OFFICE OF
THE INSPECTOR GENERAL

U.S. NUCLEAR
REGULATORY COMMISSION

Review of NRC's Handling and Marking of Sensitive Unclassified Information

OIG-03-A-01 October 16, 2002

AUDIT REPORT

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

October 16, 2002

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum/**RA**/
Assistant Inspector General for Audits

SUBJECT: REVIEW OF NRC'S HANDLING AND MARKING OF SENSITIVE UNCLASSIFIED INFORMATION (OIG-03-A-01)

Attached is the Office of the Inspector General's audit report titled, *Review of NRC's Handling and Marking of Sensitive Unclassified Information*.

This report reflects the results of our review to assess NRC's program for handling and marking sensitive unclassified information. NRC has a program and guidance for the handling and marking of sensitive unclassified information; however, the guidance may not adequately protect Official Use Only information, a category of sensitive unclassified information, from inadvertent public disclosure. Training on handling and protecting sensitive unclassified information is not provided to all NRC employees and contractors on a regular basis. Consequently, staff members are not knowledgeable of NRC's requirements and guidance for sensitive unclassified information. In addition, NRC employees are not consistently implementing the requirements to report incidents of inadvertent releases of sensitive unclassified information to the EDO, a practice that would allow for the identification of a systemic problems and the application of best practices agency-wide.

At an exit conference held on September 24, 2002, NRC officials generally agreed with the report's findings and recommendations. The comments provided at the exit meeting have been incorporated into the report where appropriate.

If you have any questions, please contact Russ Irish at 415-5972 or me at 415-5915.

Attachment: As stated

cc: John Craig, OEDO

R. McOsker, OCM/RAM
B. Torres, ACMUI
G. Hornberger, ACNW
G. Apostolakis, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, OCAA
S. Reiter, CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
W. Kane, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
M. Springer, ADM
R. Borchardt, NRR
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
M. Virgilio, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, STP
F. Congel, OE
M. Federline, NMSS
R. Zimmerman, NSIR
J. Johnson, NRR
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

EXECUTIVE SUMMARY

BACKGROUND

The Office of the Inspector General (OIG) received a congressional request to review the adequacy of the United States Nuclear Regulatory Commission's (NRC) programs for handling and releasing sensitive documents after a preliminary draft of the Yucca Mountain Review Plan was inadvertently released to the public in September 2000. The draft of the Yucca Mountain Review Plan provided guidance on evaluating a license application for a geological repository for spent nuclear fuel. The Commissioners disapproved a request to make the plan publicly available until some of the information was updated, making the plan a predecisional document. As a predecisional document, the draft of the Yucca Mountain Review Plan is an Official Use Only document and should have been treated as sensitive unclassified information protected from public disclosure until Commission approval was granted.

Official Use Only information is one category of sensitive unclassified information[1] that includes predecisional documents and information protected from public disclosure until certain conditions are met. While most of NRC's documents are released to the public, NRC has a program to prevent the public release of sensitive unclassified information.

PURPOSE

The objective of this review was to assess NRC's program for the handling, marking and protecting of Official Use Only information.

RESULTS IN BRIEF

NRC has a program and guidance for the protection and handling of sensitive unclassified information. However, the guidance does not adequately protect Official Use Only documents from inadvertent public disclosure. Specifically, the use of cover sheets with Official Use Only information is left up to the discretion of the document originator. The individual pages of documents are not always marked and are vulnerable to public disclosure if separated from the cover sheet. In addition, consistent markings are not being used on the sensitive unclassified documents that are marked, adding to the confusion surrounding the proper marking and handling of sensitive unclassified information. OIG will initiate a follow-on audit concerning the protection of Safeguards information.

[1]Sensitive Unclassified Information includes Official Use Only information, Proprietary information, and Safeguards information.

Training on handling, marking and protecting sensitive unclassified information is not provided to all NRC employees and contractors on a regular basis. Consequently, many of the staff are not knowledgeable about NRC's requirements and guidance in this area.

NRC employees are not consistently implementing the requirement to report incidents of inadvertent release of sensitive unclassified information to the Office of the Executive Director for Operations, a practice that would allow for the identification of systemic problems and the application of best practices agency-wide.

RECOMMENDATIONS

This report makes four recommendations to the Executive Director for Operations to enhance the handling, marking, and protection of sensitive unclassified information.

ABBREVIATIONS AND ACRONYMS

ADAMS	Agency-wide Documents Access and Management System
DFS	Division of Facilities and Security
DOE	Department of Energy
MD 3.4	Management Directive and Handbook 3.4
MD 12.6	Management Directive and Handbook 12.6
NRC	United States Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response
NUREG	NRC Technical Report Designation (Nuclear Regulatory Commission)
OCIO	Office of the Chief Information Officer
OEDO	Office of the Executive Director for Operations
OIG	Office of the Inspector General

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

On October 25, 2001, Senator Reid from the Senate Subcommittee on Transportation, Infrastructure, and Nuclear Safety requested that the OIG investigate the means by which a Yucca Mountain Licensing Review Plan draft was improperly obtained by the Department of Energy (DOE) and the law firm of Winston & Strawn. At the time, Winston & Strawn was the firm holding the contract with DOE for legal representation for licensing Yucca Mountain as a high-level nuclear waste repository. The preliminary draft of the Yucca Mountain Review Plan provides guidance on evaluating a license application for a geological repository for spent nuclear fuel. NRC staff recommended the draft plan be released to the public; however, the Commissioners disapproved the request until some of the information was updated. As an Official Use Only predecisional document, the draft plan should have been treated as sensitive unclassified information protected from public disclosure until approval was provided by the Commission.

OIG initiated an investigation and reported its findings to Senator Reid on February 16, 2002.[2] The report stated that NRC has programs intended to ensure that sensitive documents are handled properly and are not released inappropriately. However, this event may have demonstrated a weakness within the agency programs. The Inspector General stated that he would review the adequacy of the NRC programs for handling and releasing sensitive documents.

NRC's Program for Handling and Releasing Sensitive Unclassified Information

NRC has established the Sensitive Unclassified Information Security Program to ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure under pertinent laws, management directives, and applicable directives of other Federal agencies and organizations. A comprehensive body of guidance and information exists in NRC Management Directives, on the NRC internet, and in various NRC Technical Report Designations (NUREG). The principle directives include Management Directive and Handbook 3.4 (MD 3.4), *Release of Information to the Public,* and Management Directive and Handbook 12.6 (MD 12.6), *NRC Sensitive Unclassified Information Security Program.* The latter provides methods for inserting documents in the Agency-wide Documents Access and Management System (ADAMS).[3]

[2]Letter from Hubert T. Bell, NRC Inspector General, to Senator Harry Reid, February 16, 2002.

[3]ADAMS is the NRC's electronic record keeping system that maintains the official records of the agency. ADAMS is also NRC's public information dissemination system that places publicly available records on the NRC's Public Web Server.

MD 12.6 provides the requirements and procedures for ensuring sensitive unclassified information is adequately identified and protected from unauthorized disclosure. It includes procedures for marking the pages of the document with the type of sensitive information included, guidance for handling information originated by sources outside the NRC, and security preparations required for hearings, conferences, or discussions.

The importance of protecting sensitive unclassified information from public disclosure is highlighted in sections of MD 3.4:

> In the normal course of conducting regulatory activities NRC employees deal with many forms of sensitive information that either should not be released to members of the public or should not be released prematurely. Premature or unauthorized release of this information can jeopardize NRC agency actions, lead to diminished respect for this agency, and a loss of credibility with the public and other Federal agencies. Releases of privacy or proprietary information can violate the Privacy Act, the Trade Secrets Act, or the Standards of Conduct.

Because NRC's intent is to make as much information publicly available as possible, MD 3.4 provides guidance on the public release of agency information including draft and predecisional documents and information. MD 3.4 details the information requiring approval before release, information not routinely released, NRC policy and guidance regarding sensitive information, and a table of NRC documents routinely released to the public.

MD 3.4 states that in the event any document is inadvertently or otherwise released by the NRC, its contractors, or other Government agencies contrary to this policy, the Office of the Executive Director for Operations (OEDO) should be advised promptly of the occurrence in writing. In the case of an inadvertent release by NRC, the corrective action to be taken by the responsible office to avoid recurrence of such a release should also be communicated to the OEDO.

Prior Audit Findings

OIG found NRC's guidance and policies on sensitive information to be scattered among at least 38 management directives, manuals, and other resources. A previous OIG audit report[4] identified that this guidance was not cross-referenced or indexed. In response to that report, OCIO agreed to review functional directives and ensure they are adequately cross-referenced to MD 3.4. In fact, this action was taken in MD 3.4, Exhibit 2, *NRC Policy and Guidance Regarding Sensitive Information.*

[4]OIG/98A-16, *Review of NRC's Controls to Prevent the Inadvertent Release of Sensitive Information*, February 3, 1999.

Official Use Only Information

Official Use Only information includes personnel records, privacy data, investigative reports, and predecisional or internal NRC data. This category of information requires special handling to ensure only limited internal distribution and no disclosure to the public. Some Official Use Only information is intended to be released to the public after particular conditions have been met such as official approval or signature of the document. These documents are subject to conditional release and should be protected as Official Use Only until the condition has been met. The preliminary draft of the Yucca Mountain Review Plan fell into this category of predecisional documents.

In accordance with MD 3.4, predecisional documents are included among the information that requires approval before it can be released to the public. NRC staff must not discuss, give to, or show draft documents or information contained in predecisional documents to any licensee or the public without prior approval. It is very important that predecisional or draft documents be identified as such so that the holder of the information will be aware of the need not to disclose the information.

II. PURPOSE

The objective of this review was to assess NRC's program for the handling, marking and protecting of Official Use Only information.

III. FINDINGS

Official Use Only information is not adequately protected against inadvertent public disclosure. Specifically: 1) guidance for Official Use Only information is inadequate and does not sufficiently protect the information from public disclosure, 2) periodic training on the handling of sensitive unclassified information has not been consistently provided agency-wide, and 3) all inadvertent releases of sensitive unclassified information to the public are not reported to the OEDO.

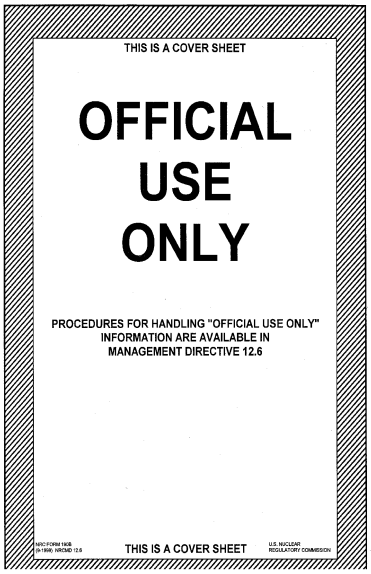
OIG understands that the implementation of a system that ensures no inadvertent releases of sensitive information occur is cost prohibitive and resource intensive. However, there are opportunities to improve the system and everyone's awareness of the handling of Official Use Only and other sensitive unclassified information.

A. GUIDANCE NEEDS IMPROVEMENT

The guidance for marking and using cover sheets with Official Use Only sensitive unclassified information may not adequately protect the information from public disclosure because the use of cover sheets is discretionary and the need to mark is left to the judgement of the originator. The lack of markings and cover sheets on Official Use Only information keeps readers from being alert to the sensitive nature of Official Use Only information and raises the chance of inadvertently releasing Official Use Only information to the public.

Guidance Does Not Adequately Protect Information From Disclosure

The use of cover sheets for Official Use Only documents identifying the type of information included in the document is discretionary. MD 12.6 does not require the use of a cover sheet for Official Use Only information, increasing a document's chance to be inappropriately released. Cover sheets for Official Use Only documents should be used "when their use facilitates identification or protection of the information." In addition, cover sheets may be used to identify and protect information that may be released to the public when certain conditions have been met. The internal web site for the Office of Administration's Division of Facilities and Security states that cover sheets should be used for Official Use Only to safeguard unclassified information exempted from public disclosure under the Freedom of information Act or the Privacy Act. A cover sheet acts as an attention grabbing device that lets a person know to protect the information in their possession from inappropriate disclosure.



Official Use Only Information Cover Sheet

According to a senior OEDO official, NRC implements a tiered approach to markings and protection of classified and sensitive unclassified information to avoid inadvertent disclosures. For example, classified national security information is marked in accordance with Executive Order 12958[5] to alert recipients about its sensitivity. The overall marking for national security information should be placed conspicuously at the top and bottom of the front cover, title page, first page and on the outside of the back cover. Internal pages should be marked with the overall

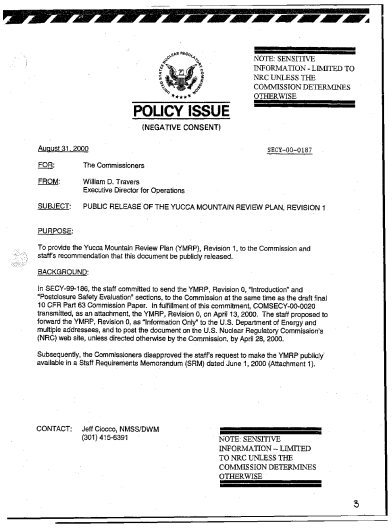
[5]Executive Order 12958, (*Classified National Security Information*), prescribes a uniform system for marking, classifying, safeguarding, and declassifying national security information.

classification or with a marking indicating the highest level of information contained on that page. While there are no Executive Orders requiring the use of markings on sensitive unclassified information, readers of sensitive unclassified information need to be alert to the necessity of protecting the information from inadvertent public disclosure.

In accordance with MD 12.6, a document that contains Official Use Only information must be marked when the originator believes the marking is essential to ensure proper handling and to ensure persons having access to the record will be aware that the document must not be publicly released. The guidance allows the originator to determine when documents containing Official Use Only information should be marked to prevent public disclosure and to restrict distribution. The originator of Official Use Only documents has the option of placing a cover sheet on a document containing such information in lieu of marking it.

Methods of Marking Documents Not Adequate

When marking is included on a document, the placement of the marking may not adequately protect the document from an inappropriate disclosure. The draft Yucca Mountain Review Plan was marked by the originator in accordance with the guidance. The transmittal memorandum was marked at the top and bottom with the statement "SENSITIVE INFORMATION - LIMITED TO NRC UNLESS THE COMMISSION DETERMINES OTHERWISE". The pages of the Review Plan itself were not marked nor was a DRAFT watermark included on the document. As shown by the following examples, once the transmittal memo is removed the document loses all of the markings that were designed to protect it.



NOTE: SENSITIVE INFORMATION - LIMITED TO NRC UNLESS THE COMMISSION DETERMINES OTHERWISE

POLICY ISSUE
(NEGATIVE CONSENT)

August 31, 2000 SECY-00-0187

FOR: The Commissioners

FROM: William D. Travers
Executive Director for Operations

SUBJECT: PUBLIC RELEASE OF THE YUCCA MOUNTAIN REVIEW PLAN, REVISION 1

PURPOSE:

To provide the Yucca Mountain Review Plan (YMRP), Revision 1, to the Commission and staff's recommendation that this document be publicly released.

BACKGROUND:

In SECY-99-190, the staff committed to send the YMRP, Revision 0, "Introduction" and "Postclosure Safety Evaluation" sections, to the Commission at the same time as the draft final 10 CFR Part 63 Commission Paper. In fulfillment of this commitment, COMSECY-00-0020 transmitted, as an attachment, the YMRP, Revision 0, on April 13, 2000. The staff proposed to forward the YMRP, Revision 0, as "Information Only" to the U.S. Department of Energy and multiple addressees, and to post the document on the U.S. Nuclear Regulatory Commission's (NRC) web site, unless directed otherwise by the Commission, by April 28, 2000.

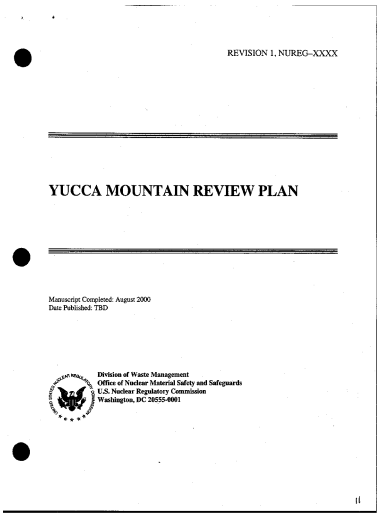
Subsequently, the Commissioners disapproved the staff's request to make the YMRP publicly available in a Staff Requirements Memorandum (SRM) dated June 1, 2000 (Attachment 1).

CONTACT: Jeff Cocco, NMSS/DWM
(301) 415-6391

NOTE: SENSITIVE INFORMATION – LIMITED TO NRC UNLESS THE COMMISSION DETERMINES OTHERWISE

3

Transmittal Memo



REVISION 1, NUREG–XXXX

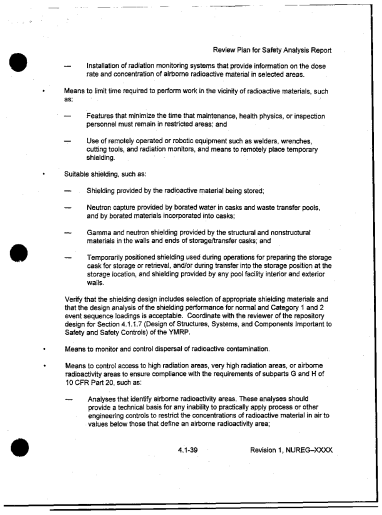
YUCCA MOUNTAIN REVIEW PLAN

Manuscript Completed: August 2000
Date Published: TBD

Division of Waste Management
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

ii

Title Page



Review Plan for Safety Analysis Report

— Installation of radiation monitoring systems that provide information on the dose rate and concentration of airborne radioactive material in selected areas.

- Means to limit time required to perform work in the vicinity of radioactive materials, such as:
  - Features that minimize the time that maintenance, health physics, or inspection personnel must remain in restricted areas; and
  - Use of remotely operated or robotic equipment such as welders, wrenches, cutting tools, and radiation monitors, and means to remotely place temporary shielding.
- Suitable shielding, such as:
  - Shielding provided by the radioactive material being stored;
  - Neutron capture provided by borated water in casks and waste transfer pools, and by borated materials incorporated into casks;
  - Gamma and neutron shielding provided by the structural and nonstructural materials in the walls and ends of storage/transfer casks; and
  - Temporarily positioned shielding used during operations for preparing the storage cask for storage or retrieval, and/or during transfer into the storage position at the storage location, and shielding provided by any pool facility interior and exterior walls.

Verify that the shielding design includes selection of appropriate shielding materials and that the design analysis of the shielding performance for normal and Category 1 and 2 event sequence loadings is acceptable. Coordinate with the reviewer of the repository design for Section 4.1.1.7 (Design of Structures, Systems, and Components Important to Safety and Safety Controls) of the YMRP.

- Means to monitor and control dispersal of radioactive contamination.
- Means to control access to high radiation areas, very high radiation areas, or airborne radioactivity areas to ensure compliance with the requirements of subparts G and H of 10 CFR Part 20, such as:
  - Analyses that identify airborne radioactivity areas. These analyses should provide a technical basis for any inability to practically apply process or other engineering controls to restrict the concentrations of radioactive material in air to values below those that define an airborne radioactivity area;

4.1-39 Revision 1, NUREG–XXXX

Page from Review Plan

Originators should place the marking "OFFICIAL USE ONLY" at the top and bottom of the first page of each document containing Official Use Only information when that marking is required to ensure proper handling. The marking "LIMITED INTERNAL DISTRIBUTION PERMITTED" must be placed in the lower left corner of the first page of the document. Requirements for multiple page documents state that markings must be placed at the top and bottom of:

- The outside of the front and back covers, if any
- The title page, if any
- The first page of text, if there is no front cover or title page
- The outside of the back page, if there is no back cover
- Each page of a document containing sensitive unclassified information

Multiple page documents can easily be separated from their covers and title pages. In addition, the pages of multiple page documents containing markings can easily be missed by readers and be inadvertently released if all of the pages are not marked.

Consistency of the Markings

To further clarify the marking and handling of Official Use Only information, a consistent set of markings should be used on documents containing Official Use Only information. MD 12.6 provides marking instructions; however, various markings are used throughout NRC. Guidance requires the originator to place the category of sensitive unclassified information on the top and bottom of the page, and a disclaimer in the lower left corner on the face of the document. For Official Use Only information the markings "OFFICIAL USE ONLY" and "LIMITED INTERNAL DISTRIBUTION PERMITTED" may be placed on the document in accordance with MD 12.6. However, markings such as "For Information Only", "OFFICIAL USE ONLY NOT FOR PUBLIC RELEASE", and "SENSITIVE INFORMATION - LIMITED TO NRC UNLESS THE COMMISSION DETERMINES OTHERWISE" have been included on NRC documents containing sensitive unclassified information. Consistent use of defined markings will make people aware of protection that should be provided to documents containing sensitive unclassified information and protect against improper disclosure.

Summary

Guidance on the use of cover sheets and markings which "merely catch the reader's attention" may not adequately protect Official Use Only information from inadvertent public disclosure. In addition, markings for Official Use Only documents can easily be missed by readers if all of the pages are not marked and may not provide adequate protection from inadvertent public or other improper release of sensitive unclassified information. Consistent use of defined markings would also assist with the protection of sensitive unclassified information from inadvertent public release and other improper disclosure.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

1. Update the guidance for Official Use Only documents to require clear identification of sensitive unclassified information to prevent its inadvertent disclosure.

2. Mandate consistent use of defined markings on documents containing Official Use Only information and clarify the markings that should be used on sensitive unclassified information.

B. LACK OF REGULAR TRAINING

Regular training on the marking and handling of sensitive unclassified information is not provided to NRC employees and contractors to instill an awareness of the definition of sensitive unclassified information and how to protect it against public disclosure. In fact, there is no criteria to provide such training and no government-wide program for sensitive unclassified information. Given the number of disclosures of sensitive unclassified information and the increase in the type of information that is now considered sensitive unclassified information, there is a need for regular training to enhance NRC employees' knowledge and protect against inadvertent releases of sensitive unclassified information.

Employees from the Office of Nuclear Security and Incident Response (NSIR) and the Division of Facilities and Security (DFS) have provided briefings or briefing materials on the protection of sensitive unclassified and classified information to NRC offices based on individual requests. The number of requests for the awareness briefings has increased since the terrorist acts of September 11, 2001. DFS has provided briefings on the protection of classified and sensitive unclassified information at the NRC Regional Offices over the past few years. These briefings were held at times when all Resident Inspectors and other staff were in attendance at the NRC Regional Offices for other scheduled training. In addition, informal training has been provided through staff meetings and discussions after information has been inadvertently released to the public.

Briefings on the protection of *classified* information are provided to new employees during their orientation on the first day of employment with the NRC. The information is provided once again when the security clearance process is completed and the employee is given a permanent identification badge. At this

time the employee will sign Standard Form 312, the Classified Information Nondisclosure Agreement. After these two offerings, no further training is offered.

Training is not provided on a regular basis because of the lack of a requirement that the instruction take place. DFS used to provide security awareness briefings periodically to all NRC employees and utilized other outlets to heighten the awareness of NRC staff including the Security Newsletter, the Security Advisory Program and Posters. In the past, NRC had a low attrition rate and classified information training was concentrated in certain areas. It is recognized by DFS and NSIR officials that there is a current need for training because of the increased number of new employees as well as the increased number of staff handling sensitive and classified information. DFS has received requests for security awareness briefings and they are reinstituting the briefings.

In an agency such as the NRC, which releases a large number of documents to the public, the lack of training can result in decreased awareness of the type of information that should not be disclosed.

Examples of Inadvertent Releases

Examples of inadvertent releases of sensitive unclassified information provided to the OIG included the release of predecisional documents, privacy information included in license documents, and sensitive information included in attachments to documents. While there were situations where the submitter mistakenly profiled the document for public release, the remaining cases were the result of a lack of knowledge about the sensitively of the information and the need for non-disclosure.

Two of the incidents reported to the OEDO did not involve the release of documents to the public, but rather they involved the oral release of sensitive information. These incidents indicate that the need for security awareness training goes beyond the preparation and profiling of documents. This is particularly true with Sensitive Homeland Security Information, a class of information that was previously not considered sensitive but has now been determined to be of a nature to assist potential terrorists and has been removed from the public domain.

Prior Recommendations for Training

Both the OIG and NRC staff have made recommendations regarding the need for training in this area in the past.[6] OIG recommended training for employees on a regular basis because the OIG found that inadvertent releases of sensitive information may be attributed to the varying levels of staff awareness and training on applicable guidance. Auditors found that the cause of inadvertent releases was a lack of awareness by some staff members of the appropriate way to handle sensitive unclassified information. The OCIO responded that agency personnel receive a wide variety of training on protecting sensitive unclassified information, but they would ask all offices to identify needs for increased awareness and training and take appropriate action to ensure it is accomplished. A task force report on an ADAMS inadvertent release recommended the development and implementation of staff training specific to document classification because they found inadequate staff knowledge of classifying documents. One root cause identified was inadequate staff knowledge due to training that focused on software implementation rather than how to classify documents.

Computer Security Awareness Training

The Computer Security Awareness Course is the only annual exposure most NRC employees and contractors receive on the handling of sensitive unclassified information. However, the coverage is specific to handling and protecting sensitive information in an electronic environment in an effort to meet the requirements of the Computer Security Act. Provisions in Office of Management and Budget Circular No. A-130, *Management of Federal Information Resources,* states individuals should have periodic refresher training to assure continued understanding and to abide by the applicable rules because "...over time, attention to security tends to dissipate". The same can be said for the need to provide awareness training focused on the protection of information. It would be prudent for the agency to provide training to continually reinforce and build upon the staff's awareness for the need to handle information appropriately.

ADAMS Training Is In Development

OCIO is developing online training to explain how ADAMS is to be used for daily work assignments. The introduction states that participants will learn how to profile and submit documents to ADAMS using NRC Form 665 and will learn the

[6] OIG/98A-16, *Review of NRC's Controls to Prevent the Inadvertent Release of Sensitive Information*, February 3, 1999, and *Root Cause Analysis Task Force on Agency-wide Documents Access and Management System (ADAMS) Inadvertent Release of Documents to the Public*, Task Force Report for the Executive Director for Operations, September 24, 2001.

impact of this form in protecting sensitive documents or releasing documents to the public. With the proliferation of e-mail, telephone conversations, and faxes, it is imperative that every NRC staff member is able to correctly identify a document that must be preserved as an official agency record. The training will be required and is good for building a greater awareness of preparing documents for public release in ADAMS.

One section of the training module explains the importance of determining if a document is sensitive, who should have access rights to the document, and if not sensitive, should the document be released to the public. Definitions of sensitive information from MD 12.6 have been included in the training package along with hyperlinks to the exact text. Document originators and managers are encouraged to read MDs 12.6 and 3.4 before making or confirming decisions about document sensitivity and public availability.

Like the Computer Security Awareness Course, the purpose of this training is not to cover the mechanics of marking and handling sensitive unclassified information. However, it does impress upon staff the need to give consideration to the guidance and whether or not documents should be released to the public.

Summary

Guidance for sensitive unclassified information exists in the Management Directives, the NRC intranet, NUREGs and NRC Yellow Announcements. The DFS Home Page includes information in a user-friendly manner on the procedures for using cover sheets, marking data, and storing sensitive unclassified information. The intranet also includes guidelines for submitting documents to ADAMS from Headquarters and the Regional Offices. The passive nature of the Management Directives, the intranet and NUREGs require staff to be aware of the existence of the information and cognizant of the need to implement the procedures. These methods are best used hand-in-hand with training sessions by providing NRC staff with resources for the information learned in the training sessions.

With the exception of the briefings for new hires, NRC lacks a systemic information security training program for existing NRC employees and contractors. While the number of inadvertent releases compared to the number of documents publicly released is small, incidents occur which can jeopardize NRC agency actions, lead to diminished respect for the Agency, and lead to a loss of credibility with the public and other Federal Agencies. With the number of incidents and people handling sensitive unclassified information increasing there is a need for annual training to prevent security awareness from diminishing over time.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

3. Conduct annual mandatory training for all NRC employees and contractors on the procedures for marking and handling sensitive unclassified information.

C. INADVERTENT RELEASES NOT REPORTED TO OEDO

All incidents of inadvertent releases have not been reported to the OEDO as required by MD 3.4. Thirteen releases were reported to the OEDO from July 2000 through August 2002. However, OCIO staff recorded that 127 ADAMS accession numbers were released due to mislabeling or other inadvertent circumstances in the years 2000 and 2001. Accession numbers identify individual files stored in ADAMS but each file is not necessarily an individual document and could consist of a package of documents. While it was not determined whether any of the 127 releases reported by OCIO were included in the thirteen reports to the OEDO, such a disparity could result in the inability to properly track the inadvertent release of sensitive unclassified information.

Neither OEDO nor OCIO were able to explain the reason for the difference in the 127 releases recorded by OCIO and 13 reports provided to the OEDO. OEDO stated that each report may represent the inadvertent release of several documents. Only one report mentioned the fact that more than one document was removed from the ADAMS public library. Therefore, this is not the apparent cause for the difference in the reported inadvertent releases of sensitive unclassified information. OCIO stated they do not report to the OEDO instances when they are asked to remove sensitive unclassified information inadvertently released to the ADAMS public library. MD Handbook 3.4 requires that the office that inadvertently released the information report the incident to the OEDO. This situation represents the lack of awareness to report such incidents to OEDO.

MD 3.4 requires each office that had an inadvertent release to not only report the incident to the OEDO but also indicate what corrective actions were taken by that office. Corrective actions reported to the OEDO include counseling staff, secretaries and managers on the lessons learned from the specific release of information, strengthening procedures and updating policy guidelines. Some of the corrective actions initiated by OEDO include: 1) introduction of colored cover sheets for better control and recognition of sensitive documents, 2) review of divisional controls and outlining recommended changes, and 3) disclose lessons learned with other regions to alert them of similar situations in an effort to avoid similar incidences. NRC employees agency-wide could benefit from the

lessons learned and corrective actions put in place. Therefore, the reporting of all incidents of inadvertent release of sensitive unclassified information to the OEDO is necessary.

Summary

All incidents of inadvertent releases of sensitive unclassified information have not been reported to the OEDO in accordance with MD 3.4. To ensure the OEDO has an opportunity to identify systemic problems, develop lessons learned, and implement best practices agency-wide, the OEDO should reinforce this requirement.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

4. Train NRC employees and contractors on the requirement to report incidents of inadvertent releases of sensitive unclassified information to the OEDO in accordance with MD 3.4.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Update the guidance for Official Use Only documents to require clear identification of sensitive unclassified information to prevent its inadvertent disclosure.

2. Mandate consistent use of defined markings on documents containing Official Use Only information and clarify the markings that should be used on sensitive unclassified information.

3. Conduct annual mandatory training for all NRC employees and contractors on the procedures for marking and handling sensitive unclassified information.

4. Train NRC employees and contractors on the requirement to report incidents of inadvertent releases of sensitive unclassified information to the OEDO in accordance with MD 3.4.

V. AGENCY COMMENTS

At an exit conference held on September 24, 2002, NRC officials generally agreed with the report's findings and recommendations. While agency officials chose not to provide a formal, written response for inclusion in the report, they did provide editorial suggestions which have been incorporated where appropriate.

SCOPE AND METHODOLOGY

OIG reviewed the adequacy of NRC's program for the protection, marking and handling of sensitive unclassified information. To accomplish this, OIG reviewed NRC Management Directives and Revision Zero of the draft of the Yucca Mountain Review Plan that was inadvertently released. Auditors also interviewed staff members of the Office of the Chief Information Officer, Office of Nuclear Security and Incident Response, Office of Administration, and Office of the Executive Director for Operations to discuss the implementation of guidance and training. In addition, OIG spoke with officials of the Office of Nuclear Reactor Regulation, the Office of Nuclear Materials Safety and Safeguards, the Office of Nuclear Regulatory Research, Region I and Region II to discuss prior releases of sensitive unclassified information and the corrective actions implemented.

This work was conducted from November 2001 through August 2002, in accordance with generally accepted Government auditing standards and included a review of management controls related to the objectives of the audit.

The major contributors to this report were Russ Irish, Acting Team Leader; Shyrl Coker, Senior Auditor; and David Ditto, Management Analyst.