AUDIT REPORT

Audit of NRC's Communications Security Program

OIG-14-A-21 September 29, 2014

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

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

OFFICE OF THE
INSPECTOR GENERAL

September 29, 2014

MEMORANDUM TO: Mark A. Satorius
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S COMMUNICATIONS SECURITY PROGRAM (OIG-14-A-21)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Communications Security Program*.

The report presents the results of the subject audit. Following the September 17, 2014, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

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

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

Attachment: As stated

cc: M. Galloway, OEDO
K. Brock, OEDO
J. Arildsen, OEDO
C. Jaegers, OEDO
RidsEdoMailCenter

EXECUTIVE SUMMARY

BACKGROUND

Nuclear Regulatory Commission (NRC) facilities are equipped with communications security (COMSEC)[1] equipment to facilitate communication of classified and sensitive unclassified information during routine and emergency operations. COMSEC equipment is designed to protect information while it is being transmitted by telephone, cable, microwave, satellite, or any other means. This includes, but is not limited to, keying materials,[2] equipment, devices, documents, and firmware or software that embodies or describes cryptographic logic or performs COMSEC functions. Examples of COMSEC equipment include a key processor, in-line encryptor (data), and a Secure Terminal Equipment (STE)[3] phone (voice). Information and material that are designated and marked as containing classified and/or sensitive unclassified information are made available only to appropriately cleared personnel who have a legitimate need-to-know.

COMSEC Program at NRC

COMSEC equipment at NRC is used to communicate sensitive and classified information and is a vital link for secure communication. NRC headquarters, region offices, and resident inspectors use a mix of classified and unclassified COMSEC equipment. As of August 2014, NRC had 696 COMSEC items in its inventory. In Fiscal Year 2013 (the most current year for which data were available during this audit), NRC spent $3,622,500 on classified information systems, which included COMSEC equipment.

[1] COMSEC is a technical term used in the Federal Government to describe material and equipment designed to secure or authenticate telecommunications. COMSEC is used to protect both classified and unclassified traffic on Government and military communications networks, including voice, video, and data. Specific encryption criteria vary depending on information's sensitivity.

[2] Keying materials contain an algorithm used to convert information from plain text to cipher text (encrypt) and convert the information from cipher text (encrypt) to plain text (decrypt).

[3] A STE consists of a host terminal and a removable security core. The host terminal is the STE, which provides the application hardware and software. The security core is the crypto card, which provides all the security services.

COMSEC Responsibilities

The Office of Nuclear Security and Incident Response is responsible for communicating policy and procedural information to the regions and making sure the regions are conforming to Federal policy. Each region has at least one COMSEC custodian and one alternative person; they are responsible for COMSEC items at resident inspector offices – both nuclear power plants and fuel cycle facilities – and for supporting resident inspector staff with equipment or network problems. The resident inspector staff are not custodians, but rather end users; thus, custodian responsibilities fall on the regional office COMSEC custodians.

OBJECTIVE

The audit objective was to determine whether NRC staff manage COMSEC systems in accordance with NRC and Federal Government COMSEC policies.

RESULTS IN BRIEF

The Office of the Inspector General evaluated NRC staff's management of the COMSEC program in accordance with Federal and agency policies. Based on this work, auditors did not identify instances where staff mismanaged the COMSEC program, or classified and sensitive information was disclosed to unauthorized personnel. However, opportunities exist to improve the COMSEC emergency plans and management of equipment maintenance contracting.

COMSEC Emergency Plans Are Not Consistently Updated and Communicated to Staff

Federal Government COMSEC policy states that emergency plans must be documented and maintained, and that staff must be aware of plans for the accounting and protection of COMSEC materials during emergencies. NRC has not fully complied with Federal Government COMSEC emergency planning requirements. This occurs because of inconsistent management emphasis on updating plans and informing personnel of their responsibilities. As a result, NRC staff who manage and use COMSEC equipment may not be prepared to uphold their COMSEC responsibilities during emergency situations such as natural disasters or hostile actions against their facilities.

Inadequate Maintenance Support Causes High Malfunction Rates for Secure Fax Machines

Federal and NRC guidance provides criteria for procurement and resource management that emphasizes efficient and effective resource use. Although NRC has a contract in place for secure fax maintenance, auditors observed a 60-percent malfunction rate across the agency's inventory of secure fax machines. The high malfunction rates of NRC's secure fax machines are attributable to a lack of performance-based contract terms that reflect the agency's equipment readiness requirements. While no NRC staff faced immediate harm because of malfunctioning secure fax machines, the quarterly testing and compensating maintenance work performed by staff on these machines is an inefficient use of agency resources.

RECOMMENDATIONS

This report makes recommendations to enhance the management of NRC's COMSEC program. A list of these recommendations appears on page 11 of this report.

AGENCY COMMENTS

An exit conference was held with the agency on September 17, 2014. Prior to this meeting, after reviewing a discussion draft, agency management provided supplemental information that has been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

COMSEC	Communications Security
CNSS	Committee on National Security Systems
CSS	Central Security Service
EKMS	Electronic Key Management System
MD	Management Directive
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
OIG	Office of the Inspector General
STE	Secure Terminal Equipment

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

ABBREVIATIONS AND ACRONYNMS iv

I. BACKGROUND 1

II. OBJECTIVE 3

III. FINDINGS 4

A. COMSEC Emergency Plans Are Not Consistently Updated and Communicated to Staff 4

B. Inadequate Maintenance Support Causes High Malfunction Rates for Secure Fax Machines... 7

IV. CONSOLIDATED LIST OF RECOMMENDATIONS 11

V. AGENCY COMMENTS 12

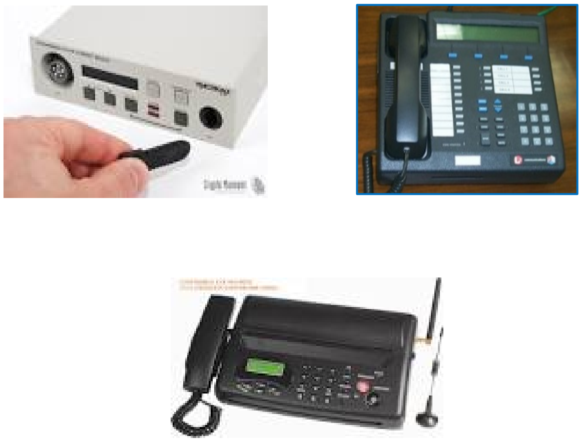
APPENDIXES

A. OBJECTIVE, SCOPE, AND METHODOLOGY....................................... 13

I. BACKGROUND

Nuclear Regulatory Commission (NRC) facilities are equipped with communications security (COMSEC)[4] equipment to facilitate communication of classified and sensitive unclassified information during routine and emergency operations. COMSEC equipment is designed to protect information while it is being transmitted by telephone, cable, microwave, satellite, or any other means. This includes, but is not limited to, keying materials,[5] equipment, devices, documents, and firmware or software that embodies or describes cryptographic logic or performs COMSEC functions. Examples of COMSEC equipment include a key processor, in-line encryptor (data), and a Secure Terminal Equipment (STE)[6] phone (voice). Information and material that are designated and marked as containing classified and/or sensitive unclassified information are made available only to appropriately cleared personnel who have a legitimate need-to-know.

Figure 1 — Examples of COMSEC Equipment.



Source: NRC

[4] COMSEC is a technical term used in the Federal Government to describe material and equipment designed to secure or authenticate telecommunications. COMSEC is used to protect both classified and unclassified traffic on Government and military communications networks, including voice, video, and data. Specific encryption criteria vary depending on information's sensitivity.

[5] Keying materials contain an algorithm used to convert information from plain text to cipher text (encrypt) and convert the information from cipher text (encrypt) to plain text (decrypt).

[6] A STE consists of a host terminal and a removable security core. The host terminal is the STE, which provides the application hardware and software. The security core is the crypto card, which provides all the security services.

Controlled Cryptographic Item is a National Security Agency (NSA) term for secure telecommunications or information handling equipment, associated cryptographic component, or other hardware items that perform a critical COMSEC function. The Electronic Key Management System (EKMS) is an NSA program responsible for COMSEC key management, accounting, and distribution. EKMS performs account registration, privilege management, ordering, distribution, and accounting to direct the management and distribution of physical COMSEC materials. NRC is currently in process of upgrading EKMS to a newer version.

COMSEC Guidance

The Committee on National Security Systems (CNSS), which is led by the Department of Defense, sets guidance on Federal Government COMSEC standards. CNSS guidance[7] prescribes the minimum standards, processes, and procedures for the routine destruction and emergency protection of COMSEC. U.S. Government departments, agencies, and military services may impose more stringent standards or requirements; however, the standards set forth in this instruction cannot be diminished. NRC adheres to CNSS instructions and standards related to the routine destruction and emergency protection of COMSEC.

COMSEC Program at NRC

COMSEC equipment at NRC is used to communicate sensitive and classified information and is a vital link for secure communications. NRC headquarters, regional offices, and resident inspectors use a mix of classified and unclassified COMSEC equipment. According to NRC guidance, one goal of the agency's cyber security program[8] is to ensure that COMSEC and classified systems comply with CNSS security requirements. NSA/Central Security Service (CSS) Policy Manual No. 3-16, *Control of Communications Security (COMSEC) Material*, and NRC Management Directive (MD) 12.4, *NRC Telecommunications Systems Security Program*, are the primary NRC guidance documents.

[7] CNSS Instruction No. 4004.1, "*DESTRUCTION AND EMERGENCY PROTECTION PROCEDURES FOR COMSEC AND CLASSIFIED MATERIAL.*"

[8] NRC Management Directive (MD) 12.5, *NRC Cyber Security Program.*

As of August 2014, NRC had 696 COMSEC items in its inventory. In Fiscal Year 2013 (the most current year for which data were available during this audit), NRC spent $3,622,500 on classified information systems, which included COMSEC equipment.

COMSEC Responsibilities

The Office of Nuclear Security and Incident Response is responsible for communicating policy and procedural information to the regions and making sure the regions are conforming to CNSS policy. Each region has at least one COMSEC custodian and one alternate; they are responsible for COMSEC items at resident inspector offices – both nuclear power plants and fuel cycle facilities – and for supporting resident inspector staff with equipment or network problems. The resident inspector staff are not custodians, but rather end users; thus, custodian responsibilities fall on the regional office COMSEC custodians.

COMSEC custodians are responsible for the receipt, custody, issue, safeguarding, accounting for, and, when necessary, destruction of COMSEC material.[9] In addition, they are responsible for the maintenance of up-to-date records and submission of all required accounting reports. There are a number of COMSEC related tasks and responsibilities that require time in addition to other information technology support duties at the regional office. These duties include quarterly STE function and secure fax testing at each of the resident inspector sites, semiannual inventory checks, data calls with resident inspector sites and the regional office, and encryption keys that must be updated.

II. OBJECTIVE

The audit objective was to determine whether NRC staff manage COMSEC systems in accordance with NRC and Federal Government COMSEC policies. Appendix A contains information on the audit scope and methodology.

[9] Under certain circumstances, end-users are also responsible for destruction of COMSEC material.

III. FINDINGS

The Office of the Inspector General (OIG) evaluated NRC staff's management of the COMSEC program in accordance with Federal and agency policies. Based on this work, auditors did not identify instances where staff mismanaged the COMSEC program, or classified and sensitive information was disclosed to unauthorized personnel. However, opportunities exist to improve the COMSEC emergency plans and management of equipment maintenance contracting.

A. COMSEC Emergency Plans Are Not Consistently Updated and Communicated to Staff

Federal Government COMSEC policy states that emergency plans must be documented and maintained, and that staff must be aware of plans for the accounting and protection of COMSEC materials during emergencies. NRC has not fully complied with Federal Government COMSEC emergency planning requirements. This occurs because of inconsistent management emphasis on updating plans and informing personnel of their responsibilities. As a result, NRC staff who manage and use COMSEC equipment may not be prepared to uphold their COMSEC responsibilities during emergency situations such as natural disasters or hostile actions against their facilities.

Federal Policy Requires Updating and Disseminating COMSEC Emergency Plans

Federal Government COMSEC policies require agencies that hold COMSEC material to maintain a current, written emergency plan appropriate for natural disasters (e.g., hurricanes in the South, tornados or floods in the Midwest, wild fires in the West) likely to occur in their location, and hostile actions (such as an enemy or terrorist attack, mob action, or civil uprising) against their facilities. Furthermore, all emergency plans are required to be reviewed annually and updated as necessary, and all authorized personnel at the facility must be aware of the existence of the plan.[10]

[10] NSA/CSS Policy Manual No. 3-16.

In addition, NRC's primary internal guidance for COMSEC program, MD 12.4, *NRC Telecommunications Systems Security Program,* states that each organization holding classified COMSEC material must maintain a current, written emergency plan for the protection of this material during emergencies.[11] NRC's management is responsible for developing internal controls – such as a current, written emergency plan, procedures, and practices – to fit the agency's operations and help staff understand and carry out their responsibilities.

Plans are necessary so that staff know how to react during an emergency. Emergency plans for natural disasters, for example, must provide preparedness procedures – such as procedures for receiving first responders, securing and removal of COMSEC materials, assessment and reporting, and post-emergency inventory. Hostile actions plans must provide preparedness procedures – such as threat assessment, physical security availability and adequacy, and facilities for implementing emergency evacuation.

NRC Compliance with Federal and Agency's Emergency Plans Requirement Inconsistent

NRC is not consistently complying with Federal Government COMSEC emergency planning requirements. OIG visited 13 facilities – including all 4 regional offices, agency headquarters, and resident inspector offices at nuclear power plants. Among these sites, only six sites maintained current emergency plan action procedures. For those offices that had plans, the plans ranged from a verbal description of the process to various types of documents including office instructions, plant and personnel safety procedures, and/or agencywide equipment destruction procedures that did not include specific information needed to safeguard and control COMSEC materials against natural disasters or hostile actions against their facilities. The remaining seven offices reported having no relevant guidance for emergency plans and procedures. Other guidance referenced instructions for transferring and decommissioning of COMSEC equipment; however, procedures – such as preparedness planning for natural disasters/accidental emergency,

[11] MD 12.4 was last issued in 1999, but was undergoing revision during this audit.

planning for hostile actions, and post emergency procedures – were not addressed in their instructions.

COMSEC Emergency Plans Not Consistently Updated and Communicated

NRC is not consistently complying with COMSEC emergency planning requirements because of inconsistent management emphasis on updating plans and informing personnel. In five of seven instances, when asked about emergency plans, resident inspectors stated that they did not keep such plans and were not aware of the plans. In addition, resident inspectors acknowledged that the regional offices might have such plans, but they had not been apprised of the plans. One rationale provided for the failure to update plans and inform personnel was the infrequent use of COMSEC equipment for actual emergency events.[12] Further, two resident inspectors questioned the need for such plans because the COMSEC items requiring special controls were already located in a secure location —i.e., inside a nuclear power plant's protected area.[13] Other NRC staff acknowledged having COMSEC emergency plans on file, but had not informed their staff of this guidance because it had not been updated since 2008.

Staff Need Updated Guidance To Perform Duties

Without current COMSEC emergency plans and informed personnel, NRC staff may not appropriately perform their COMSEC protection and accountability duties during natural disasters or hostile actions against their facilities. Further, NRC, a participant in the Federal Government's COMSEC program, has a responsibility to meet the program's requirements for ensuring its staff are prepared to fulfill their COMSEC duties in emergency situations.

Recommendations:

OIG recommends that the Executive Director for Operations

[12] COMSEC equipment at resident inspector offices is rarely used other than for testing purposes.

[13] Protected areas in nuclear power plants have physical barriers and other controls designed to limit access to authorized personnel conducting official business.

1. Develop and maintain current, written emergency plans appropriate for natural disasters and hostile actions against their facilities in accordance with NSA/CSS Policy Manual No. 3-16.

2. Review COMSEC emergency plans annually.

3. Include current emergency plan information and COMSEC equipment user duties with COMSEC equipment testing.

B. Inadequate Maintenance Support Causes High Malfunction Rates for Secure Fax Machines

Federal and NRC guidance provides criteria for procurement and resource management that emphasizes efficient and effective resource use. Although NRC has a contract in place for secure fax maintenance, auditors observed a 60-percent malfunction rate across the agency's inventory of secure fax machines. The high malfunction rates of NRC's secure fax machines are attributable to a lack of performance-based contract terms that reflect the agency's equipment readiness requirements. While no NRC staff faced immediate harm because of malfunctioning secure fax machines, the quarterly testing and compensating maintenance work performed by staff on these machines is an inefficient use of agency resources.

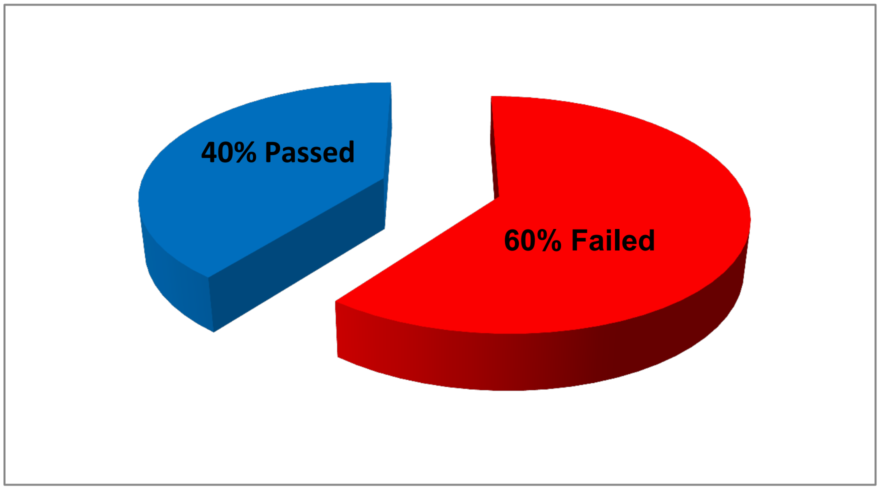
Federal and NRC Guidance Emphasizes Efficient and Effective Resource Use

Federal and NRC guidance provides criteria for procurement and resource management that emphasizes efficient and effective resource use. Government Accountability Office guidance emphasizes internal controls to help agencies meet their operational objectives through effective and efficient use of resources. Moreover, the objectives of NRC MD 11.1, *NRC Acquisition of Supplies and Services*, include achieving the best value for NRC's acquisition of supplies and services, and ensuring appropriate use of taxpayer funds when planning, negotiating, awarding, and administering contracts.

Secure Fax Machines Have High Malfunction Rates

Although NRC has a contract in place for secure fax maintenance, there is a high malfunction rate across the agency's inventory of 90 secure fax machines.[14] Auditors reviewed secure fax test result logs from the regions and found failure rates ranging from 37 percent to 81 percent during the most recent quarterly tests.[15] One region did not provide data because its staff had suspended the required functionality tests knowing in advance that their machines would fail.

Figure 2 — High malfunction rate of secure fax machines from the regions.



Source: OIG

NRC staff has attempted to maintain secure fax machines that fail due to inoperable components using an in place maintenance contract, while also allocating some funds for new secure fax machines of a different model.

As of July 24, 2014, NRC had spent a total of $63,000 for maintenance of secure fax equipment covering the period of August 2011 to December 2014. NRC recently extended the contract into the option year (starting December 2013) even though those model faxes were known to function poorly. OIG was advised that NRC could not replace all of its malfunctioning machines with a more reliable model due to limited funds.

[14] Staff interviews and documentation of fax test results show a total of 43 sites tested during the first quarter of 2014; 26 sites failed the test.

[15] Staff interviews and documentation of equipment test results show the fax machines have had functionality problems for several years.

Subsequent to this audit, NRC staff reportedly issued a new contract to replace malfunctioning secure fax machines at resident inspector sites.

NRC Lacks Performance-Based Maintenance Support Contract for Secure Faxes

The high failure rates of NRC's secure fax machines are attributable to lack of performance-based contract terms that reflect the agency's equipment readiness requirements.[16] NRC has relied on a firm-fixed price maintenance support contract worth approximately $31,000 annually to procure maintenance and support service for the 90 NRC-owned secure fax machines. Maintenance covers all parts and labor and phone technology support. The contract was renewed most recently for the December 2013 through December 2014 time period.

While the contract specifies work to be performed by the vendor, it does not include performance goals such as readiness rates for NRC's secure faxes.[17] Moreover, the contract does not link vendor compensation to defined performance metrics; thus NRC pays its vendor for work regardless of the outcome of that work.[18] NRC staff acknowledged that future maintenance support contracts would benefit from more specific language about the agency's expectations, as well as performance-based terms to hold vendors accountable for meeting work quality standards.

Malfunctioning Secure Faxes Result in Inefficient Resource Use and Diminished Communications Capabilities

While OIG did not identify immediate harm to NRC staff resulting from malfunctioning secure fax machines, staff would not have been able to use the machines for their intended purpose to send or receive sensitive written information or graphics. Additionally, the $63,000 spent over a

[16] Performance-based acquisition is the preferred method for acquiring services in the Federal Government. Under this approach, all aspects of the work and acquisition are structured around the purpose of the work to be performed (i.e., performance results or outputs) rather than the manner in which the work is to be performed.

[17] Performance-based contracts are to include performance work statements or statements of objectives that describe work in terms of required results rather than "how" the work is to be accomplished or the number of hours to be provided. See *Federal Acquisition Regulation*, Subpart 37.602.

[18] If appropriate, performance incentives are to correspond to performance standards set forth in the contract. See *Federal Acquisition Regulation*, Subpart 37.601.

3-year period to maintain inoperable machines could have been used to support other COMSEC program needs. Furthermore, the quarterly testing and compensating maintenance work performed by staff on these machines is an inefficient use of agency resources.[19] Staff expressed concerns about the administrative burden associated with testing and reported devoting considerable time to repairing the machines or helping their colleagues repair the machines,[20] despite the fact that COMSEC custodian duties are ancillary for region-based staff tasked primarily with other duties. In addition to this burden on staff time, malfunctioning of secure faxes diminishes NRC's ability to disseminate information to staff under specific emergency conditions.

Recommendation:

OIG recommends that the Executive Director for Operations

4. Procure a secure fax maintenance support contract that specifies maintenance performance standards and links these standards to vendor compensation.

[19] During each test, at least two staff are involved: one sending the test fax, and one confirming receipt or failure to receive the test fax. When fax machines fail, these tests can take up to an hour as the staff troubleshoot and attempt to fix malfunctions.

[20] In some cases, region-based COMSEC custodians drive to nearby resident inspector sites to perform maintenance work themselves. In cases where Resident Inspector sites are located far from NRC region offices, COMSEC custodians provide maintenance support by phone.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Develop and maintain current, written emergency plans appropriate for natural disasters and hostile actions against their facilities in accordance with NSA/CSS Policy Manual No. 3-16.

2. Review COMSEC emergency plans annually.

3. Include current emergency plan information and COMSEC equipment user duties with COMSEC equipment testing.

4. Procure a secure fax maintenance support contract that specifies maintenance performance standards and links these standards to vendor compensation.

V. AGENCY COMMENTS

An exit conference was held with the agency on September 17, 2014. Prior to this meeting, after reviewing a discussion draft, agency management provided supplemental information that has been incorporated into this report, as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

APPENDIX A

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The audit objective was to determine whether NRC staff manage COMSEC systems in accordance with NRC and Federal Government COMSEC policies.

SCOPE

The audit reviewed NRC's activities related to COMSEC with special emphasis on process and compliance with current laws. OIG performed the audit work at NRC headquarters in Rockville, Maryland; NRC regional offices; and licensee facilities from March 2014 to August 2014. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility of fraud, waste, and abuse in the program.

METHODOLOGY

To accomplish the audit objective, OIG reviewed and analyzed Federal Government guidance, and internal agency procedures. Guidance reviewed included the following:

- Government Accountability Office Standards for Internal Control in the Federal Government.
- National Security Agency Central Security Service Policy Manual No. 3-16, *Control Of Communications Security (COMSEC) Material.*
- Committee on National Security Systems Instruction No. 4004.1, *Destruction and Emergency Protection Procedures for COMSEC and Classified Material.*
- NRC Management Directive 12.4, *NRC Telecommunications Systems Security Program.*
- NRC Management Directive 12.5, *NRC Cyber Security Program*.

- NRC Management Directive 11.1, *NRC Acquisition of Supplies and Services.*

OIG interviewed headquarters staff, regional personnel, and resident inspectors at nuclear power plants and fuel cycle facilities to gain an understanding about COMSEC policies and procedures. Furthermore, OIG inspected COMSEC equipment at all four region offices, seven nuclear power plants, and one fuel cycle facility: Three Mile Island Nuclear Station in Middletown, PA; Salem - Hope Creek Nuclear Station in Hancock's Bridge, NJ; Braidwood Nuclear Generating Station in Braidwood, IL; Dresden Nuclear Power Plant in Morris, IL; Comanche Peak Nuclear Power Plant in Glen Rose, TX; Columbia Generating Station in Richland, WA; North Anna Power Station in Mineral, VA; and Babcock & Wilcox Nuclear Operations Group Fuel Cycle Facility in Lynchburg, VA. We selected these sites to sample commercial nuclear power reactors and fuel cycle facilities under each of the four region office jurisdictions.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The work was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Rob Woodward, Audit Manager; Neil Doherty, Senior Analyst; and Ziad Buhaissi, Senior Auditor.