56%
		[Errors found in 29 documents and 8 emails]					
Totals:	231	5	69	57	20	151	65%

Source: Analysis of the Office of Inspector General document review as conducted on a sample basis. A single document or email may include multiple marking errors.

Appendix 3

SAMPLE OF A CLASSIFIED DOCUMENT

All contents below are unclassified. Markings are example purposes only.

SECRET — **Banner Marking**

(U) PORTION MARKING BOOKLET

(S) Portion marking is the assignment of classification and required caveats to each portion of a document.

(U) All NSI documents must be portion marked.

(C) Documents containing RD and/or FRD don't require portion marking. Portions of NSI documents containing FGI must so indicate.

Portion Marking

(U) Growth

This Chart contains information that is Confidential

Derivative Declassifier review required prior to declassification

Classified By: Joe Smith, Director, DOE,HS-91
Derived From: CG-APPLE-1, 9/16/01, DOE OC
Declassify On: 01/01/2019

Classification Block

SECRET — **Banner Marking**

Source: Office of Health, Safety and Security, Office of Classification, *DC Module E: Marking Mechanics for Derivative Classification,* March 2012.

Legend: U – Unclassified; S – Secret; C – Confidential; NSI – National Security Information; RD – Restricted Data; FRD – Formerly Restricted Data; FGI – Foreign Government Information

Appendix 4

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

The objective of this inspection was to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within the Department of Energy (Department); and identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within the Department.

SCOPE

Consistent with the Council of the Inspectors General on Integrity and Efficiency, *Standard User's Guide for Inspectors General Conducting Evaluations under Public Law 111-258, the "Reducing Over-Classification Act,"* our inspection focused on National Security Information pertaining to eight areas: (1) original classification authority; (2) general program management; (3) original classification and marking; (4) derivative classification and marking; (5) self-inspections; (6) reporting; (7) security education and training; and (8) intelligence component cross-cutting issues.

This performance-based inspection was performed from March 2013 through March 2014, at Department Headquarters in Washington, DC, the Nevada Field Office in Las Vegas, Nevada, and Sandia National Laboratories in Albuquerque, New Mexico. The inspection was conducted under Office of Inspector General Project Number S12IS013.

METHODOLOGY

To accomplish the inspection objective, we:

- Reviewed and analyzed Federal and Department regulations on classification.
- Interviewed Federal and Contractor officials, including classification officers, original classifiers, and derivative classifiers.
- Selected a judgmental sample totaling 231 documents and emails that were derivatively classified by selected derivative classifiers during the period from Fiscal Year 2012 through current, for each Department element. The sample was determined to reflect the relative size of the inspected element. Further, the sample consisted of documents and emails randomly selected during the course of the inspection.
- Obtained and reviewed original classification determinations made in the last 5 years.

We conducted this performance-based inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the inspection to obtain sufficient,

appropriate evidence to provide a reasonable basis for our conclusions and observations based on our inspection objective. We believe the evidence obtained provided a reasonable basis for our conclusions and observations based on our inspection objective. Accordingly, the inspection included tests of controls and compliance with laws and regulations to the extent necessary to satisfy the inspection objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection. Finally, we relied on computer-processed data, to some extent, to satisfy our objective. We confirmed the validity of such data, when appropriate, by conducting interviews and analyzing source documents.

An exit conference was waived by the Office of Health, Safety and Security, National Nuclear Security Administration, Office of Intelligence and Counterintelligence, and Office of the Chief Information Officer.

Appendix 5

RELATED REPORTS

Office of Inspector General Report

- Inspection Report on *Internal Controls over Accountable Classified Removable Electronic Media at Oak Ridge National Laboratory*, (INS-O-09-02, May 2009). The Department of Energy Office of Inspector General found that (1) a number of Secret//Restricted Data media had not been identified as Accountable Classified Removable Electronic Media (ACREM) and placed into a system of accountability; (2) other ACREM protections and controls were not implemented; and (3) other media devices were stored in a security area without an analysis of vulnerabilities. Several recommendations were made to the Manager, Oak Ridge Office, regarding improving controls over ACREM. Corrective actions had been taken to address the recommendations.

U.S. Government Accountability Office

- Report on *Managing Sensitive Information, Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System*, (GAO-06-785, June 2006). The Government Accountability Office found that an October 2005 shift in responsibility for classification oversight to the Office of Security Evaluations has created uncertainty about whether a high level of performance in oversight will be sustained. The Agency recommended that (1) the Department of Energy conduct a similar number of reviews, as it did before October 2005; (2) apply selection procedures that more randomly indentify classified documents for review; and (3) disclose the selection procedures in future classification inspection reports. Corrective actions had been taken to address the recommendations.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

March 10, 2014

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL
OFFICE OF THE INSPECTOR GENERAL (IG-1)

FROM: GLENN PODONSKY
CHIEF HEALTH, SAFETY AND SECURITY OFFICER
OFFICE OF HEALTH, SAFETY AND SECURITY

SUBJECT: COMMENTS FOR IG DRAFT INSPECTION REPORT on "Review of Controls over the Department's Classification of Information" (S12IS013)

Thank you for your work on the draft inspection report conducted during 2013 at selected sites, including Headquarters in Washington, District of Columbia; Sandia Field Office, and Sandia National Laboratories in Albuquerque, New Mexico; and Nevada Field Office in Las Vegas, Nevada, to assess whether the Department's management and execution of its classified National Security Information (NSI) program has been appropriately established and implemented. The draft inspection report concluded that certain aspects of the Department's NSI program could be improved.

The Department of Energy (DOE) has a critical mission in the Government, that of protecting the Nation's nuclear weapons-related information. The importance of this task led Congress to pass the Atomic Energy Act giving the Atomic Energy Commission the sole responsibility for the classification of this information. Since that time, the predecessor agencies to the DOE and the DOE have developed a unique classification system that ensures that trained subject matter experts with written authority (Derivative Classifiers) use classification guidance to make classification determinations and the declassification of classified documents is performed by not just one, but two subject matter experts with appropriate authority. These rigorous standards, which exceed those for NSI, have not only ensured the protection of nuclear weapons-related information but also prevent the declassification of sensitive documents and over-classification. These requirements have served the Department well for many years, and numerous inspections attest to the quality of classification decisions made by DOE reviewers. Any analysis of the DOE classification program must consider the impact of requirements for Restricted Data (RD) and Formerly Restricted Data (FRD). The subject inspection report addresses only NSI based on Executive Order (E.O.) 13526. Subsequent corrective actions must take into consideration the long established and proven processes established to classify and protect RD and FRD. This is particularly important in the case of classified emails containing NSI where the E.O. requirement to fully mark the classification of each email is problematic because not all email users are Derivative Classifiers, authorized to make final classification determinations. Potential solutions such as permitting all email users to be DCs for NSI will require extensive coordination among several offices and may

1

require policy changes. The cost of change and the potential to degrade the existing classification program for RD and FRD information must be considered.

The draft report contains seven recommendations. DOE concurs with the all of the recommendations.

Office of Health, Safety and Security Response

Recommendation 1: Update the Department Order 475.2A, *Identifying Classified Information* to incorporate guidance on the process for formal classification challenges.

Management Decision: DOE concurs. DOE is in the process of updating DOE Order 475.2A to consolidate national requirements from 10 CFR Part 1045, *Nuclear Classification and Declassification*, and 32 CFR 2001, *Classified National Security Information: Final Rule*, on procedures for submitting formal classification challenges.

Action Plan:

- Obtain permission from the Directives Review Board to revise DOE Order 475.2A—March 2014
- Submit revised order to RevCom—June 2014
- Complete RevCom Process—September 2014

Estimated Completion Date: September 30, 2014

Recommendation 2: Ensure that the Department guidance is updated to make certain that emails containing classified NSI are properly marked while in the original electronic format.

Management Decision: DOE concurs. While the requirements in 32 CFR 2001 regarding marking in the electronic environment are clear, DOE recognizes that these requirements have not been fully implemented and additional guidance is necessary.

Action Plan: Working with the Office of the Chief Information Officer, the Office of Security Policy will lead the effort to develop and issue DOE-specific guidance concerning marking in the electronic environment.

- Complete the guidance in draft – June 2014
- Complete final version – September 2014

Estimated Completion Date: September 30, 2014

Recommendation 3: Provide appropriate training and guidance on classification marking for working papers to assist derivative classifiers and others with security clearances in more effectively marking classified information;

Management Decision: DOE concurs. The requirements in DOE Order 471.6 are clear. Local managers, who are responsible for tailoring security training to their specific needs, must incorporate the use and marking of working papers into their training and implementation based on the results of required self-assessments of their respective programs.

Action Plan: The Senior Agency Official (SAO) will send a reminder memorandum to Program Secretarial Offices (PSOs) that programs must provide training, guidance, and oversight, as appropriate to ensure working papers are properly marked.

Estimated Completion Date: May 30, 2014

Recommendation 4: Ensure that individuals with security clearances, including derivative classifiers, are trained and made aware of their responsibilities to make formal challenges;

Management Decision: DOE concurs. As noted in Recommendation 1, DOE Order 475.2A will be modified to ensure that all individuals understand that they are expected and encouraged to make challenges, when necessary.

Action Plan: To ensure awareness and implementation of revisions to the Order regarding classification challenges, the SAO will send a reminder memorandum PSOs that programs must provide training and guidance to ensure employees are expected and encouraged to make formal challenges.

Estimated Completion Date: October 30, 2014

Recommendation 5: Ensure that emails containing classified NSI are appropriately marked while in the original electronic format.

Management Decision: DOE concurs. The implementation of national policy is the responsibility of program offices. A memorandum from the SAO reminding programs of the requirement to mark classified NSI email in accordance with 32 CFR 2001.23 will begin to address the issue. Offices will have to assess the financial impact of implementing solutions and consider potential revisions to current policies.

Action Plan: The SAO will send a memorandum to Program Secretarial Offices (PSOs) that all email potentially containing classified NSI must be reviewed by a DC and when classified must be marked in accordance with 32 CFR 2001.23. The memorandum will also state that self-assessments must include a review of classified NSI email to ensure it is properly reviewed and marked.

Estimated Completion Date: May 30, 2014

Recommendation 6: Implement a process to hold derivative classifiers accountable for implementing NSI classification requirements, including marking of classified NSI documents and emails.

Management Decision: DOE concurs. There are currently several requirements holding DCs accountable for proper classification. The performance plans for Federal DCs must include classification as an element for DCs who make a significant number of classification determinations annually (DOE Order 475.2A, 5f(12)). In addition, DC authority must be terminated by the appointing official if the authority is not exercised reliably (DOE Order 475.2A, Attachment 2, 2e(8)). The Order further states (Attachment 4, Paragraph 4) that any knowing, willful, or negligent action that results in the misclassification of information, documents, or material may result in termination of the classification official's authority. Additional consequences such as disciplinary action or the issuance of a security infraction may result in accordance with other DOE directives. The Heads of Elements and appointing officials are responsible for determining the process to ensure these requirements are met. Although DCs must be held accountable, DOE cautions that aggressive questioning or penalizing DCs for good faith classification determinations based on guidance would result in fewer personnel fulfilling this role, which would risk degradation of the DOE classification program.

DOE recognizes that requirements concerning marking in the electronic environment are not fully implemented. DOE also recognizes that further guidance is necessary. Regardless, 32 CFR 2001.23 provides sufficient guidance to mark email containing NSI.

Action Plan: The SAO will send a reminder memorandum to PSOs that programs must hold DCs accountable for the proper classification and marking of classified documents in accordance with national and DOE policies and that requirements for marking email containing NSI are contained in 32 CFR 2001.23. The memorandum will also include a reminder that the performance contract used to rate Federal personnel whose duties significantly involve the creation of classified documents must include the designation of classified information as a critical element in order to ensure DCs are held accountable.

Estimated Completion Date: October 30, 2014

Office of Intelligence and Counterintelligence Response

Recommendation 7: The Director, Office of Intelligence and Counterintelligence, should ensure that self-assessments and document decision reviews are conducted at Headquarters and at field intelligence elements, as required;

Management Decision: Concur. The Office of Intelligence and Counterintelligence agrees with the recommendation and will seek ways to expand the number of self-assessments and document decision reviews conducted.

Action Plan: DOE-IN will reconsider longstanding proposals to approve SCI access for Federal classification officers in the field, balancing the necessary access with legitimate security considerations. DOE-IN will also review how we might establish a process that

4

reduces the amount of time spent on each self-assessment and field-training event, and will look for ways to increase the number of sites undergoing review or self-assessment in any given year. DOE-IN expects to develop and begin implementing a plan NLT September 30, 2014. Satisfactory achievement of these goals is likely to take longer, but implementation of a remediation plan will begin by the end of FY2014.

Estimated Completion Date: September 30, 2014

IG Report No. DOE/IG-0904

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message clearer to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report that would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact our office at (202) 253-2162.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://energy.gov/ig

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.