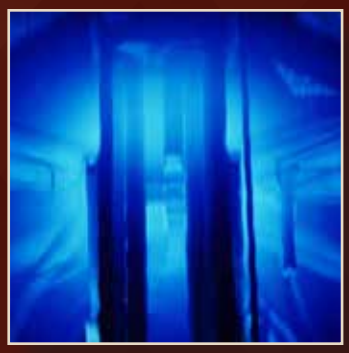
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Semiannual Report
TO CONGRESS

April 1, 2014–September 30, 2014

OIG VISION

OIG will identify the most critical risks and vulnerabilities in agency operations in a timely manner to allow the agency to take any necessary corrective action and to prevent and detect fraud, waste, and abuse.

OIG MISSION

The NRC OIG's mission is to independently and objectively audit and investigate programs and operations to promote effectiveness and efficiency, and to prevent and detect fraud, waste, and abuse.

COVER PHOTOS:

Top Left: Gamma Knife® used for treating brain tumors. (Photo courtesy: Elekta)

Top Right: Blue glow of radiation known as the "Cerenkov effect" from nuclear fuel in a nuclear reactor.

Bottom Left: Reactor vessel head.

Bottom Right: Cooling tower at Limerick nuclear power station. (Photo courtesy: Exelon)

A MESSAGE FROM THE INSPECTOR GENERAL

I am pleased to present this Semiannual Report to Congress on the activities and accomplishments of the Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) from April 1, 2014, to September 30, 2014.

Our work reflects the legislative mandate of the Inspector General Act of 1978, as amended, which is to identify and prevent fraud, waste, and abuse through the conduct of audits and investigations relating to NRC programs and operations. In addition, the Consolidated Appropriations Act, 2014, provided that notwithstanding any other provision of law, the Inspector General of the Nuclear Regulatory Commission is authorized in 2014 and subsequent years to exercise the same authorities with respect to the Defense Nuclear Facilities Safety Board (DNFSB), as determined by the Inspector General of the Nuclear Regulatory Commission, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the Nuclear Regulatory Commission.

NRC OIG carries out its mission through its Audits and Investigations Programs. The audits and investigations highlighted in this report demonstrate our commitment to ensuring integrity and efficiency in NRC's programs and operations.

During the period covered by this report, NRC OIG continued its commitment to promote economy, efficiency, and effectiveness in critical NRC technical and corporate management programs and operations and those of DNFSB. The work highlighted in this report includes audits of NRC's oversight of its cyber security inspection program at nuclear power plants, NRC oversight of Agreement State licensees opperating in NRC jursdiction under reciprocity, and whether the method for retaining and documenting information supporting the Yucca Mountain licensing process is compliant with Federal requirements. Additionally the work highlighted in this report includes audits of DNFSB's purchase card program and Freedom of Information Act process.

During this semiannual reporting period, we issued 10 audit reports. As a result of this work, OIG made a number of recommendations to improve the effective and efficient operation of NRC's safety, security, and corporate management programs and those of DNFSB. OIG also opened 12 investigations, and completed 19 cases. One of the open cases was referred to the Department of Justice, and 25 allegations were referred to NRC management for action.

The NRC OIG remains committed to the integrity, efficiency, and effectiveness of NRC and DNFSB programs and operations, and our audits, investigations, and other activities highlighted in this report demonstrate this ongoing commitment. My staff continuously strives to maintain the highest possible standards of professionalism and quality in its audits and investigations. I would like to acknowledge our auditors, investigators, and support staff for their superior work and ongoing commitment to the mission of this office.

Finally, the success of the NRC OIG would not be possible without the collaborative efforts between my staff and those of the NRC and DNFSB to address OIG findings and to timely implement recommended corrective actions. I wish to thank them for their dedication and support, and I look forward to their continued cooperation as we work together to ensure the integrity and efficiency of agency and DNFSB operations.

Hubert T. Bell
Inspector General

Nuclear steam turbine.

CONTENTS

Resident Inspector performs a walk through inspection at Calvert Cliffs nuclear power station.

HIGHLIGHTS

The following three sections highlight selected audits and investigations completed during this reporting period. More detailed summaries appear in subsequent sections of this report.

NRC Audits

- U.S. Nuclear Regulatory Commission (NRC) facilities are equipped with communications security (COMSEC) 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. COMSEC equipment at NRC is used to communicate sensitive and classified information and is a vital link for secure communication. The audit objective was to determine whether NRC staff manage COMSEC systems in accordance with NRC and Federal Government COMSEC policies.

- Sequestration is the cancellation of budgetary resources provided by discretionary appropriations or direct spending law. Sequestration has been used as a means to control the U.S. budget since enactment of the Balanced Budget Emergency Deficit Control Act of 1985. In August 2011, the Budget Control Act of 2011 specified cuts to eventually be taken each year from 2013 to 2021. The American Taxpayer Relief Act of 2012 specified the start of the sequestration mandate during FY 2013, unless Congress agreed to spending cuts to reduce the deficit to prevent the application of the sequestration mandate. Congress made no such agreement. As a result, the President signed the order to sequester approximately $85 billion of the FY 2013 budget for the Federal Government. Of this total, NRC's portion was eventually determined to be $52 million. The audit objective was to evaluate NRC's sequestration process.

- Federal regulations provide that Federal agencies should strive to (1) convey written instructions and document agency policies and procedures through effective directives management and (2) provide agency personnel with information needed in the right place, at the right time, and in a useful format. At NRC, management directives are issued to (1) promulgate internal policy and procedures of agencywide interest or application that concern a high profile, mission-critical agency function or program and (2) impose substantive requirements on more than one NRC office. The audit objectives were to evaluate the adequacy of NRC's compliance with Management Directive 1.1, *NRC Management Directives System*, particularly in the areas of keeping management directives accurate and up-to-date, and whether opportunities exist to improve the process.

- In 1983, the Nuclear Waste Policy Act assigned the Department of Energy (DOE) responsibility for constructing and operating a nuclear waste repository for high-level radioactive waste (HLW) and NRC the task of licensing and regulating the HLW repository. In 2002, President Bush signed legislation selecting Yucca Mountain as the repository site. In 2008, DOE submitted a license application for construction authorization to build the repository at Yucca Mountain, but filed a motion to withdraw its application in March 2010.

In October 2010, the then-NRC Chairman directed NRC staff to prepare the orderly closeout of its technical safety review, and in 2011, the Atomic Safety and Licensing Board Panel suspended the adjudicatory hearing of the DOE's license application. Stakeholders pursued legal action to direct NRC to complete its technical safety review, which culminated in an August 2013 United States Court of Appeals for the District of Columbia Circuit Writ of Mandamus for NRC to continue with the Yucca Mountain licensing process. NRC issued a Commission Order in November 2013 to finish the remaining volumes of the Safety Evaluation Report. The audit objective was to determine if agency policy and procedures on document management are compliant with Federal requirements and provide reasonable assurance that documentation related to the review of the Yucca Mountain facility has been appropriately managed and retained.

- The Freedom of Information Act (FOIA) is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government. The FOIA process begins when the agency (1) receives an incoming FOIA request, (2) assigns it a number, and (3) determines which NRC offices need to review their records to identify whether they have information pertinent to the request and sends a request to those offices. FOIA coordinators in responsive offices provide an estimate of the search, review, and duplication effort required to produce documents identified as within the scope of the request. NRC's FOIA office then estimates the associated processing fees, advises the requester as to the amount due, and assigns the request to the appropriate offices to identify and provide all relevant documents from their office within an assigned timeframe. FOIA coordinators consult as needed with agency staff in the responding offices and/or the Office of the General Counsel to prepare a response. The response is reviewed and signed by the FOIA officer, and sent to the requester. The audit objective was to determine whether the FOIA process is efficient and complies with the current laws.

- Reciprocity is NRC recognition of certain Agreement State licenses for work performed in areas of NRC jurisdiction. Areas of NRC jurisdiction include non-Agreement States, areas of exclusive Federal jurisdiction, and offshore waters. The term reciprocity is also used in Agreement States to identify Agreement State recognition of an NRC license and licenses from other Agreement States for work performed in their jurisdiction. Reciprocity authorizes Agreement State licensees to work in NRC jurisdiction for short periods of time without having to obtain a specific license. The audit objective was to determine whether NRC provides adequate oversight of Agreement State licensees operating in NRC jurisdiction under reciprocity.

- Cyber threats to NRC licensees are dynamic and multi-dimensional due to the continuously evolving capabilities of potential adversaries and emerging technologies. The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in digital systems that could be exploited either from outside or inside of a plant's protected area. Licensees operating a nuclear power plant are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-

attacks in accordance with 10 Code of Federal Regulations 73.54, which is also known as the "Cyber Security Rule." The audit objective was to determine the adequacy of NRC's cyber security inspection program for nuclear power plants.

- On July 22, 2010, the Improper Payments Elimination and Recovery Act (IPERA) was signed into law, which amended the Improper Payments Information Act of 2002 (IPIA) and generally repealed the Recovery Auditing Act. IPERA also directed the Office of Management and Budget to issue implementing guidance to agencies. IPERA requires Federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. In addition, IPERA requires each agency to conduct recovery audits with respect to each program and activity of the agency that expends $1,000,000 or more annually, if conducting such audits would be cost-effective. The audit objective was to assess NRC's compliance with the IPERA and report any material weaknesses in internal control.

Defense Nuclear Facilities Safety Board Audits

- The Governmentwide Purchase Card Program was established in the late 1980s as a way for agencies to streamline Federal acquisition processes. Purchase cards provide a low-cost, efficient vehicle for obtaining goods and services directly from vendors. They can be used for micro-purchases, as well as to place orders and make payments on contract activities. The Defense Nuclear Facilities Safety Board (Board) has had a purchase card program in place since late 1998. In December 2005, the Board issued Administrative Directive 211.2, Charge Card Management Program, which serves as the principal guide for the Board's charge card programs. The Board has a designated Program Coordinator for the purchase card program who is responsible for day-to-day program management. The Program Coordinator provides oversight of the purchase card program and serves as the liaison between cardholders and the contracting bank. The audit objective was to determine whether internal controls are in place and operating effectively to maintain compliance with applicable purchase card laws, regulations, and Board policies.

- In response to written FOIA requests, Federal agencies must disclose the requested records, unless they are protected from release under one of the nine FOIA statutory exemptions. In 2009, the President and the Attorney General each issued memoranda emphasizing that the FOIA "should be administered with a clear presumption: in the face of doubt, openness prevails." The President also directed agencies to "take affirmative steps to make information public" and not to "wait for specific requests from the public." The General Manager within the Office of the General Manager is the Chief FOIA Officer and manages the Board's FOIA program. During fiscal year 2013, Board staff processed 14 FOIA requests. The audit objective was to determine whether the Board's FOIA process is efficient and complies with current laws.

NRC Investigations

- OIG conducted an investigation into an allegation that an NRC employee improperly wrote and dispatched a letter to a contractor involved in the operation and development of the NRC Radiological Assessment System for Consequences Analysis (RASCAL) computer system, for which the employee was the NRC project manager, urging that the contractor should retain a particular employee. The RASCAL system is an important NRC tool for making independent dose and consequence projections during radiological incidents and emergencies.

- OIG completed an investigation into an allegation that the current NRC Chairman violated 10 CFR 2.347 (Ex-parte Communications) when she met with selected representatives of several citizens groups at the Seabrook Nuclear Power Plant in Seabrook, NH, and discussed adjudicatory matters regarding licensing proceedings.

- OIG completed an investigation into an allegation that an NRC manager named individuals who were to fill vacancies before a related vacancy announcement closed and improperly preselected individuals for the vacancy.

- OIG completed an investigation into an incident whereby an e-mail was sent to more than 5,000 NRC employee e-mail addresses, of which 4,149 were valid, requesting them to execute a command, which required they provide their NRC network account information because their in-box had exceeded its mailbox quota. Eight employees executed the command and provided their login information.

- OIG conducted an investigation into circumstances surrounding an e-mail being sent to NRC indicating that an individual had found a vulnerability on the public facing NRC.gov Web site and hacked into it. The individual reported being unable to gain access to the databases, but wanted to make a deal to provide all pertinent information regarding the hack.

OVERVIEW OF NRC AND OIG

NRC's Mission

NRC was formed in 1975, in accordance with the Energy Reorganization Act of 1974, to regulate the various commercial and institutional uses of nuclear materials. The agency succeeded the Atomic Energy Commission, which previously had responsibility for both developing and regulating nuclear activities.

NRC's mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. NRC's regulatory mission covers three main areas:

- **Reactors**—Commercial reactors that generate electric power and research and test reactors used for research, testing, and training.
- **Materials**—Uses of nuclear materials in medical, industrial, and academic settings and facilities that produce nuclear fuel.
- **Waste**—Transportation, storage, and disposal of nuclear materials and waste, and decommissioning of nuclear facilities from service.

Under its responsibility to protect public health and safety, NRC has three principal regulatory functions: (1) establish standards and regulations, (2) issue licenses for nuclear facilities and users of nuclear materials, and (3) inspect facilities and users of nuclear materials to ensure compliance with the requirements. These regulatory functions relate both to nuclear power plants and other uses of nuclear materials—like nuclear medicine programs at hospitals, academic activities at educational institutions, research, and such industrial applications as gauges and testing equipment.

NRC maintains a current Web site and a public document room at its headquarters in Rockville, MD; holds public hearings and public meetings in local areas and at NRC offices; and engages discussions with individuals and organizations.

OIG History, Mission, and Goals

OIG History

In the 1970s, Government scandals, oil shortages, and stories of corruption covered by newspapers, television, and radio stations took a toll on the American public's faith in its Government. The U.S. Congress knew it had to take action to restore the public's trust. It had to increase oversight of Federal programs and operations. It had to create a mechanism to evaluate the effectiveness of Government programs. And, it had to provide an independent voice for economy, efficiency, and effectiveness within the Federal Government that would earn and maintain the trust of the American people.

In response, Congress passed the landmark legislation known as the Inspector General Act (IG Act), which President Jimmy Carter signed into law in 1978. The IG Act created independent Inspectors General, who would protect the integrity of Government; improve program efficiency and effectiveness; prevent and detect fraud, waste, and abuse in Federal agencies; and keep agency heads, Congress, and the American people fully and currently informed of the findings of IG work.

Today, the IG concept is a proven success. The IGs continue to deliver significant benefits to our Nation. Thanks to IG audits and investigations, billions of dollars have been returned to the Federal Government or have been better spent based on recommendations identified through those audits and investigations. IG investigations have also contributed to the prosecution of thousands of wrongdoers. In addition, the IG concepts of good governance, accountability, and monetary recovery encourage foreign governments to seek advice from IGs, with the goal of replicating the basic IG principles in their own governments.

OIG Mission and Goals

NRC's OIG was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendment to the IG Act. NRC OIG's mission is to independently and objectively audit and investigate programs and operations to promote effectiveness and efficiency, and to prevent and detect fraud, waste and abuse.

The Consolidated Appropriations Act, 2014, provided that notwithstanding any other provision of law, the Inspector General of the Nuclear Regulatory Commission is authorized in 2014 and subsequent years to exercise the same authorities with respect to the Defense Nuclear Facilities Safety Board (DNFSB), as determined by the Inspector General of the Nuclear Regulatory Commission, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the Nuclear Regulatory Commission.

OIG is committed to ensuring the integrity of NRC and DNFSB programs and operations. Developing an effective planning strategy is a critical aspect of accomplishing this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, OIG developed a Strategic Plan that includes the major challenges and critical risk areas facing NRC.

The plan identifies OIG's priorities and establishes a shared set of expectations regarding the goals OIG expects to achieve and the strategies that will be employed to do so. OIG's Strategic Plan features three goals, which generally align with NRC's mission and goals:

1. **Strengthen NRC's efforts to protect public health and safety and the environment.**

2. **Enhance NRC's efforts to increase security in response to an evolving threat environment.**

3. **Increase the economy, efficiency, and effectiveness with which NRC manages and exercises stewardship over its resources.**

NRC OIG PROGRAMS AND ACTIVITIES

Audit Program

The OIG Audit Program focuses on management and financial operations; economy or efficiency with which an organization, program, or function is managed; and whether the programs achieve intended results. OIG auditors assess the degree to which an organization complies with laws, regulations, and internal policies in carrying out programs, and they test program effectiveness as well as the accuracy and reliability of financial statements. The overall objective of an audit is to identify ways to enhance agency operations and promote greater economy and efficiency. Audits comprise four phases:

- **Survey phase**—An initial phase of the audit process is used to gather information, without detailed verification, on the agency's organization, programs, activities, and functions. An assessment of vulnerable areas determines whether further review is needed.

- **Verification phase**—Detailed information is obtained to verify findings and support conclusions and recommendations.

- **Reporting phase**—The auditors present the information, findings, conclusions, and recommendations that are supported by the evidence gathered during the survey and verification phases. Exit conferences are held with management officials to obtain their views on issues in the draft audit report. Comments from the exit conferences are presented in the published audit report, as appropriate. Formal written comments are included in their entirety as an appendix in the published audit report.

- **Resolution phase**—Positive change results from the resolution process in which management takes action to improve operations based on the recommendations in the published audit report. Management actions are monitored until final action is taken on all recommendations. When management and OIG cannot agree on the actions needed to correct a problem identified in an audit report, the issue can be taken to the NRC Chairman for resolution.

Each October, OIG issues an *Annual Plan* that summarizes the audits planned for the coming fiscal year. Unanticipated high-priority issues may arise that generate audits not listed in the *Annual Plan*. OIG audit staff continually monitor specific issues areas to strengthen OIG's internal coordination and overall planning process. Under the OIG Issue Area Monitor (IAM) program, staff designated as IAMs are assigned responsibility for keeping abreast of major agency programs and activities. The broad IAM areas address nuclear reactors, nuclear materials, nuclear waste, international programs, security, information management, and financial management and administrative programs.

Investigative Program

OIG's responsibility for detecting and preventing fraud, waste, and abuse within NRC includes investigating possible violations of criminal statutes relating to NRC programs and activities, investigating misconduct by NRC employees, interfacing with the Department of Justice on OIG-related criminal matters, and coordinating investigations and other OIG initiatives with Federal, State, and local investigative agencies and other OIGs. Investigations may be initiated as a result of allegations or referrals from private citizens; licensee employees; NRC employees; Congress; other Federal, State, and local law enforcement agencies; OIG audits; the OIG Hotline; and OIG initiatives directed at areas bearing a high potential for fraud, waste, and abuse.

Because NRC's mission is to protect the health and safety of the public, OIG's Investigative Program directs much of its resources and attention to investigating allegations of NRC staff conduct that could adversely impact matters related to health and safety. These investigations may address the following allegations:

- Misconduct by high-ranking NRC officials and other NRC officials, such as managers and inspectors, whose positions directly impact public health and safety.
- Failure by NRC management to ensure that health and safety matters are appropriately addressed.
- Failure by NRC to appropriately transact nuclear regulation publicly and candidly and to openly seek and consider the public's input during the regulatory process.
- Conflicts of interest involving NRC employees and NRC contractors and licensees, including such matters as promises of future employment for favorable or inappropriate treatment and the acceptance of gratuities.
- Fraud in the NRC procurement program involving contractors violating Government contracting laws and rules.

OIG has also implemented a series of proactive initiatives designed to identify specific high-risk areas that are most vulnerable to fraud, waste, and abuse. A primary focus is electronic-related fraud in the business environment. OIG is committed to improving the security of this constantly changing electronic business environment by investigating unauthorized intrusions and computer-related fraud, and by conducting computer forensic examinations. Other proactive initiatives focus on determining instances of procurement fraud, theft of property, Government credit card abuse, and fraud in Federal programs.

OIG General Counsel Regulatory Review

Regulatory Review

Pursuant to the Inspector General Act, 5 U.S.C. App. 3, Section 4(a)(2), OIG reviews existing and proposed legislation, regulations, policy, and implementing Management Directives (MD), and makes recommendations to the agency concerning their impact on the economy and efficiency of agency programs and operations.

Regulatory review is intended to provide assistance and guidance to the agency prior to the concurrence process so as to avoid formal implementation of potentially flawed documents. The OIG does not concur or object to the agency actions reflected in the regulatory documents, but rather offers comments.

Comments provided in regulatory review reflect an objective analysis of the language of proposed agency statutes, directives, regulations and policies resulting from OIG insights from audits, investigations, and historical data and experience with agency programs. OIG review is structured so as to identify vulnerabilities and offer additional or alternative choices.

To effectively track the agency's response to OIG regulatory review, comments include a request for written replies within 90 days, with either a substantive reply or status of issues raised by OIG.

From April 1, 2014, through September 30, 2014, OIG regulatory review activities included examination of documents including Commission papers (SECYs), Staff Requirements Memoranda, Federal Register Notices, and Management Directives, as well as draft policies and statutes.

Comments provided on particular matters during this period are described below:

- Management Directive (MD) and Directive Handbook (DH) 9.10, *The Office of the Secretary, (SECY)*, summarizes the SECY responsibilities, including executive management services to support the Commission and to implement Commission decisions and advice and assistance to the Commission and the NRC staff on the planning, scheduling, and conduct of Commission business. OIG suggested it would be helpful for the MD to identify from whom the delegation of authority is given to the Secretary.

- MD and DH 12.2, *Classified Information Security Program*, is intended to ensure that all NRC personnel responsible for controlling, handling, and marking classified information (National Security Information, Restricted Data, and Formerly Restricted Data) and activities involving this information adhere to the procedures in this MD. The OIG review noted that the revised MD did not appear to comply with 32 CFR 2001.60(e), which requires that inspections be performed at least annually, and suggested clarification of the inspection language to assure compliance with this provision. OIG also suggested a requirement that the OIG duty agent be notified upon receipt of notification of the loss or possible compromise of classified information.

- MD and DH 12.7, *NRC Safeguards Information Security Program*, implements NRC policy to ensure that Safeguards Information is properly handled and protected from unauthorized disclosure in accordance with the Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011 et seq.). OIG suggested clarification as to the office responsible for conducting preliminary inquiries in this program.

- MD and DH 8.18, *NRC Generic Communications Program*, provides implementation for NRC policy to have an effective generic communications program for the purpose of communicating with the nuclear industry on matters having generic applicability. Regulatory review comments suggested that the Office of the General Counsel be identified as the authority for legal adequacy in each of the paragraphs that reference legal compliance in the MD. OIG also suggested addition of a provision for effectiveness reviews to include solicitation of feedback from stakeholders concerning opportunities to improve the generic communications process.

- MD and DH 10.49, *Student Loan Repayment Program*, is intended to adopt and implement the student loan repayment provisions of Title V of the *United States Code*, Section 5379 (5 U.S.C. 5379, as amended), and applicable implementing regulations from the Office of Personnel Management. OIG's comment on this draft related the need to include the authority of the Deputy Inspector General in authorizing student loan repayment for OIG employees.

- MD and DH 10.1, *Recruitment, Appointments, and Merit Staffing*, provides direction to assure appointments are effected in a fair and equitable manner following basic general Federal sector employment guidelines. Further, it provides essential guidance to ensure agencywide uniformity in the application of appointment and employment practices to assure appointment and assignment of employees who are well qualified to carry out the mission of the agency efficiently and effectively without regard to political affiliation, race, color, religion, national origin, sex, marital status, age, or handicapping condition; without favoritism based on personal relationship or patronage; and with proper regard for their privacy and constitutional rights.

  In its review of this draft, OIG identified a significant matter related to document retention in personnel actions, and commented extensively on the need for additional direction and clarification. OIG related a concern that the lack of adequate guidance regarding documents that must be retained to assure compliance with current Equal Employment Opportunity Commission requirements would hamper the agency in defending discrimination complaints on merit promotion actions. From its review, OIG found the guidance in the draft directive handbook inadequate in that it failed to provide specific directions as to what documents need to be retained.

In addition, OIG suggested that the MD and DH enumerate documents considered "all official records of the panel" and to identify and detail exactly what is expected to compose "a record of its proceedings sufficient to address any questions or challenges about applicant rankings." Further, OIG suggested that the MD describe precisely what are considered "documents necessary to reconstruct the action," and define fully and give examples of, documents considered "personal notes," and "preliminary candidate evaluations." In sum, OIG sought to obtain guidance in the MD which would describe in detail all documents to be retained, the required retention period, and enumeration of events which could trigger or change the retention requirements.

OIG notes that the agency declined to include these specific directions in the MD and DH, and advised that it would consider creating an operational document containing more detailed recordkeeping guidance. This reply was not considered responsive to the concerns raised by OIG.

Other OIG General Counsel Activities

Support of the Inspector General Community in Training

The Council of Counsels to Inspectors General, a group of attorneys who serve as legal advisors in the Federal Inspector General (IG) community, sponsors a training program for law students working as summer interns in IG offices in the Washington, D.C., area. As part of the introductory session for this year's program, Maryann Grodin, the NRC OIG General Counsel, along with Kirt West, Counsel to the IG at the National Reconnaissance Office provided a presentation on the concept and history of the IG offices in the Federal Government. In addition to the statutory history, they related the political and philosophical context of IG legal authority and functions. They illustrated these legal concepts with examples from their experiences as IG Counsel and with significant litigation and legislation in the IG community.

Whistleblowers in the Federal Courts Presentation

"Whistleblowers in the Federal Courts" presentation at the September Federal Bar Association Annual Conference.

The OIG General Counsel spoke as a panel member at the September Federal Bar Association Annual Conference. The panel, moderated by R. Scott Oswald of the Employment Law Group, also included Stephen Jonas of WilmerHale and Zachary Cunha, Department of Justice (DOJ), Assistant United States Attorney, Rhode Island. The presentation included types of whistleblowers, statutory provisions applicable to employment and fraud disclosures, expansion of these statutes to contractor employees, and recent amendments enhancing protection against retaliation. Updating information in the 1994 Federal Bar Journal article, "Nuclear Whistleblowers, An Environment of Change," authored with Alexandra B. Keith, Ms. Grodin related the Inspector General's investigative and coordinating role in Federal cases. She also used this opportunity to display the NRC OIG Whistleblower Web site and publicize the IG community focus on whistleblower protection. Other panel members discussed client representation issues and DOJ litigation processes.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing NRC as of October 1, 2013* *(as identified by the Inspector General)*	
Challenge 1	*Management of regulatory processes to meet a changing environment in the oversight of nuclear materials.*
Challenge 2	*Management of NRC security programs.*
Challenge 3	*Management of regulatory processes to meet a changing environment in the oversight of nuclear facilities.*
Challenge 4	*Management of regulatory processes associated with high-level radioactive waste.*
Challenge 5	*Management of information technology.*
Challenge 6	*Administration of all aspects of financial management and procurement.*
Challenge 7	*Management of human capital.*

**The most serious management and performance challenges are not ranked in any order of importance.*

NRC AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed eight financial and performance audits or evaluations, all of which are summarized here that resulted in numerous recommendations to NRC management. In addition, the Defense Contract Audit Agency completed four contract audits for OIG.

Audit Summaries

Audit of NRC's Communications Security Program

OIG Strategic Goal: Security

COMSEC Equipment

Source: NRC

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 equipment at NRC is used to communicate sensitive and classified information and is a vital link for secure communication. NRC headquarters, regional 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.

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

Audit Results:

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

[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.*

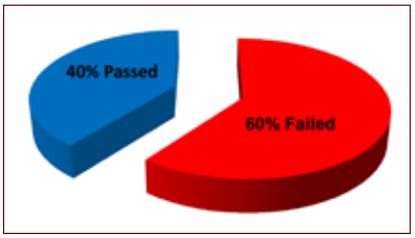
was disclosed to unauthorized personnel. However, opportunities exist to improve the COMSEC emergency plans and management of equipment maintenance contracting.

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

Secure Fax Machine Failure Rate



Source: NRC

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.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Sequestration Process

OIG Strategic Goal: Corporate Management

Sequestration is the cancellation of budgetary resources provided by discretionary appropriations or direct spending law. Sequestration has been used as a means to control the budget of the United States since enactment of the *Balanced Budget Emergency Deficit Control Act* of 1985. Following the enactment of the Balanced Budget Emergency Deficit Control Act, several sequestrations followed in the 1980s and 1990s. In August 2011, the Budget Control Act of 2011 specified cuts to eventually be taken each year from 2013 to 2021.[4] *The American Taxpayer Relief Act* of 2012, which was enacted on January 2, 2013, specified the start of the sequestration mandate during

[4] *According to NRC staff, the Bipartisan Budget Act of 2013, Pub. L. No. 113-67 (2013) suspended sequestration in fiscal years 2014 and 2015.*

FY 2013, unless Congress agreed to spending cuts to reduce the deficit to prevent the application of the sequestration mandate. Congress made no such agreement. As a result, the President signed the order to sequester approximately $85 billion of the FY 2013 budget for the Federal Government. Of this total sequestration amount, NRC's portion was eventually determined to be $52 million.

To meet the required sequestration mandate, a variety of offices were involved in the decisions surrounding which areas to cut. In October 2012, the Office of the Executive Director for Operations (OEDO) and the Office of the Chief Financial Officer (OCFO) determined the dollar amounts to be cut from the agency business lines.[5] On December 27, 2012, the Commission approved a proposed plan and related funding adjustments of $86 million.[6] OEDO and OCFO then communicated the dollar amount of the cuts to the agency, which included deputy executive directors and business line managers. In turn, these managers rolled the dollar figures down to the agency staff in the respective program offices, which were tasked with identifying specific cuts and then reporting the proposed cuts back up to agency executives.

The audit objective was to evaluate NRC's sequestration process.

Audit Results:

NRC made $52 million in sequestration reductions; however, agency managers responsible for implementing sequestration conveyed an unclear and inconsistent understanding of the basis for identifying reductions under the FY 2013 sequestration process. This occurred because NRC did not have agencywide guidance that established a consistent method for implementing sequestration reductions. The sequestration mandate that began in FY 2013 is scheduled to last approximately 9 years. Improved agencywide guidance that specifically addresses sequestration reductions would help the agency in making the reductions in a more efficient manner. The ability of the agency to prioritize different offices' activities and projects to make the necessary cuts will become increasingly difficult without an agencywide process for prioritizing work under sequestration.

(Addresses Management and Performance Challenge #3)

---

[5] *A business line is a component part of the agency under the direction of a "responsible lead office" (e.g., Office of New Reactors. Examples of a business line include high level waste, new reactors, and financial management. Business lines often include supporting offices (e.g., Office of Nuclear Regulatory Research does not lead a business line, but has a supporting role for several business lines). Business line managers are the lead staff for establishing internal control processes to reasonably ensure that the agency's internal control complies with Federal and NRC requirements.*

[6] *This estimated calculation, which was later reduced to $52 million, was based on the Budget Control Act of 2011.*

Audit of NRC's Process for Revising Management Directives

OIG Strategic Goal: Corporate Management

Federal regulations provide that Federal agencies should strive to (1) convey written instructions and document agency policies and procedures through effective directives management and (2) provide agency personnel with information needed in the right place, at the right time, and in a useful format. At NRC, management directives are issued to (1) promulgate internal policy and procedures of agencywide interest or application that concern a high profile, mission-critical agency function or program and (2) impose substantive requirements on more than one NRC office. Management directives do not propose new policy; instead, directives reflect policy decisions already made and provide the process and guidance for implementing that policy.

NRC MD 1.1, *NRC Management Directives System*, issued March 18, 2011, describes the process for issuing and revising directives. These directives are to be reviewed and reissued or certified as relevant at least every 5 years.

As of November 5, 2013, NRC maintained 164 MDs in its electronic catalog on NRC's Internal Web site. The average age of these 164 MDs is 8.3 years.

The audit objectives were to evaluate the adequacy of NRC's compliance with MD 1.1, particularly in the areas of keeping MDs accurate and up-to-date, and whether opportunities exist to improve the process.

Audit Results:

Although the agency strives for compliance with MD 1.1, NRC generally is not in compliance with keeping MDs accurate and up-to-date. Therefore, opportunities exist to improve program efficiency and increase compliance with MD 1.1 by (A) issuing MDs timely, and (B) centralizing authoritative guidance.

MDs Not Issued Timely

The issuance of NRC's management directives is not always timely. Federal regulations require that agencies make every effort to document policies and procedures and provide access to them in a timely manner. Additionally, agency policy requires MDs to be revised or certified as relevant every 5 years. The revision of NRC MDs is not always timely because there are multiple internal control weaknesses. As a result, agency operations may not be optimally performed and knowledge management programs may not be effective.

Authoritative Guidance Is Fragmented

Federal regulations and agency guidance require NRC to strive to provide staff with information needed in the right place, at the right time, and in a useful format to conduct agency business. However, NRC's MD system does not always contain up-to-date guidance. This is because the agency lacks sufficient internal controls over revisions made to MDs by yellow policy announcements.[7] As a result, staff may not have adequate, up-to-date guidance to conduct agency operations effectively, and staff could be confused or unsure about the correct guidance to follow.

(Addresses Management and Performance Challenge #7)

Audit of NRC's Method for Retaining and Documenting Information Supporting the Yucca Mountain Licensing Process

Proposed site of high-level waste repository at Yucca Mountain.
Source: NRC

OIG Strategic Goal: Safety

In 1983, *the Nuclear Waste Policy Act* assigned the Department of Energy (DOE) responsibility for constructing and operating a nuclear waste repository for high-level radioactive waste (HLW) and NRC the task of licensing and regulating the HLW repository. In 2002, President George W. Bush signed the *Yucca Mountain Development Act*, selecting Yucca Mountain as the site for the HLW repository. In 2008, DOE submitted to NRC a license application for construction authorization to build a HLW repository at Yucca Mountain, but subsequently filed a motion to withdraw its application for a construction authorization in March 2010. In October 2010, Gregory Jaczko, then NRC Chairman, directed NRC staff to prepare the orderly closeout of their technical safety review. Subsequently, in 2011, the Atomic Safety and Licensing Board Panel suspended[8] the adjudicatory hearing of the DOE's license application for the construction authorization of a HLW repository at Yucca Mountain.

Interested stakeholders pursued legal action to direct NRC to complete its technical safety review of the Yucca Mountain HLW repository construction authorization license application. This effort culminated in an August 2013 United States Court of Appeals for the District of Columbia Circuit Writ of Mandamus for NRC to continue with the Yucca Mountain licensing process using the $11.1 million in appropriated funds for Yucca Mountain. In complying with the Writ of Mandamus, NRC issued a Commission Order in November 2013 to finish the remaining volumes of the Safety Evaluation Report (SER).[9]

The audit objective was to determine if agency policy and procedures on document management are compliant with Federal requirements and provide reasonable assurance that documentation related to the review of the Yucca Mountain facility has been appropriately managed and retained.

Audit Results:

The records needed by NRC staff were available following the November 2013 Commission Order requiring the completion of the Yucca Mountain technical safety review. However, the Commission was out of compliance with the agency records management policy during the period of time that the licensing process was suspended.

---

[7] *The term "yellow policy announcement" refers to NRC's Policy Announcements that inform NRC employees of new or revised policy.*

[8] *OIG uses the terms "suspend," "suspended," or "suspension" to identify that the Yucca Mountain licensing process was postponed without a timeline for continuation.*

[9] *The review and evaluation of a license application is documented in an SER. For the Yucca Mountain licensing application, a total of five SER volumes were planned for issuance, one of which was completed and issued publicly prior to the suspension of the license application review.*

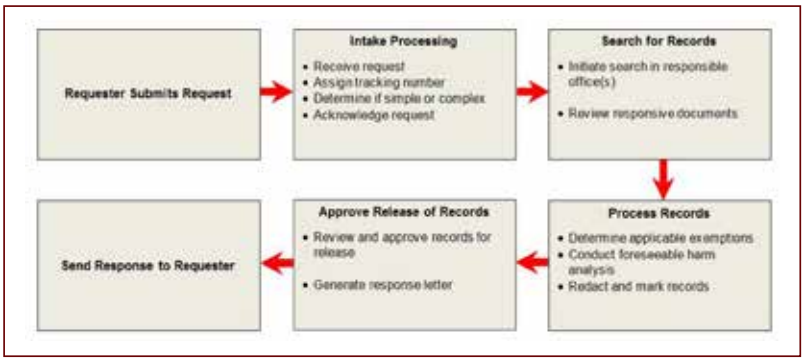
NRC did create a disposition schedule for the records in its possession in 2008, thus fulfilling the National Archives and Records Administration Federal requirement of establishing a retention schedule. Following the Writ of Mandamus issued in August 2013, and the resulting Commission Order, NRC has taken steps to come into compliance with the agency's records management policy.

(Addresses Management and Performance Challenge #4)

Audit of NRC's Freedom of Information Act Process

OIG Strategic Goal: Corporate Management

Freedom of Information Act Process



Source: NRC

The *Freedom of Information Act* (FOIA) is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government. NRC's FOIA program is managed by the FOIA, Privacy, and Information Collections Branch (FOIA office) within the Office of Information Services, Customer Service Division.

The FOIA process begins when the agency (1) receives – via mail, facsimile, or Internet – an incoming FOIA request, (2) assigns it a number, and (3) determines which NRC offices need to review their records to identify whether they have information pertinent to the request and sends a request to those offices. FOIA coordinators in responsive offices provide an estimate of the search, review, and duplication effort required to produce any documents identified as within the scope of the request.

The FOIA office then estimates the associated processing fees (for which the requester may be responsible), advises the requester as to the amount due, and assigns the request to the appropriate offices to identify and provide to the FOIA office all relevant documents from their office within an assigned timeframe. To facilitate appropriate disclosure of records, the FOIA coordinators consult as needed with agency staff in the responding offices and/or the Office of the General Counsel to prepare a response. The response is reviewed and signed by the FOIA officer and sent to the requester.

The audit objective was to determine whether the FOIA process is efficient and complies with the current laws.

Audit Results:

NRC generally responds to FOIA requests in accordance with Federal requirements. The agency meets the timeliness requirements for simple FOIA requests and adheres to the vast majority of FOIA regulations; however, opportunities exist to improve

program efficiency and increase Federal compliance by (A) fully using technology and enhancing training requirements and (B) adhering to review and approval regulations.

Operational Efficiency Could Be Improved

The efficiency of NRC's FOIA program can be improved by fully using available technology and enhancing agency training. Federal agencies should have the necessary tools and training to respond promptly and efficiently to FOIA requests. However, NRC management has not implemented effective internal controls. As a result, FOIA processing costs are high and the timeliness requirements are not consistently met.

Management Level Reviews Are Inconsistent

NRC is not in compliance with FOIA regulations as initial disclosure reviews of FOIA records are done at inconsistent management levels. Federal regulations state that, during the initial disclosure review, the head of the responsible office must review agency records to determine whether the agency records are exempt from disclosure; however, there is no enforcement of this policy and there is no method to track these reviews. Additionally, NRC's internal guidance differs from the Code of Federal Regulations. This may result in (A) a reduced number of discretionary releases or (B) the inadvertent release of sensitive information.

(Addresses Management and Performance Challenge #7)

Audit of NRC's Oversight of Reciprocity Licensees

OIG Strategic Goal: Safety

Reciprocity is NRC recognition of certain Agreement State[10] licenses for work performed in areas of NRC jurisdiction. Areas of NRC jurisdiction include non-Agreement States, areas of exclusive Federal jurisdiction, and offshore waters. The term reciprocity is also used in Agreement States to identify Agreement State recognition of an NRC license and licenses from other Agreement States for work performed in their jurisdiction.

Reciprocity authorizes Agreement State licensees to work in NRC jurisdiction for short periods of time without having to obtain a specific license. Thus, NRC regulations provide that any person who holds a specific license from an Agreement State is granted a general license[11] to conduct the same activity in NRC jurisdiction.

[10] *An Agreement State is any State with which NRC has entered into an agreement under subsection 274b of the Atomic Energy Act of 1954, as amended, that gives the State the authority to license and inspect byproduct, source, and noncritical quantities of special nuclear materials used or possessed within its borders.*

[11] *A general license is authorized by a regulation that sets forth the terms of the license. The reciprocity general license is defined in 10 CFR 150.20. In contrast, specific licenses are issued to named individuals who have filed an acceptable application to use certain types or quantities of radioactive materials.*

Being granted a general license by NRC is recognition of the Agreement State license and is referred to as reciprocity recognition.

Some types of activities conducted under reciprocity include radiography, portable gauge use, medical procedures, well-logging, leak-testing, and calibration.

The NRC regional offices – in particular, Regions I, III, and IV[12] – are primarily responsible for the implementation of reciprocity. Regional offices have the responsibility to review documents submitted by Agreement State licensees to ensure the proposed activities are in accordance with NRC regulations. The regional offices also schedule, conduct, and track inspections to achieve the overall objectives of the inspection program.

The audit objective was to determine whether NRC provides adequate oversight of Agreement State licensees operating in NRC jurisdiction under reciprocity.

Audit Results:

OIG determined that NRC provides adequate oversight to Agreement State licensees performing regulated activities in NRC jurisdiction. Therefore, OIG made no recommendations.

OIG identified and reviewed the following aspects of NRC oversight of Agreement State licensees operating in NRC jurisdiction under reciprocity:

- **Verification of information submitted.** OIG found that reciprocity recognitions, which Agreement State licensees must submit prior to conducting work in NRC jurisdiction, are processed in accordance with NRC regulations.

- **Communication with licensees and communication among NRC regions.** OIG found that NRC communicates with Agreement State licensees and regional offices communicate appropriately with one another.

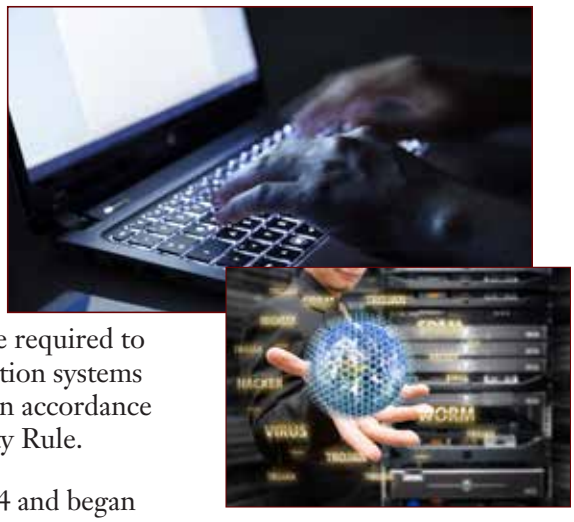
- **Inspections.** OIG found that NRC regions conduct inspections to ensure the safety and security of activities conducted under reciprocity.

- **Enforcement of NRC regulations.** OIG found that NRC issues enforcement sanctions against Agreement State licensees that fail to request reciprocity as required by NRC regulations. NRC also issues enforcement sanctions against Agreement State licensees that violate NRC regulations while conducting activities in NRC jurisdiction. When violations occur within NRC jurisdiction, NRC handles Agreement State licensees the same as an NRC licensee.

(Addresses Management and Performance Challenge #1)

[12] *In October 2003, all radioactive materials licensing and inspection functions in Region II were transferred to Region I.*

Audit of NRC's Cyber Security Program for Nuclear Power Plants



OIG Strategic Goal: Corporate Management

Cyber threats to NRC licensees are dynamic and multi-dimensional due to the continuously evolving capabilities of potential adversaries and emerging technologies. The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in digital systems that could be exploited either from outside or inside of a plant's protected area. Licensees operating a nuclear power plant are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks in accordance with 10 CFR 73.54, which is also known as the Cyber Security Rule.

In January 2013, NRC issued Temporary Instruction 2201/004 and began cyber security inspections of nuclear power plants in accordance with the Cyber Security Rule. The Cyber Security Rule required nuclear power plants licensed by NRC to submit a Cyber Security Plan with a proposed implementation schedule to the Commission for review and approval. However, the rule did not mandate an effective date for implementation of licensees' cyber security programs. As a result, NRC staff worked with the nuclear power industry to develop seven interim implementation milestones (i.e., Milestones 1-7) based on organizational and technical security controls to be used while licensees prepare for full implementation, which NRC and licensees commonly refer to as Milestone 8. NRC expects licensees to implement their respective Milestone 8 cyber security programs beginning in late calendar year 2014 through the end of calendar year 2017. NRC's Milestone 8 inspections will occur on a rolling basis as licensees come into full compliance with their regulatory commitments.

The audit objective was to determine the adequacy of NRC's cyber security inspection program for nuclear power plants.

Audit Results:

The audit determined that NRC has adequate management controls in place for the cyber security inspection program.[13] Although OIG did not identify any findings or make any recommendations, this report describes specific challenges related to resource management and inspection guidance as NRC moves toward full implementation of its cyber security inspection program

Management Controls for the Cyber Security Inspection Program

The Cyber Security Rule took effect in 2009 and established regulatory requirements for the nuclear power industry. Subsequent to the rule, NRC:

- Developed, in consultation with industry, an interim inspection program based on technical milestones.

[13] *Management controls include organizational structure and delegation of authority, human capital management, program monitoring, and communication with internal and external stakeholders.*

- Created a preliminary inspector training program for headquarters- and region-based staff.
- Performed pilot inspections at nuclear power plants and used those inspections to test and develop interim inspection guidance.
- Created a Cyber Security Directorate within the Office of Nuclear Security and Incident Response to consolidate program management in a single organization at NRC.
- Issued multiple supplementary guidance documents for use by NRC staff and licensees.
- Engaged industry stakeholders through conferences and staff meetings.

Challenges as the Program Moves Into Full Implementation

Resource Challenges

Milestone 8 will expand the current scope of cyber security inspections and create resource management challenges for NRC. Currently, NRC's inspection scope is limited to critical digital components and systems[14] associated with target set equipment.[15] Milestone 8 inspections will expand inspection scope to cover *all* critical digital components and systems with a safety, security, and emergency preparedness function. In addition, NRC will begin inspecting "balance of plant" equipment,[16] which traditionally falls under Federal Energy Regulatory Commission jurisdiction. Recruiting, retaining, and training adequate numbers of inspectors with appropriate skills, and determining the appropriate level of contractor support for inspections, is important to ensuring that NRC inspection teams are adequately staffed to conduct Milestone 8 inspections thoroughly and consistently in accordance with NRC standards.

Guidance Challenges

NRC faces challenges as it develops guidance for use by inspectors as well as licensees. In particular, sampling guidance for inspectors will become especially important with the expanded scope of Milestone 8 inspections. NRC is working to address this issue, in part through endorsement of industry-developed guidance for "consequence based analysis" of critical digital assets. Additionally, during early Milestone 1-7 inspections, some licensee performance problems were reportedly attributable to lack of alignment between industry and NRC guidance, as well as misinterpretation by licensees of key technical definitions. NRC can thus enhance the transparency of Milestone 8 inspections and foster regulatory stability by issuing clear guidance that incorporates lessons learned from prior inspections.

(Addresses Management and Performance Challenge #2)

---

[14] *NRC guidance refers to "critical digital assets," which are defined as digital assets that must be protected against cyber attacks in accordance with 10 CFR 73.54.*

[15] *A target set is defined as a minimum combination of equipment or operator actions that, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in radiological sabotage. Specifically, this entails significant core damage or a loss of coolant and exposure of spent fuel, barring extraordinary actions by plant operators.*

[16] *"Balance of plant" refers to the interface between a power plant and the electrical grid, such as electrical distribution equipment leading out to a plant's first inter-tie with the offsite distribution system.*

Audit of NRC's FY 13 Compliance with the Improper Payments Elimination and Recovery Act of 2010

OIG Strategic Goal: Corporate Management

On July 22, 2010, the *Improper Payments Elimination and Recovery Act* (IPERA) was signed into law, which amended the I*mproper Payments Information Act of 2002* (IPIA) and generally repealed the Recovery Auditing Act. IPERA also directed the Office of Management and Budget (OMB) to issue implementing guidance to agencies. IPERA requires Federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments.[17] In addition, IPERA requires each agency to conduct recovery audits[18] with respect to each program and activity of the agency that expends $1,000,000 or more annually, if conducting such audits would be cost-effective. On April 14, 2011, OMB issued Memorandum M-11-16, *Issuance of Revised Parts I and II to Appendix C of OMB Circular A-123*, as implementing guidance for the requirements of IPERA.

OMB guidance also specifies that each agency's Inspector General should review agency improper payment reporting in the agency's annual Performance and Accountability Report (PAR) or Annual Financial Report (AFR), and accompanying materials, to determine whether the agency complied with IPIA, as amended by IPERA.[19]

According to OMB guidance, compliance with IPIA, as amended by IPERA, means that the agency has:

- Published a PAR or AFR for the most recent fiscal year and posted that report and any accompanying materials required by OMB on the agency Web site.
- Conducted a program specific risk assessment for each program or activity that conforms with Section 3321 of Title 31 U.S.C (if required).
- Published improper payment estimates for all programs and activities identified as susceptible to significant improper payments under its risk assessment (if required).
- Published programmatic corrective action plans in the PAR or AFR (if required).
- Published, and has met, annual reduction targets for each program assessed to be at risk and measured for improper payments.

[17] *According to IPERA, an improper payment is (A) any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements; and (B) includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts. IPERA provides a detailed explanation of what is considered a "significant" improper payment (Section 2 (a) (3) (A)).*

[18] *Recovery audits are also referred to as "payment recapture audits."*

[19] *Although IPERA amends IPIA, the authorizing legislation is still named IPIA.*

- Reported a gross improper payment rate of less than 10 percent for each program and activity for which an improper payment estimate was obtained and published in the PAR or AFR.

- Reported information on its efforts to recapture improper payments.

If the agency does not meet one or more of these requirements, it is not compliant with IPIA, as amended by IPERA. The agency's Inspector General should also evaluate the accuracy and completeness of agency reporting and performance in reducing and recapturing improper payments.

The objective of this audit was to assess NRC's compliance with the IPERA and report any material weaknesses in internal control.

Audit Results:

Based on review of NRC's FY 2013 PAR and other documentation provided by the agency, OIG determined that the agency is in compliance with the requirements of IPERA. OIG has also concluded that agency reporting of improper payments is accurate and complete.

(Addresses Management and Performance Challenge #6)

Audits in Progress

Audit of NRC's Nuclear Reactor Safety Business Lines

OIG Strategic Goal: Corporate Management

The nuclear reactor safety business lines are a part of NRC's overall internal control framework for improving the accountability and effectiveness of NRC programs and operations. In compliance with the Federal Managers' Financial Integrity Act as well as OMB Circular A-123—*Management's Responsibility for Internal Control*—NRC has established business lines for major programs, including two nuclear reactor safety business lines. The responsible business line managers for these reactor safety business lines are the Directors of the Office of Nuclear Reactor Regulation and the Office of New Reactors.

Nuclear reactor safety business line managers establish internal control processes to reasonably ensure that the agency's internal controls comply with Federal and NRC requirements. This includes internal controls for both financial and non-financial, programmatic activities. As per MD 4.4, *Internal Control*, business line managers are required to develop and maintain an Internal Control Plan, assess risks, and test programmatic, non-financial internal controls.

The audit objective is to determine the extent to which NRC has developed effective reactor safety business line internal control processes for non-financial programmatic activities.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Receipt, Recordation, and Reconciliation of Revenue

OIG Strategic Goal: Corporate Management

The *Chief Financial Officer's Act* of 1990, as amended aimed to bring more effective financial management to the Federal Government and provide decision-makers with complete, reliable and timely financial information. The *Independent Offices Appropriation Act* requires NRC to charge fees to cover the costs of specific goods and services provided to the public. The *Omnibus Budget Reconciliation Act* of 1990, as amended, requires that NRC recover approximately 90 percent of its budget authority by collecting fees from its applicants and licensees.

Numerous NRC management directives support fee analysis, assessment, and collection requirements.

The audit objective is to determine whether NRC has established and implemented an effective system of internal control over the receipt, recordation, and reconciliation of fees owed to the agency.

(Addresses Management and Performance Challenge #6)

Audit of NRC's FY 2014 Financial Statements

OIG Strategic Goal: Corporate Management

Under the *Chief Financial Officers Ac*t and the *Government Management and Reform Act*, OIG is required to audit the financial statements of the NRC. OIG will measure the agency's improvements by assessing corrective action taken on prior audit findings. The report on the audit of the agency's financial statements is due on November 15, 2014. In addition, the OIG will issue reports on:

- Special Purpose Financial Statements.
- Implementation of the Federal Managers' Financial Integrity Act.
- Summary of Performance and Financial Information.

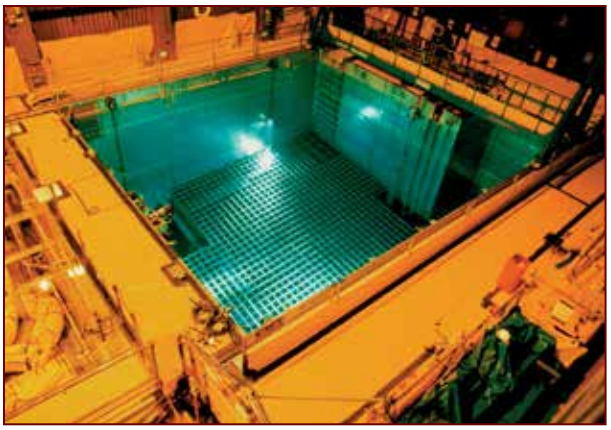
The audit has the following objectives:

- Express opinions on the agency's financial statements and internal controls.
- Review compliance with applicable laws and regulations.
- Review the controls in the NRC's computer systems that are significant to the financial statements.
- Assess the agency's compliance with Office of Management and Budget Circular A-123, Revised, *Management's Responsibility for Internal Control.*

(Addresses Management and Performance Challenge #6)

Audit of NRC's Oversight of Spent Fuel Pools

OIG Strategic Goal: Safety



Spent fuel pool.
Source: NRC

The tragic events of March 11, 2011, when an earthquake and tsunami struck Japan, damaging several reactors at the Fukushima Dai-ichi site, have brought increased attention to the spent fuel pools (SFPs) at nuclear power plants. All U.S. nuclear power plants store spent nuclear fuel in SFPs. These pools are made of reinforced concrete several feet thick, with steel liners. The water is typically about 40 feet deep, and serves both to shield the radiation and cool the fuel. Most SFPs at U.S. nuclear power plants were not originally designed to have a storage capacity for all the spent fuel generated by their reactors. SFP expansion through the use of high-density storage racks has been the technology most widely used to increase in-pool storage

capacity over the past 40 years. The majority of nuclear power plant operators have increased spent fuel storage capacity through re-racking their SFPs at least once. The nuclear industry has produced approximately 65,200 metric tons of commercial spent fuel over the past four decades, of which 75 percent is stored in SFPs, while the remainder is in dry storage casks. With the majority of spent fuel being stored in SFPs, the safe operation of these pools is essential to protecting public health, safety, and the environment.

NRC's requirements for SFPs can be found in 10 CFR. NRC staff use these rules to determine if fuel will remain safe under anticipated operating and accident conditions. There are requirements on topics such as radiation shielding, heat removal, and criticality. NRC also conducts inspections, verifying that spent fuel pools and related operations are consistent with a plant's license. SFP operations are inspected during each refueling outage.

The audit objective is to determine if NRC's oversight of spent fuel pools and the nuclear fuel they contain provides adequate protection for public health, safety, and the environment.

(Addresses Management and Performance Challenge #4)

Audit of NRC's Process for Ensuring Integrity in Scientific Research

OIG Strategic Goal: Safety

NRC is engaged in various research activities to include collecting, analyzing, and disseminating information about the operational safety of commercial nuclear power plants and certain nuclear materials activities. Additionally, NRC conducts research to reduce uncertainties in areas of potentially high safety risk or significance. NRC also engages in cooperative research with other Federal agencies, the nuclear industry, universities, and international partners.

Recently, there has been an effort throughout the Federal Government to ensure the highest level of integrity in scientific and technological processes. NRC commits to conducting its regulatory activities, including research, with integrity.

The audit objective is to determine whether NRC has controls in place to assure that scientific research is objective, credible, and transparent.

(Addresses Management and Performance Challenge #1)

Audit of NRC's Task Interface Agreement Process

OIG Strategic Goal: Safety

The Task Interface Agreement (TIA) process is used to address questions or concerns raised within the NRC regarding nuclear reactor safety and the related regulatory and oversight programs. The process should ensure that the concerns are resolved in a timely manner and that Office of Nuclear Reactor Regulation (NRR) responses are appropriately communicated.

A TIA is a written request for technical assistance to NRR from a regional or program office. A TIA contains questions on subjects involving regulatory or policy interpretations, specific plant events, or inspection findings. The requesting organization may use a TIA to obtain information on specific plant licensing basis; applicable staff positions for an issue, policy, or regulatory requirements interpretation; NRR technical positions; or the safety/risk significance of plant configurations or plant operating practices.

Ensuring that adequate, appropriate, and timely feedback is provided to NRC staff is central to the agency's mission to protect public health and safety and the environment.

The audit objective is to determine if the agency's TIA process facilitates effective and efficient responses.

(Addresses Management and Performance Challenge #3)

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for FY 2014

OIG Strategic Goal: Security

The *Federal Information Security Management Act* (FISMA) was enacted on December 17, 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act, which expired in November 2002. FISMA outlines the information security management requirements for agencies, including the requirement for an annual review and annual independent assessment by agency Inspectors General. In addition, FISMA includes new provisions such as the development of minimum standards for agency systems, aimed at further strengthening the security of the Federal Government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

FISMA provides the framework for securing the Federal Government's information technology, including both unclassified and national security systems. All agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their security programs.

The objective is to conduct an independent evaluation of the NRC's implementation of FISMA for FY 2014.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Information Technology Procurement Process

OIG Strategic Goal: Corporate Management

The information technology (IT) procurement process is that by which NRC obtains IT equipment and services to support its mission. Given the current budget environment in which Federal agencies must maintain IT readiness with constricted funds, it is essential that IT procurement be approached strategically as it significantly impacts whether the NRC will attain its vision, mission, and strategic goals. The recent OIG audit report, *Audit of NRC's Information Technology Governance*, highlighted the challenge NRC faces in funding IT to support mission needs. To support its mission, NRC must procure IT infrastructure and services economically, efficiently, and effectively.

According to Management Directive 11.1, *NRC's Acquisition of Supplies and Services*, "It is the policy of the U.S. Nuclear Regulatory Commission that the NRC's acquisition of supplies and services support the agency's mission; are planned, awarded, and administered efficiently and effectively; and are accomplished in accordance with applicable Federal statutes and procurement regulations. The primary implementing regulations are the Federal Acquisition Regulation (FAR) and the Nuclear Regulatory Commission Acquisition Regulation (NRCAR)." Entities with key IT procurement roles include NRC's Chief Information Officer, who establishes and ensures that appropriate agencywide IT resource acquisition policies, plans, and procedures are in place to meet the requirements of IT-related Federal statutes, regulations, and policies; and provides leadership and oversight for information technology, information management, and information systems security; and the Office of Information Services, which plans, directs, and oversees the delivery of the centralized information technology infrastructure, applications, and information management (IM) services, and the development and implementation of IT and IM plans, architecture, and policies.

The audit objective is to assess the effectiveness of NRC's IT procurement process in meeting the agency's current and future IT needs.

(Addresses Management and Performance Challenge #5)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC

OIG Strategic Goal: Corporate Management

In January 2000, Congress enacted the *Reports Consolidation Act* of 2000, which requires Federal agencies to provide an annual report that would consolidate financial and performance management information in a more meaningful and useful format for Congress, the President, and the public. Included in the act is a requirement that, on an annual basis, IGs summarize the most serious management and performance challenges facing their agencies. Additionally, the act provides that IGs assess their respective agency's efforts to address the challenges.

The audit has the following objectives:

- Identify the most serious management and performance challenges facing NRC.
- Assess the agency's efforts to address the management and performance challenges.

(Addresses all management and performance challenges)

Nuclear power station cooling tower.

NRC INVESTIGATIONS

During this reporting period, OIG received 119 allegations, initiated 12 investigations, and closed 19 cases. In addition, the OIG made 25 referrals to NRC management and one to the Department of Justice.

Investigative Case Summaries

Alleged Improper Communication with Contractor

OIG Strategic Goal: Corporate Management

OIG conducted an investigation based on an allegation that an NRC employee improperly wrote and dispatched a letter to a contractor involved in the operation and development of the NRC Radiological Assessment System for Consequences Analysis (RASCAL) computer system, for which the employee was the NRC project manager, urging the contractor to retain a particular employee. The RASCAL system is an important NRC tool for making independent dose and consequence projections during radiological incidents and emergencies.

NRC managers involved with the project indicated that the NRC employee had not sought or received authorization to send the letter to the contractor. NRC managers also indicated that the project manager had used a format that gave the letter the appearance of official correspondence on NRC letterhead, when it was in fact merely an e-mail document providing the employee's own personal views. OIG investigated this matter to determine whether the NRC employee's actions constituted a violation of Federal conflict of interest statutes and/or NRC regulations.

Investigative Results:

OIG found that the employee, while acting as NRC project manager for a contract to operate and develop the RASCAL system, e-mailed a letter to a manager employed by the contractor responsible in part for running and refining the system. In this correspondence, the NRC employee praised a particular contractor employee engaged on the project, asked that the employee be retained through December 2014, and suggested that contractor employee should remain involved in the contract through at least 2015.

This letter from the NRC employee to the contractor's manager bore an image of an NRC logo that was electronically pasted into the letter, giving an official appearance similar to that of NRC letterhead, even though the e-mail did not constitute or duplicate actual NRC letterhead. The appearance of the correspondence, in combination with the NRC employee's position as project manager concerning the contract, incorrectly conveyed the impression to the contractor that the views expressed in the letter were an official NRC agency position. When interviewed by the OIG, the employee admitted to sending this letter, and attributed the dispatch of the letter to a strong motivation to complete the project successfully. The employee attributed the use of the NRC logo

without clearance to inexperience with the proper procedures for handling official correspondence. While the dispatch of the letter and the use of the logo were not cleared by NRC management, OIG found no indications of any inappropriate personal financial relationship between the NRC employee and the contractor employee in question, and thus no indications of a violation of Federal conflict of interest statutes. The NRC employee retired from the Government in January 2014, while the investigation was still pending.

(Addresses Management and Performance Challenge #7)

Possible Hacking Attempt of NRC.Gov Web Site by a Member of the Public

OIG Strategic Goal: Security

OIG conducted an investigation into circumstances surrounding an e-mail being sent to NRC indicating that an individual had found a vulnerability on the public facing NRC.gov Web site and hacked into it. The individual reported being unable to gain access to NRC databases, but wanted to make a deal to provide all pertinent information regarding the intrusion.

OIG found the e-mail in question originated from a foreign country and coordinated its investigation with the Federal Bureau of Investigation (FBI). This coordination revealed the individual identified by OIG was the subject of a multi-State investigation for hacking and extortion.

The OIG investigation found that an NRC server, which housed the public facing NRC.gov Web site, had been compromised as early as April 2011. However, the applications placed on the server during the compromise were not used to access the NRC network or gain access to NRC internal resources.

The OIG investigation also found that the server had not been fully scanned by the NRC and it was not until a subsequent quarterly full scan in 2012 that the NRC identified vulnerabilities that were used by someone to gain unauthorized access into the public facing NRC.gov Web site. OIG coordinated the investigation with NRC officials and learned the NRC now has additional tools to scan NRC servers regularly to identify vulnerabilities and as well has alerts in place that notify NRC officials of any changes to NRC's applications.

(Addresses Management and Performance Challenge #5)

NRC Chairman Allegedly Violated Ex-Parte Communications During a Meeting with Stakeholders Involving Seabrook Nuclear Power Plant

OIG Strategic Goal: Corporate Management

OIG completed an investigation into an allegation that the current NRC Chairman violated 10 CFR 2.347 (Ex-parte Communications) when she met with selected representatives of several citizens groups at the Seabrook Nuclear Power Plant in Seabrook, NH, on November 7, 2013, and discussed adjudicatory matters regarding licensing proceedings. A local newspaper reported that the NRC Chairman visited the Seabrook Nuclear Power Plant earlier in November 2013 and, while there, invited parties (interest groups) presented concerns to the NRC Chairman. According to the article, each group presented specific concerns to the NRC Chairman regarding the concrete degradation that was allegedly impacting structural integrity in safety structures at the plant, the belief that the plant should not be relicensed based on a history of inadequate plant management and weak NRC oversight, the fact that climate changes will affect the relicensing period of 2030-2050, and about NRC practices that make information needed by the public inaccessible. The article indicated that the NRC Chairman listened, but the article did not indicate any statements made by the NRC Chairman.

An alleger, reading the article, believed the NRC Chairman engaged in ex-parte communications by meeting citizens in private and having discussions regarding licensing proceedings.

Investigative Results:

The OIG investigation determined the NRC Chairman was made aware of topics that she should not discuss regarding the Seabrook license renewal. Further, the investigation determined the NRC Chairman was careful about the discussions she held with the stakeholders and she did not engage in any substantive discussion during the site visit about any of the issues that had been raised in the ongoing adjudication associated with the license renewal application for Seabrook Station, Unit 1.

OIG reviewed a document that was made available to the public and provided to several parties to inform the parties that the NRC Chairman would be touring Seabrook Station, Unit 1 to obtain a general familiarity with the facility. The notice stated that the NRC Chairman would not engage in any substantive discussion during the site visit about any of the issues that had been raised in the ongoing adjudication associated with the license renewal application for Seabrook Station, Unit 1.

The investigation also determined the NRC Chairman's office issued a "Notice to the Parties" in the Seabrook licensing renewal proceeding regarding the contested issue of alkali-silica reaction (ASR) in concrete that was discussed when the NRC Chairman visited the Seabrook Nuclear Power Plant. The notice was written to inform the parties pursuant to 10 CFR § 2.347(c), that during both the site visit with the licensee and the meeting with representatives certain interest groups, the subject of ASR, was raised. OIG did not identify any evidence of misconduct by the NRC Chairman.

(Addresses Management and Performance Challenge #7)

Preselection for NRC Vacancy Announcement by an NRC Manager

OIG Strategic Goal: Corporate Management

OIG completed an investigation into an allegation that an NRC manager named individuals that were to fill vacancies before a related vacancy announcement closed and improperly preselected individuals for the vacancy.

Investigative Results:

OIG found that the NRC manager provided false material statements to the OIG while under oath and preselected employee candidates prior to the completion of the certified eligibility lists. OIG also found that the manager told an NRC human resources employee that the manager wanted to hire the same individuals prior to the closing date of the vacancy, and the issuance of the certified lists. The OIG investigation determined the manager's actions gave the appearance to NRC staff that the manager was not impartial in the selection, and violated 5 CFR, Section 2301, *Merit System Principles*, regarding fair and open competition of applicants, and 5 CFR, Section 2302, *Prohibited Personnel Practices.*

(Addresses Management and Performance Challenge #7)

NRC Employees Targeted for Logon Credential Harvesting

OIG Strategic Goal: Security

OIG completed an investigation into information that an e-mail was sent to more than 5,000 NRC employee e-mail addresses, of which 4,149 were valid, from an edu address, with the subject line of "System Administrator." The e-mail stated it was being sent because the in box had almost exceeded its limit, and that the receiver should go to a link provided, to update their account information and mail box quota.

Eight employees executed the command to access the link and provided their login information.

Investigative Results:

The OIG investigation found that some of the Internet Protocol (IP) addresses related to the e-mail were part of a known Nigerian money scam scheme. The e-mail link redirected users to a form that had fields for the recipient to provide their NRC network username and password. Of the more than 5,000 e-mails sent, of which 4,149 were valid e-mail addresses, 8 NRC employees clicked on the link and provided their NRC network login credential information. NRC directed the employees to change their passwords to address the vulnerability. OIG learned that no malware was downloaded to these employees' computers from the link.

The OIG Cyber Crimes Unit (CCU) investigation determined the e-mail in question originated from a compromised educational e-mail account of a university graduate student.

The CCU reviewed logs from the Web site hosting provider that hosted the Web page containing the login prompt used to capture the NRC employees' login information. A review of the logs revealed the account was created and all connections were from an IP address located in Nigeria.

The CCU briefed the appropriate NRC officials on the results of this investigation, enabling them to take appropriate action to prevent further compromise of NRC employees' network account information.

(Addresses Management and Performance Challenge #5)

Grand Gulf nuclear power station. Photo courtesy Entergy-nuclear

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created the Defense Nuclear Facilities Safety Board (Board) as an independent agency within the Executive Branch to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's (DOE) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. Since DOE is a self-regulating entity, the Board constitutes the only independent technical oversight of operations at the Nation's defense nuclear facilities. The Board is composed of experts in the field of nuclear safety with demonstrated competence and knowledge relevant to its independent investigative and oversight functions.

The Consolidated Appropriations Act, 2014, provided that notwithstanding any other provision of law, the Inspector General of the Nuclear Regulatory Commission is authorized in 2014 and subsequent years to exercise the same authorities with respect to the Defense Nuclear Facilities Safety Board, as determined by the Inspector General of the Nuclear Regulatory Commission, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the Nuclear Regulatory Commission.

DNFSB AUDITS

To help the Board improve the efficiency and effectiveness of their programs and operations, OIG completed two program audits and has four audits in progress.

Audit Summaries

Audit of the Board's Purchase Card Program

The Governmentwide Purchase Card Program was established in the late 1980s as a way for agencies to streamline Federal acquisition processes. Purchase cards provide a low-cost, efficient vehicle for obtaining goods and services directly from vendors. They can be used for micro-purchases,[20] as well as to place orders and make payments on contract activities.

The General Services Administration (GSA) oversees the Governmentwide Purchase Card Program. GSA contracts with several banks, including Citibank — the bank used by the Board — to provide purchase cards to Federal employees. The Federal Acquisition Regulation, which is the primary procurement authority for agencies, was reissued in March 2005.

[20] *A micro-purchase is an acquisition of supplies or services in which the aggregate amount does not exceed $3,000. For services subject to the Service Contract Act, the amount cannot exceed $2,500. For construction projects subject to the Davis-Bacon Act, the limit is $2,000.*

Oversight of the Governmentwide Purchase Card Program is also the responsibility of OMB. In August 2005, OMB issued Circular A-123, Appendix B, *Improving the Management of Government Charge Card Programs*,[21] which establishes minimum requirements and suggests best practices for agency purchase card programs. This circular requires each agency to develop and maintain written policies and procedures for use of purchase cards.

On October 5, 2012, the President signed into law the *Government Charge Card Abuse Prevention Act* of 2012. This act requires agencies to establish and maintain safeguards and internal controls for Government charge cards and establishes additional reporting and audit requirements.

The Board has had a purchase card program in place since late 1998. In December 2005, the Board issued Administrative Directive 211.2, *Charge Card Management Program*, which serves as the principal guide for the Board's charge card programs. The Board has an updated directive currently in draft. *DNFSB Purchase Card Policy and Procedures*[22] is a supplement to the directive and was last revised in April 2012.

Administrative Directive 211.2 sets forth the policies, procedures, and responsibilities associated with the Board's charge card programs. The Board has a designated Program Coordinator for the purchase card program who is responsible for day-to-day program management. The Program Coordinator provides oversight of the purchase card program and serves as the liaison between cardholders and the contracting bank.

The audit objective was to determine whether internal controls are in place and operating effectively to maintain compliance with applicable purchase card laws, regulations, and Board policies.

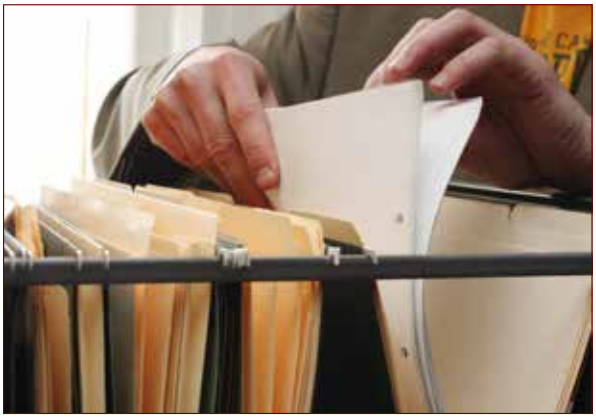
Audit Results:

The Board's purchase card program internal controls are generally in place and operating effectively to maintain compliance with applicable purchase card laws. The Board appeared to use its purchase cards appropriately during the period under review and no instances of fraud, waste, or abuse were identified. However, opportunities exist to improve internal controls and Federal compliance. Specifically, some of the purchase card controls are incomplete, outdated, or not fully implemented. The purchase card internal controls need improvement because the Board's management has not (1) sufficiently addressed key topics in their existing policies and procedures, (2) updated Administrative Directive 211.2, (3) submitted Administrative Directive 211.2 to OMB, or (4) enforced all of the internal controls written into the directive. As a result, internal controls are less effective and the potential for personal use, misuse, or loss is increased.

[21] *OMB Circular A-123, Appendix B, Improving the Management of Government Charge Card Programs, was last revised on January 15, 2009.*

[22] *This is the official title of the Board's purchase card policy and procedure document.*

Audit of the Board's Freedom of Information Act Process



FOIA is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government. In response to such written requests, Federal agencies must disclose the requested records, unless they are protected from release under one of the nine FOIA statutory exemptions.

In 2009, the President and the Attorney General each issued memoranda emphasizing that the FOIA "should be administered with a clear presumption: in the face of doubt, openness prevails." The President also directed agencies to "take affirmative steps to make information public" and not to "wait for specific requests from the public."

The General Manager within the Office of the General Manager is the Chief FOIA Officer and manages the Board's FOIA program. During fiscal year 2013, Board staff processed 14 FOIA requests.

The audit objective was to determine whether the Board's FOIA process is efficient and complies with the current laws.

Audit Results:

The Board generally meets FOIA timeliness requirements; however, opportunities exist to enhance program efficiency and compliance with Federal and internal guidance by improving internal controls, training, and FOIA document management. Specifically, OIG found that Board staff do not always follow FOIA guidance when searching for records and responding to FOIA requests. The Board is required to adhere to Federal and internal FOIA guidance. However, management has not implemented effective internal controls and made FOIA training available to all Board staff. As a result, inaccurate and incomplete FOIA responses have occurred.

Auditors also found that FOIA documentation at the Board is dispersed and not efficiently maintained. The Board has not designed and implemented controls for FOIA documentation management. As a result, inefficiencies exist and there is an increased potential for misplaced or lost FOIA documents at the Board.

Audits in Progress

Audit of the Board's FY 2014 Financial Statements

Under the Chief Financial Officers Act, as updated by the Accountability of Tax Dollars Act of 2002 and OMB Bulletin 14-02 (Audit Requirements for Federal Financial Statements), OIG is required to audit the financial statements of the Board. OIG will measure the agency's improvements by assessing corrective action taken on prior audit findings. The report on the audit of the agency's financial statements is due on November 15, 2014. In addition, OIG will issue reports on the Board's implementation of the Federal Managers' Financial Integrity Act.

The audit has the following objectives:

- Express opinions on the agency's financial statements and internal controls,
- Review compliance with applicable laws and regulations.
- Review the controls in the DNFSB's computer systems that are significant to the financial statements.
- Assess the agency's compliance with OMB Circular A-123, Revised, *Management's Responsibility for Internal Control.*

Audit of the Board's Travel Card and Travel Program

The *Government Charge Card Abuse Prevention Act of 2012* (Charge Card Act), Public Law 112-194, requires all executive branch agencies to establish and maintain safeguards and internal controls for charge cards. OMB provided supplemental guidance through Memorandum M-13-21, *Implementation of the Government Charge Card Abuse Prevention Act of 2012*, dated September 6, 2013. The guidance requires each agency head to provide an annual certification that the appropriate policies and controls are in place or that corrective actions have been taken to mitigate the risk of fraud and inappropriate charge card practices. The annual certification should be included as part of the existing annual assurance statement under the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512(d)(2)).

Under the Charge Card Act, IGs are required to conduct periodic risk assessments of agency charge card programs to analyze the risks of illegal, improper, or erroneous purchases. These risk assessments shall be used by OIGs to determine whether an audit or review should be performed and what the nature, scope, and timing of the audit should be. OIG conducted a risk assessment for the Board Travel Card Program. As a result of this risk assessment, OIG has determined that an audit of the Board's Travel Card and Travel Program should be performed.

The audit objective is to determine whether internal controls are in place and operating effectively to maintain compliance with applicable travel card and travel program laws, regulations, and Board policies.

Independent Evaluation of the Board's Implementation of FISMA for FY 2014

FISMA was enacted on December 17, 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act, which expired in November 2002. FISMA outlines the information security management requirements for agencies, including the requirement for an annual review and annual independent assessment by agency Inspectors General. In addition, FISMA includes new provisions such as the development of minimum standards for agency systems, aimed at further strengthening the security of the Federal Government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

FISMA provides the framework for securing the Federal Government's information technology including both unclassified and national security systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget and Congress on the effectiveness of their security programs.

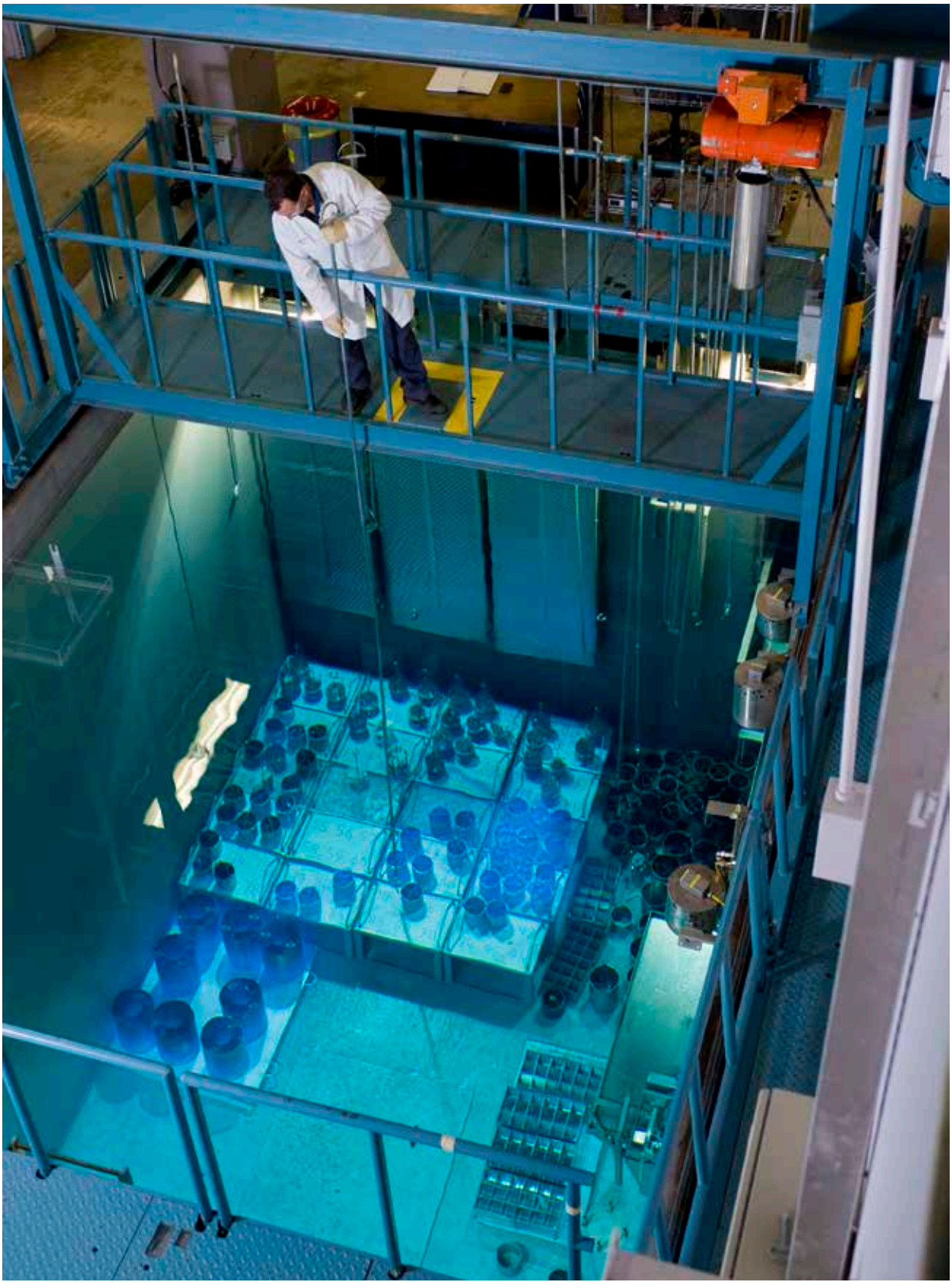
The objective is to conduct an independent evaluation of the Board's implementation of FISMA for FY 2014.

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Board

In January 2000, Congress enacted the *Reports Consolidation Act of 2000*, which requires Federal agencies to provide an annual report that would consolidate financial and performance management information in a more meaningful and useful format for Congress, the President, and the public. Included in the act is a requirement that, on an annual basis, IGs summarize the most serious management and performance challenges facing their agencies. Additionally, the act provides that IGs assess their respective agency's efforts to address the challenges.

The objectives are to:

- Identify the most serious management and performance challenges facing the Board.
- Assess the agency's efforts to address the management and performance challenges.



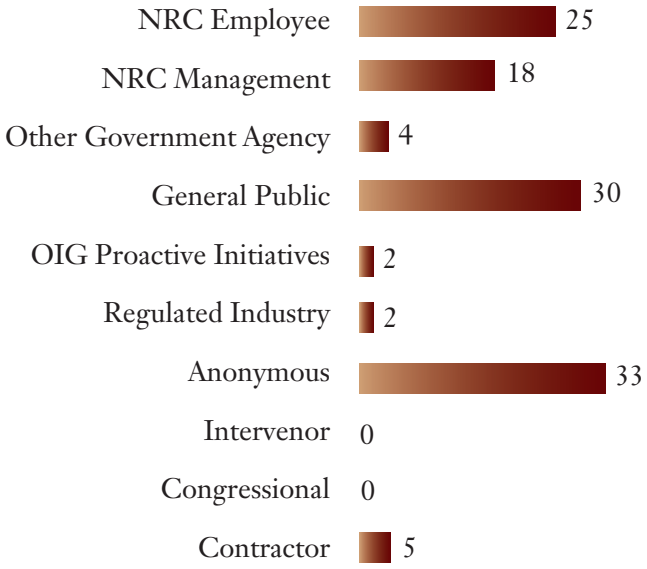
Commercial nuclear irradiator.

SUMMARY OF NRC OIG ACCOMPLISHMENTS

April 1, 2014, through September 30, 2014

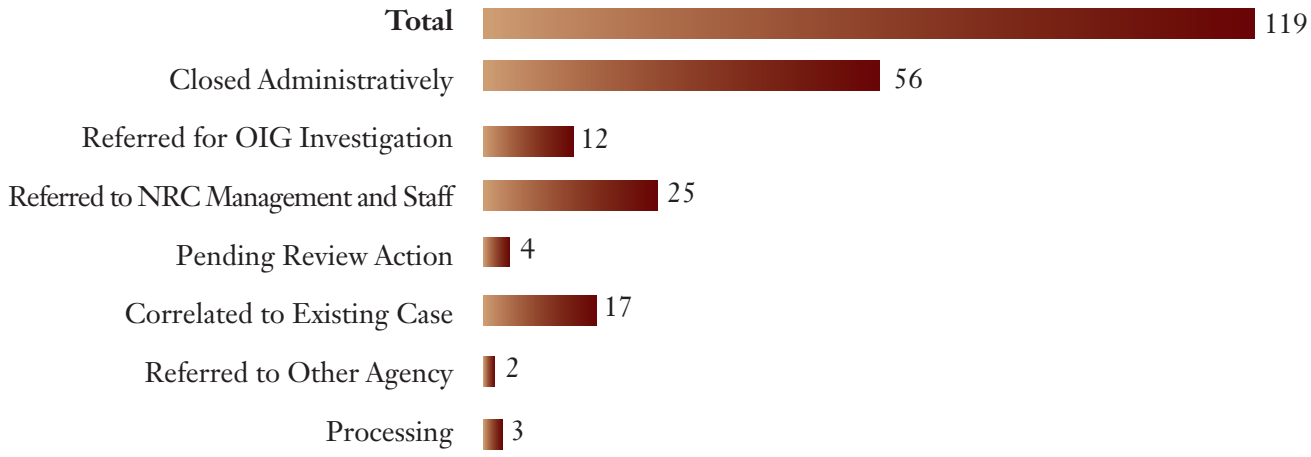
Investigative Statistics

Source of Allegations



Allegations resulting from Hotline calls: 11 **Total: 119**

Disposition of Allegations



Status of Investigations

DOJ Referrals 1
DOJ Acceptance 0
DOJ Pending 2
DOJ Declinations 1
Criminal Convictions 0
Criminal Penalty Fines 0
NRC Administrative Actions:
- Counseling and Letter of Reprimand 1
- Terminations and Resignations 4
- Suspensions and Demotions 0
- Other (Letter from Chairman and Review of Policy) 0

State Referrals 1
State Declinations 0
State Accepted 0
PFCRA[22] Referral 1
PFCRA Acceptance 0
PFCRA Declinations 0

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Cases in Progress
Conflict of Interest	0	2	1	1
Employee Misconduct	12	3	7	8
Event Inquiry	0	0	0	0
External Fraud	5	1	0	6
False Statements	3	0	0	3
Management Misconduct	17	2	8	11
Miscellaneous	3	3	3	3
Proactive Initiatives	9	0	0	9
Technical Allegations	4	1	0	5
Theft	1	0	0	1
Grand Total	**54**	**12**	**19**	**47**

[22] *Program Fraud Civil Remedies Act.*

Audit Listings

Date	Title	Audit Number
09/30/2014	Audit of the Board's Freedom of Information Act Process	DNFSB-14-A-02
09/29/2014	Audit of NRC's Communications Security Program	OIG-14-A-21
09/29/2014	Audit of the Board's Purchase Card Program	DNFSB-14-A-01
09/15/2014	Audit of NRC's Sequestration Process	OIG-14-A-20
09/15/2014	Audit of NRC's Process for Revising Management Directives	OIG-14-A-19
07/23/2014	Audit of NRC's Method for Retaining and Documenting Information Supporting the Yucca Mountain Licensing Process	OIG-14-A-18
06/16/2014	Audit of NRC's Freedom of Information Act Process	OIG-14-A-17
05/22/2014	Audit of NRC's Oversight of Reciprocity Licensees	OIG-14-A-16
05/07/2014	Audit of NRC's Cyber Security Inspection Program for Nuclear Power Plants	OIG-14-A-15
04/08/2014	Audit of NRC's FY13 Compliance With the Improper Payments Elimination & Recovery Act of 2010	OIG-14-A-14

Contract Audit Reports

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs	Unsupported Costs
04/10/2014	**Dade Moeller & Associates** Independent Evaluation of Dade Moeller & Associates' Fiscal Year 2014 Provisional Billing Rates NRC-HQ-11-C-04-0012	0	0
04/22/2014	**Southwest Research Institute** Independent Evaluation of Southwest Research Institute Major Contractor Labor FY 2012 Floor Check NRC-02-04-014 NRC-02-06-018 NRC-02-06-021 NRC-02-07-006 NRC-03-09-070 NRC-03-10-066 NRC-03-10-070 NRC-03-10-078 NRC-03-10-081 NRC-04-07-108 NRC-04-10-144 NRC-41-08-004 NRC-41-09-011 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058	0	0
09/03/2014	**Southwest Research Institute** Independent Evaluation of Southwest Research Institute Major Contractor Labor FY 2013 Floor Check NRC-02-04-014 NRC-02-06-018 NRC-02-06-021 NRC-02-07-006 NRC-03-09-070 NRC-03-10-066 NRC-03-10-070 NRC-03-10-078 NRC-03-10-081 NRC-04-07-108 NRC-04-10-144 NRC-41-08-004 NRC-41-09-011 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058	0	0

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs	Unsupported Costs
09/09/2014	**Southwest Research Institute** Independent Audit of Southwest Research Institute's March 12, 2014 Forward Pricing Rate Proposal NRC-02-04-014 NRC-02-06-018 NRC-02-06-021 NRC-02-07-006 NRC-03-09-070 NRC-03-10-066 NRC-03-10-070 NRC-03-10-078 NRC-03-10-081 NRC-04-07-108 NRC-04-10-144 NRC-41-08-004 NRC-41-09-011 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058	0	0

Audit Resolution Activities

TABLE I

OIG Reports Containing Questioned Costs[24]

Reports		Number of Reports	Questioned Costs (Dollars)	Unsupported Costs (Dollars)
A.	For which no management decision had been made by the commencement of the reporting period	0	0	0
B.	Which were issued during the reporting period	0	0	0
	Subtotal (A + B)	0	0	0
C.	For which a management decision was made during the reporting period:			
	(i) dollar value of disallowed costs	0	0	0
	(ii) dollar value of costs not disallowed	0	0	0
D.	For which no management decision had been made by the end of the reporting period	0	0	0

[24] *Questioned costs are costs that are questioned by OIG because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; a finding that, at the time of the audit, such costs are not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.*

TABLE II

OIG Reports Issued with NRC Recommendations That Funds Be Put to Better Use[25]

Reports		Number of Reports	Dollar Value of Funds
A.	For which no management decision had been made by the commencement of the reporting period	0	0
B.	Which were issued during the reporting period	0	0
C.	For which a management decision was made during the reporting period:		
	(i) dollar value of recommendations that were agreed to by management	0	0
	(ii) dollar value of recommendations that were not agreed to by management	0	0
D.	For which no management decision had been made by the end of the reporting period	0	0

[25] *A "recommendation that funds be put to better use" is a recommendation by OIG that funds could be used more efficiently if NRC management took actions to implement and complete the recommendation, including reductions in outlays; deobligation of funds from programs or operations; withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; costs not incurred by implementing recommended improvements related to the operations of NRC, a contractor, or a grantee; avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or any other savings which are specifically identified.*

TABLE III

NRC Significant Recommendations Described in Previous Semiannual Reports on Which Corrective Action Has Not Been Completed

Date	Report Title	Number
5/26/2003	**Audit of NRC's Regulatory Oversight of Special Nuclear Materials**	**OIG-03-A-15**
	Recommendation 1: Conduct periodic inspections to verify that material licensees comply with material control and accountability (MC&A) requirements, including, but not limited to, visual inspections of licensees' special nuclear material (SNM) inventories and validation of reported information.	
	Recommendation 3: Develop and implement a quality assurance process that ensures that collected enforcement data is accurate and complete.	
2/02/2009	**Audit of the Committee to Review Generic Requirements**	**OIG-09-A-06**
	Recommendation 1: Develop, document, implement, and communicate an agencywide process for reviewing backfit issues to ensure that generic backfit are appropriately justified based on NRC regulations and policy.	
7/12/2012	**Audit of NRC's Inspections, Test, Analyses and Acceptance Criteria (ITAAC) Process**	**OIG-12-A-16**
	Recommendation 10: Develop and implement a change management process to address future change in the ITAAC process that can create barriers to effective communication and coordination.	

ABBREVIATIONS AND ACRONYMS

AFR	Annual Financial Report
CCU	Computer Crimes Unit
CFR	Code of Federal Regulations
COMSEC	Communications Security
DH	Directive Handbook
DOE	Department of Energy
DNFSB	Defense Nuclear Facilities Safety Board
DOJ	Department of Justice
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigations
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FY	fiscal year
GSA	General Services Administration
HLW	high-level radioactive waste
HOC	Headquarters Operations Center (NRC)
IAM	Issue Area Monitor
IG	Inspector General
IM	information management
IP	Internet Protocol
IPERA	Improper Payments Elimination and Recovery Act
IPIA	Improper Payments Information Act of 2002
IT	information technology
ITAAC	inspections, tests, analyses, and acceptance criteria
MD	Management Directive
NRC	U.S. Nuclear Regulatory Commission
NRCAR	Nuclear Regulatory Commission Acquisition Regulation
NRR	Office of Nuclear Reactor Regulation (NRC)
OCFO	Office of the Chief Financial Officer (NRC)
OEDO	Office of the Executive Director for Operations (NRC)
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PAR	Performance and Accountability Report
SER	safety evaluation report
SFP	spent fuel pool
STE	secure terminal equipment
TIA	Task Interface Agreement

REPORTING REQUIREMENTS

The Inspector General Act of 1978, as amended (1988), specifies reporting requirements for semiannual reports. This index cross-references those requirements to the applicable pages where they are fulfilled in this report.

Citation	Reporting Requirements	Page
Section 4(a)(2)	Review of Legislation and Regulations	6–8
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	11–22, 30–34, 36–38
Section 5(a)(2)	Recommendations for Corrective Action	11–22, 36–38
Section 5(a)(3)	Prior Significant Recommendations Not Yet Completed	49
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	43
Section 5(a)(5)	Information or Assistance Refused	None
Section 5(a)(6)	Listing of Audit Reports	44
Section 5(a)(7)	Summary of Significant Reports	11–22, 30–34, 36–38
Section 5(a)(8)	Audit Reports — Questioned Costs	47
Section 5(a)(9)	Audit Reports — Funds Put to Better Use	48
Section 5(a)(10)	Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made	None
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions With Which the OIG Disagreed	None

Sec. 989C. of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111-203) requires Inspectors General to include the results of any peer review conducted by another Office of Inspector General during the reporting period; or if no peer review was conducted, a statement identifying the date of the last peer review conducted by another Office of Inspector General; and a list of any peer review conducted by the Inspector General of another Office of the Inspector General during the reporting period.

Section 989C.	Peer Review Information	52

APPENDIX

Peer Review Information

The OIG Audit and Investigative Programs undergo a peer review every three years.

Peer Reviews of NRC OIG Conducted by Another Office of Inspector General

Investigations

The NRC OIG Investigative program was peer reviewed most recently by the Corporation for National and Community Service Office of Inspector General on September 16, 2013.

Audits

The NRC OIG Audit Program was peer reviewed most recently by the National Archives and Records Administration Office of Inspector General on September 27, 2012.

Peer Reviews by NRC OIG Conducted of Another Office of Inspector General

During this reporting period, NRC OIG peer reviewed the U.S. Government Printing Office audit organization.

NRC OIG also peer reviewed the Agency for International Development investigative opperations organization.

OIG STRATEGIC GOALS

1. Safety: Strengthen NRC's efforts to protect public health and safety and the environment.
2. Security: Enhance NRC's efforts to increase security in response to an evolving threat environment.
3. Corporate Management: Increase the economy, efficiency, and effectiveness with which NRC manages and exercises stewardship over its resources.

The NRC OIG Hotline

The Hotline Program provides NRC employees, other Government employees, licensee/utility employees, contractors, and the public with a confidential means of reporting suspicious activity concerning fraud, waste, abuse, and employee or management misconduct. Mismanagement of agency programs or danger to public health and safety may also be reported. We do not attempt to identify persons contacting the Hotline.

What should be reported:

- Contract and Procurement Irregularities
- Conflicts of Interest
- Theft and Misuse of Property
- Travel Fraud
- Misconduct
- Abuse of Authority
- Misuse of Government Credit Card
- Time and Attendance Abuse
- Misuse of Information Technology Resources
- Program Mismanagement

Ways To Contact the OIG

Call:
OIG Hotline
1-800-233-3497
TDD: 1-800-270-2787
7:00 a.m. – 4:00 p.m. (EST)
After hours, please leave a message.

Submit:
Online Form
www.nrc.gov
Click on Inspector General
Click on OIG Hotline

Write:
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program, MS O5 E13
11555 Rockville Pike
Rockville, MD 20852-2738

NUREG-1415, Vol. 28, No. 1
October 2014