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

Office of the Inspector General

Semiannual Report to Congress

April 1, 2013–September 30, 2013

OIG VISION

"We are agents of positive change striving for continuous improvement in our agency's management and program operations."

OIG MISSION

NRC OIG's mission is to (1) independently and objectively conduct and supervise audits and investigations relating to NRC's programs and operations; (2) prevent and detect fraud, waste, and abuse; and (3) promote economy, efficiency, and effectiveness in NRC's programs and operations.

COVER PHOTO:

McGuire Nuclear Station.
Photo coutesy of Duke Energy, LLC

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, 2013, to September 30, 2013.

Our work reflects the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse through the conduct of audits and investigations relating to NRC programs and operations. The audits and investigations highlighted in this report demonstrate our commitment to ensuring integrity and efficiency in NRC's programs and operations.

During this reporting period, we focused our efforts on agency programs and operations that are critical to the success of the agency's core safety and security mission. Our work focused on areas such as compliance with the regulations set forth in 10 CFR Part 51, adherence to the "Reducing Over-Classification Act," and compliance with NRC access authorization policies. Our efforts in focusing on these areas are designed to assist the agency in making attentive, meaningful, and consistent programmatic and management decisions that maximize efficiency and effectiveness.

NRC's ability to effectively accomplish its safety and security mission is influenced by the effectiveness of its corporate management programs in areas such as information technology and financial resources. One of OIG's strategic goals is to increase the economy, efficiency, and effectiveness with which NRC manages and exercises stewardship over its resources. In this edition of the *Semiannual Report*, we highlighted our efforts in identifying and addressing the risks associated with the principal corporate management areas of the NRC, such as protecting Safeguards Information, preventing and detecting misuse in the travel charge card program, proper financial control over the budget execution process, and information technology readiness for Three White Flint North.

During this semiannual reporting period, we issued seven program 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. OIG also opened 39 investigations, and completed 35 cases. Seven of the open cases were referred to the Department of Justice, and six allegations were referred to NRC management for action.

The NRC OIG remains committed to the integrity, efficiency, and effectiveness of NRC programs and operations, and our audits, investigations, and other activities highlighted in this report demonstrate this ongoing commitment. OIG continuously strives to maintain the highest possible standards of professionalism and quality in their 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 agency to address OIG findings and to implement recommended corrective actions timely. 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 operations.

Hubert T. Bell
Inspector General

Virgil C. Summer nuclear power station. *Photo courtesy of South Carolina Electic & Gas Company*

Contents

Keewaunee nuclear power station. *Photo courtesy of Dominion Power.*

Highlights

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

Audits

- The U.S. Nuclear Regulatory Commission (NRC) developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI) documents. SLES features two distinct components: a secure wireless Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents. The SGI LAN component is a network with a secure architecture and is dedicated for use in SGI data processing. The E-Safe component is a secure electronic data repository for SGI records. E-Safe users are able to create, capture, search, and retrieve data from this repository. The adoption of these various techniques into SGI operations was intended to ensure that E-Safe will contain all SGI created or received by NRC, thereby eliminating the need to maintain separate, individual collections of SGI. The audit objective was to determine if SLES meets its operational capabilities and applicable security controls.

- NRC established its travel charge card program to facilitate employee travel in support of the agency's mission. Specifically, the purpose for using Government travel charge cards (referred to as travel cards) is to reduce the overall cost of travel to the Federal Government through lower administrative costs and by taking advantage of rebates offered by card vendors based on the volume of transactions and on prompt payment of bills. The Federal Travel Regulation mandates the use of travel cards for all official travel expenses unless specifically exempted. Under the program, travel cards can be used to pay for expenses related to official Government travel, such as lodging, meals, and rental cars. During fiscal year (FY) 2011, approximately $16.8 million was charged for NRC travel under this program. The audit objective was to assess the adequacy and effectiveness of NRC's policies, procedures, and internal controls over the travel card program for preventing and detecting travel charge card misuse and delinquencies.

- The U.S. Government requires Federal agencies to establish an effective funds control process to ensure funds are used only for the purpose set forth by Congress and that expenditures do not exceed amounts authorized. The NRC budget process consists of strategic planning, budget formulation, submission of the agency's budget to the Office of Management and Budget and Congress, approval of the budget by Congress, budget execution, and the reporting of budget and performance results. The budget execution phase refers generally to the time period during which the budget authority made through an appropriation remains available for obligation by NRC. NRC's task during the budget execution process is to spend appropriated funds to carry out its mission in accordance with fiscal statutes. From FY 2008 through FY 2012, NRC's budget appropriation ranged from $926.1 million to $1,066.9 million. The audit objectives were to determine whether (1) NRC maintains proper financial control over appropriated

and apportioned funds to ensure compliance with applicable Federal laws, policies, and regulations and (2) opportunities exist to improve the budget execution process.

- The NRC headquarters campus in Rockville, MD, comprises three buildings: One White Flint North, Two White Flint North, and the recently completed Three White Flint North (3WFN). NRC planned this new building to provide adequate office space for all headquarters employees on one centralized campus, replacing NRC offices located at four separate leased spaces in Montgomery County, MD. Prior to moving staff into 3WFN, NRC must ensure that the information technology (IT) infrastructure is in place to allow staff to be fully functional in the new facility. This includes ensuring that IT systems located at other NRC headquarters facilities are transported to 3WFN, installed, and tested so that employees have access to the systems needed to do their jobs. The audit objective was to evaluate NRC's IT readiness during the transition to 3WFN.

- The National Environmental Policy Act of 1969 (NEPA) established a national policy to encourage productive and enjoyable harmony between man and his environment, promote efforts that will prevent or eliminate damage to the environment, and enrich the understanding of ecological systems and natural resources important to the United States. To implement NEPA, Federal agencies must undertake an assessment of the environmental effects of their proposed actions prior to making a decision. The two major purposes of the NEPA process are better informed decisions and citizen involvement. NEPA requires that Federal agencies prepare a detailed statement on the environmental impacts and effects, alternatives to the action, and irreversible commitments of resources involved in the action. This detailed statement is called an Environmental Impact Statement. NRC regulations to implement NEPA are found in Title 10, Code of Federal Regulations, Part 51 (10 CFR Part 51). The audit objective was to determine whether NRC complies with the regulations in 10 CFR Part 51 relative to the preparation of environmental impact statements.

- The Reducing Over-Classification Act states that over-classification of information interferes with information sharing, increases information security costs, and needlessly limits stakeholder and public access to information. Further, the act asserts that over-classification negatively affects dissemination of information within the Federal Government; with State, local, and tribal entities; and with the private sector. Lastly, the act states that Federal agencies that perform classification are responsible for promoting compliance with applicable laws, executive orders, and other authorities pertaining to classification. The audit objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component, and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

- The objective of NRC's personnel security program is to provide assurance that those with access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material are reliable and trustworthy. NRC's Personnel Security Branch (PSB) administers the personnel security program, granting or denying access to classified information. Access authorization is an administrative determination that an individual is eligible for a security clearance for access to Restricted Data or National Security Information. Access authorization eligibility requires an affirmative determination by PSB that the person in question is an acceptable security risk. Maintaining access authorization requires periodic background reinvestigations and adherence to security requirements. Additionally, individuals are required to self-report information to PSB that might compromise their continued eligibility for access to NRC facilities, material, or classified information. The audit objective was to determine if NRC has processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility.

Investigations

- OIG completed an investigation based on a number of allegations in an anonymous letter sent to Congress and the NRC Commission, alleging that an NRC Region IV manager retaliated against regional staff for raising safety issues involving inspection activities at the Fort Calhoun Station nuclear power plant, concerning an onsite fire, and the adequacy of flood protection measures. It was further alleged that Region IV has a chilled workplace environment that dissuades inspectors from identifying safety issues that may be challenged by regional management.

- OIG completed an investigation into a congressional concern that a Region III staff member provided inaccurate and misleading information pertaining to a pressure boundary leak in a pipe at FirstEnergy's Nuclear Power Station, Davis-Besse, located in Oak Harbor, OH.

- OIG completed an investigation into allegations that an NRC employee used their Washington Metropolitan Area Transit Authority (Metro) Transit Subsidy Benefits Program (TSBP) funds to pay for parking for the employee's privately owned vehicle. An initial review of the employee's Metro Transit Subsidy SmarTrip transaction history revealed there were several occasions where the employee paid for parking without reimbursing the money received from the TSBP.

- OIG completed an investigation into an anonymous allegation that an NRC contractor was not providing information technology infrastructure services and support mandated under its contract with NRC. According to the allegation, the NRC contractor was not providing printers, supplies, and maintenance that NRC desperately needed and was cutting costs by providing inexperienced personnel to work on the contract.

- OIG completed an investigation into an allegation that an unknown individual(s) sent a spear phishing e-mail to approximately 215 NRC e-mail accounts containing a link to harvest NRC network user ID and passwords (credentials). At least 12 NRC users were identified as having clicked on the link and accessing the Google Doc spreadsheet page.

- OIG completed an investigation initiated by a letter from Congress. The letter conveyed that a constituent, a former Small Business Administration (SBA) 8(a) business owner, alleged that NRC inappropriately awarded an SBA 8(a) contract that the alleger previously held to a different contractor to provide human resources support to NRC's Region I office.

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 in 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 (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 (1) independently and objectively conduct and supervise audits and investigations relating to NRC programs and operations; (2) prevent and detect fraud, waste, and abuse; and (3) promote economy, efficiency, and effectiveness in NRC programs and operations.

OIG is committed to ensuring the integrity of NRC 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.**

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 investigations of alleged conduct by NRC staff that could adversely impact matters related to health and safety. These investigations may address allegations of:

- 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.

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, 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. OIG does not concur or object to the agency actions reflected in the regulatory documents, but rather offers comments and requests responsive action within specified timeframes.

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's 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, 2013, through September 30, 2013, OIG reviewed agency documents, including Commission papers, Staff Requirements Memoranda, Federal Register Notices, regulatory actions, and statutes.

The following comments were provided during this reporting period:

- The most significant matter addressed during this period was draft *Management Directive 4.X*, *Budget Formulation*. This draft is a major revision and update to the Financial Management part of the directive system. Separating budget formulation from the former chapter section where it was previously part of *Management Directive 4.7*, *NRC Long Range Planning*, *Programming and Budget Formulation*, this new directive comprehensively describes the budget process. The draft was generally well constructed and organized. OIG comments focused on suggesting additional clarification of the roles of each organization involved in each step in the formulation process, and the benefit of including a glossary of the terms used in the directive.

Other OIG Activities

The OIG General Counsel, Maryann Lawrence Grodin, supported the IG community in training and presentations. The Department of Justice Attorney General guidelines for statutory law enforcement authority for criminal investigators include the requirement for periodic refresher training on specified legal issues. The *Inspector General Criminal Investigator Academy* was tasked with formulating the syllabus for the training and identification of appropriate teaching staff. Ms. Grodin was part of a group of attorneys from several IG offices who constructed a model 3-hour course and participated in training a cadre of attorney-trainers. Additionally, Ms. Grodin, along with attorneys from other IG offices, presented the *Civil and Administrative Remedies* class as part of the *Inspector General Periodic Refresher Training Program* in Denver, CO and Shepardstown, WV, to agents from more than a dozen Federal agencies.

Ms. Grodin also participated in the *Inspector General Criminal Investigator Academy Curriculum Review Working Group for the Periodic Refresher Training Program.* The working group focused on assessing the training program's effectiveness in meeting the objectives detailed in the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority.

The *Council of Counsels to Inspectors General*, a group of attorneys who serve as legal advisors in the Federal IG community, sponsors a training program for law students working as summer interns in IG offices in the Washington, DC, area. As part of the introductory session for this year's program, Ms. Grodin, along with Kirt West, Counsel to the Inspector General 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 counsels, and related cases they had worked on in the IG community.

Management and Performance Challenges

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission as of October 1, 2012* *(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 internal NRC security and oversight of licensee security programs.*
Challenge 3	*Management of regulatory processes to meet a changing environment in the oversight of nuclear facilities.*
Challenge 4	*Management of issues associated with the safe storage of high-level radioactive waste when there is no long-term disposal solutions.*
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.*

Audits

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

Audit Summaries

Audit of NRC's Safeguards Information Local Area Network and Electronic Safe

OIG Strategic Goal: Corporate Management

NRC developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI) documents.

SLES features two distinct components: a secure wireless Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents. The SGI LAN component is a network with a secure architecture and is dedicated for use in SGI data processing. The E-Safe component is a secure electronic data repository for SGI records. E-Safe users are able to create, capture, search, and retrieve data from this repository. The adoption of these various techniques into SGI operations was intended to ensure that E-Safe will contain all SGI created or received by NRC, thereby eliminating the need to maintain separate, individual collections of SGI.

The audit objective was to determine if SLES meets its operational capabilities and applicable security controls.

Audit Results:

NRC has developed a secure electronic system to store SGI while also reducing paper SGI and the space needed to store SGI documents; however, opportunities exist for improvement. Specifically, the system (1) does not fully meet user needs and (2) uses inconsistent access rights.

SLES Does Not Fully Meet User Needs

Information technology systems should improve agency productivity and efficiency while reducing paper.[1] SLES was created to allow NRC staff to share SGI in a secure and effective manner. However, SLES does not fully meet user needs; for example, the SLES official folder and document organization is confusing and not intuitive, and the search function is poor and does not let individuals with "browse" permission see document titles when conducting a formal search through the SLES search engine. Moreover, while SLES has reduced the amount of SGI paper documents maintained by NRC offices, a significant amount still remains. This has occurred because NRC management has not given SLES high priority, specifically:

[1] *Paperwork Reduction Act of 1995.*

- There is no single individual who serves as a business "champion"[2] for integrating SLES into the NRC business process.
- NRC lacks adequate communication channels to discuss system issues between SLES staff and its users.

As a result, the system is not being used to its potential and more resources must be used to maintain paper SGI records, possibly resulting in fiscal waste.

Access Rights Are Inconsistent

Federal regulations mandate security controls to protect systems and networks from inappropriate access and unauthorized use. SLES access rights do not consistently meet the intent of the SGI "need-to-know" requirement or an information system's "least privilege" principle because there is no standard process for granting SGI access to individuals or for verifying user access rights. Providing SLES users access rights that exceed an individual's need-to-know or go beyond organizational business needs increases the risk that SGI could be compromised. Additionally, not having a formal policy in place limits access to some individuals who may need SGI access to effectively do their jobs.

(Addresses Management and Performance Challenge #5)

Audit of NRC's Travel Charge Card Program

OIG Strategic Goal: Corporate Management

Card Type	Category	Item Count	Value
Individually Billed Accounts	Common Carrier[6]	7,249	$ 356,227
	Rental Car, Other Auto	16,701	$ 1,563,235
	Food	14,858	$ 303,297
	Hotel	15,468	$ 6,260,023
	Cash Disbursements	3,773	$ 717,226
	Other	1,369	$ 216,522
	Subtotal	59,418	$ 9,416,530
Centrally Billed Accounts	Common Carrier	13,569	$ 6,889,762
	Travel Agent Fee	32,750	$ 478,701
	Subtotal	46,319	$ 7,368,463
TOTAL		105,737	$16,784,993

Source: OIG analysis of Citibank data

NRC established its travel charge card program (referred to as the program) to facilitate employee travel in support of the agency's mission. Specifically, the purpose for using Government charge cards designated for travel purposes (referred to as travel cards) is to reduce the overall cost of travel to the Federal Government through lower administrative costs and by taking advantage of rebates offered by card vendors based on the volume of transactions and on prompt payment of bills. The Federal Travel Regulation mandates the use of travel cards for all official travel expenses unless specifically exempted. Under the program, travel cards can be used to pay for expenses related to official Government travel, such as lodging, meals, and rental cars. During FY 2011, approximately $16.8 million was charged for travel under this program. As of September 2011, approximately 2,618 employees had individually billed cards, and NRC held 5 centrally billed cards.

The audit objective was to assess the adequacy and effectiveness of NRC's policies, procedures, and internal controls over the travel card program for preventing and detecting travel charge card misuse and delinquencies.

[2] *A champion voluntarily works to facilitate the adoption, implementation, and success of a cause, policy, program, project, or product.*

Audit Results

NRC's travel card program has policies, procedures, and internal controls in place to prevent and detect travel card misuse and delinquencies. NRC also has policies in place to lower the overall cost of official travel to the agency. However, OIG determined the efficiency and effectiveness of NRC's management of rebates and quarterly data reporting to the Office of Management and Budget (OMB) can be improved. Specifically, opportunities exist to (1) maximize NRC's rebates by using recommended Federal strategies and (2) improve quarterly reported data accuracy by employing available tools.

Also, during the course of the audit, OIG found that nearly two-thirds of agency card holders were not in compliance with OMB training requirements. OIG discussed this matter with Office of the Chief Financial Officer (OCFO) staff, who agreed with this finding and took corrective action.

Opportunity To Maximize Rebates

NRC's travel card program management does not maximize travel card rebates. For example, NRC does not monitor use of the card by frequent travelers, mandate split disbursement,[3] or pay centrally billed accounts within a day of invoice receipt – all conventional strategies for improving rebates for use of the travel card. OIG's analysis of the FY 2011 rebate shows that the agency could have received approximately $60,000 more than the $96,242 it received on net charges of approximately $16.8 million. NRC does not maximize its rebate because program management staff do not effectively use strategies identified in OMB Circular A-123, Appendix B, available to Federal agencies to increase rebate payments. Specifically, the agency does not pay invoices as received in centrally billed accounts for the productivity rebate and does not explore basis point options for the sales rebate. As a result, NRC does not receive the maximum rebate, which, in turn, makes program costs unnecessarily high. Further, NRC is not in full compliance with OMB requirements to maximize rebates.

Opportunity To Improve Reported Data Quality

OMB requires travel card program managers to report program data at least quarterly. OCFO officials responsible for the travel card program did not report accurate or supportable quarterly data to OMB. In FY 2011, NRC reported incorrect or unsupportable information for 6 of the 14 required data elements. This occurred because program managers did not effectively use the tools available through Citibank's electronic access system[4] and other sources. As a result, NRC management did not receive accurate information to inform program decisions.

(Addresses Management and Performance Challenge #6)

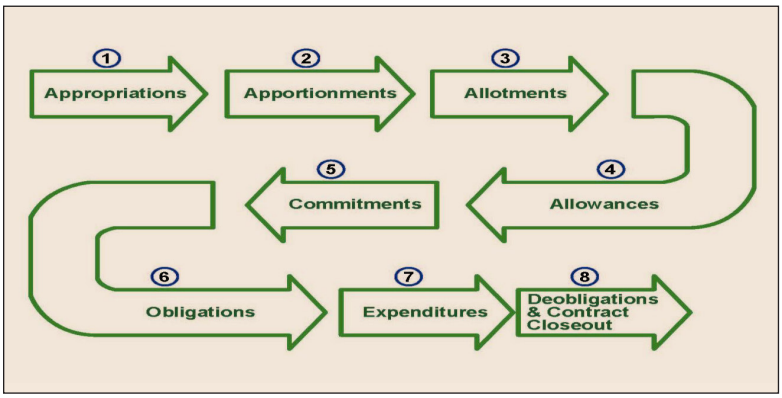
---

[3] *The Government pays the credit card vendor directly when a traveler uses the card and files a voucher for reimbursement, while additional money owed to the traveler goes to the traveler's bank account. Without split disbursement, the traveler receives the entire voucher settlement and in turn pays the credit card bill.*

[4] *The charge card contractor's Internet-based system that provides account access and a variety of reports that assist in the effective management of the charge card programs.*

Audit of NRC's Budget Execution Process

OIG Strategic Goal: Corporate Management



Source: NRC OCFO

The U.S. Government requires Federal agencies to establish an effective funds control process to ensure funds are used only for the purpose set forth by Congress and that expenditures do not exceed amounts authorized. The NRC budget process consists of strategic planning; budget formulation; submission of the agency's budget to OMB and Congress; approval of the budget by Congress; budget execution; and the reporting of budget and performance results. The budget execution phase refers generally to the time period during which the budget authority made through an appropriation remains available for obligation by NRC. NRC's task during the budget execution process is to spend appropriated funds to carry out its mission in accordance with fiscal statutes. Between FY 2008 and FY 2012, NRC's budget appropriation ranged from $926.1 million to $1,066.9 million.[5]

The audit objectives were to determine whether (1) NRC maintains proper financial control over appropriated and apportioned[6] funds to ensure compliance with applicable Federal laws, policies, and regulations and (2) opportunities exist to improve the budget execution process.

Audit Results:

Overall, the agency maintains proper financial control over appropriated and apportioned funds to ensure compliance with applicable Federal laws, policies, and regulations. However, OIG identified opportunities for improvement in the following areas:

- Incomplete implementation of Planning, Budgeting, and Performance Management process.
- Insufficient understanding of Financial Accounting and Integrated Management Information System (FAIMIS) reporting capabilities.
- Incomplete delegation and budget execution training records.

Addressing these concerns will strengthen NRC's budget execution process.

---

[5] *The FY 2010 enacted budget was $1,066.9 million.*

[6] *After Congress passes an appropriation, the Office of Management and Budget provides apportionments of funds, usually on a quarterly basis, to Federal agencies to make money available for use for specified time periods, programs, activities, projects, objects, or any combination of these.*

Incomplete Implementation of Planning, Budgeting, and Performance Management Process

NRC developed the Planning, Budgeting, and Performance Management process to integrate NRC's (1) strategic planning, (2) budget formulation (resource determination process), (3) budget execution (or monitoring performance process), and (4) performance assessment activities. However, NRC's budget formulation and execution processes are not aligned. In practice, NRC's budget formulation is based on business lines but executed at the allowance holder level. For example, an NRC office may have the lead on two business lines that cross multiple offices. During budget execution, that same office controls expenditures only within its office. Moreover, inconsistent use of financial management system codes further inhibits budget implementation. Although the agency recognizes this problem, management has not yet implemented all the elements in the Planning, Budgeting, and Performance Management process, and has not enforced the use of certain financial management system codes. As a result, NRC's current budget process inhibits the agency's ability to determine agency business line costs.

Insufficient Understanding of System Reporting Capabilities

NRC staff do not fully understand how to obtain budget information from FAIMIS that would be useful for decisionmaking. In October 2010, NRC began using FAIMIS as the agency's core financial system and the official system of record for budget transactions. OIG conducted multiple interviews with staff throughout the agency who work on budget execution and learned that staff have difficulty obtaining and understanding budget execution reports. Although program managers need both operational and financial data to determine whether they are meeting agency goals, the agency has not provided sufficient training on FAIMIS reporting functionalities and report availability. Without a full understanding of system capabilities to access budget information, staff may not have the data needed to make informed business decisions.

Incomplete Delegation and Budget Execution Training Records

According to Federal and agency guidance, NRC must maintain appropriate records and make such documentation available. However, supporting documents regarding financial management delegations and budget execution training are incomplete. This has occurred because management does not have written recordkeeping procedures for maintaining these documents. In addition, agency guidance does not specify whether allowance holder delegations should be to the position or specific individual. Without appropriate documentation, individuals may be executing transactions outside their authority.

(Addresses Management and Performance Challenges #6)

Audit of NRC's Information Technology Readiness for Three White Flint North

OIG Strategic Goal: Corporate Management

The NRC headquarters campus in Rockville, MD, comprises three buildings: One White Flint North, Two White Flint North, and the recently completed Three White Flint North (3WFN). NRC planned this new building to provide adequate office space for all headquarters employees on one centralized campus, replacing NRC offices located at four separate leased spaces in Montgomery County, MD.

Prior to moving staff into 3WFN, NRC must ensure that the information technology (IT) infrastructure is in place to allow staff to be fully functional in the new facility. This includes ensuring that IT systems located at other NRC headquarters facilities are transported to 3WFN, installed, and tested so that employees have access to the systems needed to do their jobs.

NRC has moved its Professional Development Center and Office of the Chief Human Capital Officer to 3WFN. Staff from other NRC offices will occupy 3WFN in 2013 as NRC revises its move schedule to align with new General Services Administration space requirements.[7]

The audit objective was to evaluate NRC's IT readiness during the transition to 3WFN.

Audit Results:

IT systems should undergo testing and necessary corrective action to ensure readiness for users upon deployment. Infrastructure testing included network connectivity and individual workstation testing.[8] Based on interviews, contract analysis, and direct observation, OIG determined that NRC tested IT infrastructure in 3WFN and has appropriate plans for future system deployments in 3WFN.

Infrastructure testing included network connectivity and individual workstation testing. NRC and its network maintenance contractor have procedures to move staff IT equipment into their new 3WFN workspace, and for testing this equipment before staff return to work. Some data systems, such as High Performance Computing,[9] have separate contracts that provide for equipment setup and testing in 3WFN. Further, NRC's new Operations Center in 3WFN will undergo several months of testing to familiarize staff with the facility and its IT equipment, including mock exercises designed to simulate incident response scenarios involving NRC headquarters and regional personnel.

OIG auditors concluded that NRC has performed appropriate IT system deployment planning and testing, and that these measures provide adequate IT readiness at 3WFN.

(Addresses Management and Performance Challenge #5)

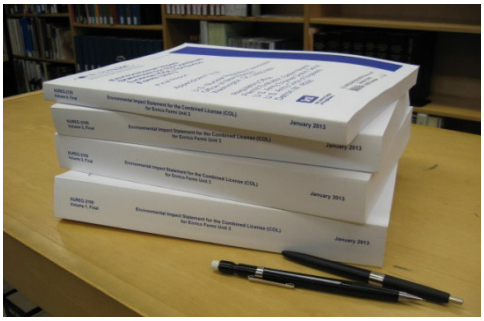
---

[7] *Since the issuance of this audit report, two additional NRC offices have moved into 3WFN: the Office of Nuclear Security and Incident Response and Office of Nuclear Material Safety and Safeguards.*

[8] *NRC conducted testing of electrical and other infrastructure in 3WFN at the end of the building's construction phase in 2012.*

[9] *NRC's High Performance Computing System is used to perform nuclear reactor safety analysis, such as fluid dynamics computations.*

Audit of NRC's Compliance with 10 CFR Part 51 Relative to Environmental Impact Statements



NRC's most recent final EIS, published in four volumes.
Source: OIG

OIG Strategic Goal: Safey

The National Environmental Policy Act of 1969 (NEPA) established a national policy to encourage productive and enjoyable harmony between man and his environment, promote efforts that will prevent or eliminate damage to the environment, and enrich the understanding of ecological systems and natural resources important to the United States. To implement NEPA, Federal agencies must undertake an assessment of the environmental effects of their proposed actions prior to making a decision. The two major purposes of the NEPA process are better informed decisions and citizen involvement. NEPA requires that Federal agencies prepare a detailed statement on the environmental impacts and effects, alternatives to the action, and irreversible commitments of resources involved in the action. This detailed statement is called an Environmental Impact Statement (EIS).

NRC regulations to implement NEPA are found in Title 10, Code of Federal Regulations, Part 51 (10 CFR Part 51). The purposes of NEPA and its implementation dovetail with NRC's organizational values of openness and transparency, as expressed in the Principles of Good Regulation and the Strategic Plan. NRC activities generate a great deal of public interest. For their participation to be meaningful, stakeholders must have access to clear and understandable information about NRC's role, process, activities, and decisionmaking.

The audit objective was to determine whether NRC complies with the regulations in 10 CFR Part 51 relative to the preparation of environmental impact statements.

Audit Results:

In recent years, NRC has taken steps to enhance its NEPA reviews and procedures. These initiatives have generated important discussions and provide a context for long-term progress. However, OIG identified areas of noncompliance with 10 CFR Part 51 relative to disclosure and public involvement. In order to clearly communicate the results of and involve the public in its environmental reviews, NRC management should strengthen its EIS preparation process by:

- Publishing a Record of Decision (ROD) that complies with 10 CFR 51.102 and 51.103.[10]
- Publishing an EIS that complies with the format provided in 10 CFR Part 51, Appendix A.
- Performing all regulatory requirements for scoping for EISs that tier off of a generic EIS.[11]

[10] *The ROD ties together the results of the environmental review and serves as an important vehicle for informing the public of the agency's conclusions and recommendations.*

[11] *NRC uses the term generic EIS to refer to a programmatic EIS, which assesses the scope and impact of the environmental effects that would be associated with an action at numerous sites.*

Records of Decision Not in Full Compliance With Regulations

NRC offices with EIS preparation responsibilities do not publish a ROD that complies with the requirements in 10 CFR Part 51. NRC regulations provide specific criteria for the publication of a ROD and what must be included in a ROD. NRC does not publish a ROD that complies with its regulations because within the agency there are incorrect and varying interpretations of what the regulations require. Thus, NRC is not in compliance with its regulations. As a result, NRC (1) does not adequately notify the public, including Congress, Federal agencies, government partners, and other stakeholders, of its decision and the basis of that decision and (2) undermines its extensive efforts to be clear, open, and transparent.

NRC EISs Do Not Follow the Required Format

NRC's EISs do not follow the format described by 10 CFR Part 51, Appendix A. Appendix A to 10 CFR Part 51 identifies the format elements that must be included. NRC's EISs do not follow the Appendix A format because controls are not in place to assure use of that format. Thus, NRC is not in compliance with its regulations. As a result, NRC (1) does not clearly present, in an accessible way, the proposed action, alternatives, and conclusions to stakeholders and (2) undermines its extensive efforts to be clear, open, and transparent.

NRC Not in Full Compliance With Scoping Regulations

NRC did not fully comply with scoping regulations for in-situ uranium recovery EISs that tier off of a generic EIS. NRC regulations require scoping when preparing an EIS and specify actions the agency must take during the scoping process. NRC did not fully comply with the scoping regulations because there is an incorrect understanding of the regulations related to scoping for EISs that tier off of a generic EIS. Thus, NRC is not in compliance with its regulations. By not fully complying with the regulations, NRC may exclude some interested persons who wish to participate in the process. Additionally, NRC undermines its extensive efforts to be clear, open, and transparent.

(Addresses Management and Performance Challenges #1 and #3)

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

OIG Strategic Goal: Security

The Reducing Over-Classification Act[12] (the Act) states that over-classification of information interferes with information sharing, increases information security costs, and needlessly limits stakeholder and public access to information. Further, the Act asserts that over-classification negatively affects dissemination of information within

[12] *Public Law 111-258/H.R. 553, "Reducing Over-Classification Act," October 7, 2010.*

the Federal Government; with State, local, and tribal entities; and with the private sector.[13] Lastly, the Act states that Federal agencies that perform classification are responsible for promoting compliance with applicable laws, executive orders, and other authorities pertaining to classification.

NRC must protect classified information related to Federal Government programs for securing nuclear materials and facilities. Classification is the process of identifying information that must be protected against unauthorized disclosure in the interest of national security. Classification may be performed only by personnel who have been delegated special authority and undergone required training. Specifically, Original Classifiers can make an initial determination, in the interest of national security, that information requires protection from unauthorized disclosure. In contrast, Derivative Classifiers may only restate or paraphrase information that has already been classified.

On December 29, 2009, the President of the United States signed Executive Order 13526, "Classified National Security Information" (the Order), which establishes current principles, policies, and procedures for classification. On June 25, 2010, the National Archives and Records Administration's Information Security Oversight Office issued a directive (the Directive) in the CFR[14] that included guidance to be used by Federal agencies in implementing the Order.

In accordance with the Act's requirements, the audit objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and effectively administered within such department, agency, or component, and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

Audit Results:

OIG auditors reviewed NRC policies and procedures for its classified information security program and developed five findings with corresponding recommendations to improve agency compliance with current Federal Government standards. Auditors also reviewed a non-statistical sample of classified documents produced by NRC staff and found a limited number of marking errors but no evidence of systemic misclassification.

Original Classifier Training

The Order and the Directive require Original Classifiers to undergo annual training.[15] Further, Original Classifiers who do not undergo annual training are to have their authority suspended.[16] Through interviews with 3 of 11 NRC personnel who have original classification authority, auditors learned that these personnel had not taken

[13] *Public Law 111-258, Section 2, "Findings."*

[14] *32 CFR Parts 2001 and 2003.*

[15] *E.O. 13526, Section 1.3(d) and 32 CFR 2001.71(c).*

[16] *Original Classifiers may receive a waiver if they are unable to take required training because of unavoidable circumstances.*

required training. Required Original Classifier training has not occurred because NRC's Management Directive 12.2, *NRC Classified Information Security Program*, does not prescribe training in accordance with current Federal standards. NRC's Original Classifiers who fail to meet their training requirements cannot perform classification work in an emergency, or in other unexpected circumstances that might require them to exercise their authority. Further, this training is intended to cover relevant administrative duties in addition to classification that Original Classifiers may need to perform as part of their work.

Training Certification Is Not Documented as Required

Federal law requires documentation of training for Original and Derivative Classifiers. Public Law 111-258 specifically states that training for Original and Derivative Classifiers is a prerequisite, "as evidenced by an appropriate certificate or other record" for obtaining original classification authority or derivatively classifying information, and for maintaining such authority.[17] However, NRC classifiers are not issued training certificates or other documentation after completing required training. NRC staff explained that individual classifiers' training information is managed by e-mail correspondence, and that cognizant staff maintain a record of this activity. In contrast, other programs at NRC use the agency's automated training system, *iLearn*, to track training dates and validate credentials that require specific training. Managing classifier training requirements and credentials centrally in NRC's *iLearn* system would provide classifiers and their supervisors better visibility over training obligations, and would facilitate compliance with Public Law 111-258 criteria. It would also mitigate risk associated with reliance on a single person to manage training requirements and records through e-mail correspondence and computer desktop files.

NRC Conducts Self-Inspections With Limited Scope

Federal standards require agencies to conduct routine self-inspections of classified information security programs. Specifically, the Order and the Directive state that self-inspections are to include regular reviews of representative samples of original and derivative classifications, and misclassifications are to be corrected.[18] NRC conducts self-inspections of its classified information security program.[19] However, these self-inspections do not include representative samples of classifications insofar as the Office of Nuclear Security and Incident Response (the NRC office responsible for classified information security) does not review work produced by classifiers from other offices. Management Directive (MD) 12.2 calls for a self-inspection program, but does not reflect current Federal standards. Specifically, NRC's guidance does not call for representative sampling of agency classifications and correction of misclassifications. Expanded self-inspections would improve NRC's oversight of classification activity.

[18] *E.O. 13526 Section 5.4(d)(4), and 32 CFR 2001.60.*

[19] *NRC reported having conducted two self-inspections in FY 2012.*

NRC Does Not Include Classification Duties in Staff Position Descriptions and Performance Evaluations

Current Federal standards require NRC and other agencies to include classification duties in staff performance management. However, most Derivative Classifiers at NRC do not have classification duties in their position descriptions and are not rated on these tasks. Cognizant NRC staff are aware of this requirement but face labor negotiation challenges in meeting it. Developing a solution would benefit NRC because Federal policy emphasizes the importance of classification duties as well as employees' roles in promoting classified information security. NRC staff who routinely process and/or handle classified information cannot be held accountable and incentivized for this work if it is not considered as part of their formal position description used for performance evaluations.

Management Directive 12.2 Needs Comprehensive Update

NRC's internal policy requires the agency's management directives to be updated to reflect changes in Federal law and regulation, and to be revised every 5 years following a management directive's last complete revision. NRC has not updated MD 12.2 to reflect current Federal policy and some agency practices. NRC's process for revising management directives has deferred revision of MD 12.2 (last approved in July 2006, with exception of one page that was updated in August 2007) until 2014. NRC should comply with internal standards for management directive revision to ensure staff have current and accurate guidance to support their work. Beyond the practical importance of timely management directive revisions, alignment between NRC guidance and higher level Federal guidance is important for positioning NRC as a responsive, transparent regulatory organization.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Ongoing Eligibility for Access Authorization

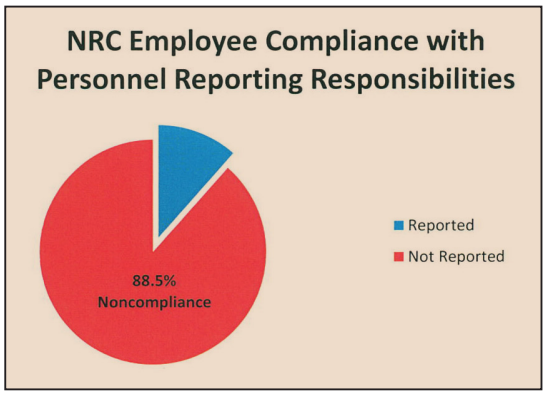
OIG Strategic Goal: Security

The objective of NRC's personnel security program is to provide assurance that those with access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material[20] are reliable and trustworthy. In order to provide such assurance, NRC's Personnel Security Branch (PSB) administers the personnel security program, granting or denying access to classified information.[21]

---

[20] *Special nuclear material (SNM) is defined by Title I of the Atomic Energy Act of 1954 as plutonium, uranium-233, or uranium enriched in the isotopes uranium-233 or uranium-235. The definition includes any other material that the Commission determines to be SNM, but does not include source material. NRC has not declared any other material as SNM.*

[21] *The Office of Personnel Management (OPM) Federal Investigative Services Division is NRC's investigative provider. NRC applicants, employees, contractors, and licensees are submitted for investigation through OPM.*



Source: OIG

Access authorization is an administrative determination that an individual is eligible for a security clearance for access to Restricted Data[22] or National Security Information.[23] Access authorization eligibility requires an affirmative determination by PSB that the person in question is an acceptable security risk. The determination is a comprehensive, commonsense judgment, made after consideration of all the information, favorable or unfavorable, relevant to whether granting access authorization would be clearly consistent with the national interest.

A favorable determination results in PSB issuing a security clearance. Classified access requirements determine the type of clearance issued. All NRC employees are required to have a security clearance. PSB primarily issues the following clearances: Q Clearance – Top Secret, and L Clearance – Secret. As of August 2013, 1,196 NRC employees had Q clearances, 3,146 had L clearances, and 296 were designated as L(H) (Secret – High Public Trust).[24]

Maintaining access authorization requires periodic background reinvestigations and adherence to security requirements. Individuals who possess "Q," "L(H)," or "L" security clearances undergo reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access authorization. PSB initiates a reinvestigation every 5 years for "Q" and "L(H)" (high public trust) clearances and every 10 years for "L" clearances. Additionally, individuals are required to self-report information to PSB that might compromise their continued eligibility for access to NRC facilities, material, or classified information.

The audit objective was to determine if NRC has processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility.

Audit Results:

NRC employees are required to comply with personnel reporting responsibilities for continued access authorization. Specifically, employees are required to report certain events that may bring into question their reliability and trustworthiness. For example, the following are some of the events employees are required to report:

[22] *Restricted Data: Information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.*

[23] *National Security Information: Information classified by an Executive Order, whose compromise would cause damage to the national security.*

[24] *NRC also issues L(H) high public trust clearances. Classified access requirements for individuals with L and L(H) clearances are the same. However, individuals with L(H) clearances undergo a more rigorous initial background investigation and receive more frequent periodic reinvestigations.*

- Use of intoxicating beverages habitually to excess without evidence of rehabilitation.
- Use of, trafficking in, sale, transfer, or possession of an illegal drug or other controlled substance (except as prescribed by a physician licensed to dispense drugs in the practice of medicine), without evidence of rehabilitation.
- Arrests, charges, detentions, or any criminal conduct that indicates a history or pattern of criminal activity that creates doubt about a person's judgment, reliability, or trustworthiness.
- Any financial considerations that indicate an inability or an unwillingness to satisfy debts, and financial problems linked to gambling, drug abuse, alcoholism, or other issues of a security concern.

NRC employees rarely comply with personnel reporting responsibilities for continued access authorization. OIG reviewed a judgmentally selected sample of 35 NRC employee background reinvestigations to determine compliance with reporting responsibilities and found 26 files containing information developed during the reinvestigation concerning certain events that might bring into question staff reliability and trustworthiness. These events should have been reported to PSB prior to the initiation of the reinvestigation. (The majority of the reportable events were financial in nature.) However, only 3 of 26 employees (approximately 11.5 percent) complied with personnel reporting responsibilities and reported to PSB as required by regulation.

NRC does not have sufficient processes in place to ensure that NRC employees comply with personnel reporting responsibilities for continued NRC access authorization eligibility. Specifically, NRC does not regularly inform employees of personnel reporting responsibilities and there is no process to impose consequences for not self-reporting.

Certain types of information must be assiduously protected. When a person's actions show evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on to protect classified information. The unauthorized disclosure of classified information can cause irreparable damage to the national security and loss of human life.

(Addresses Management and Performance Challenge #2)

Audits in Progress

Audit of NRC's Implementation of Its NEPA Responsibilities

OIG Strategic Goal: Safety

NEPA required Federal agencies to consider the environmental impacts of actions under their jurisdiction. NEPA requires that an EIS of the proposed action be prepared for major Federal actions significantly affecting the quality of the human environment. Consultations among stakeholders to ensure compliance with statutory mandates, such as with Section 7 of the Endangered Species Act of 1973 and Section 106 of the National Historic Preservation Act of 1966, are also part of the NEPA review process.

NEPA broadly impacts NRC. Several agency offices conduct environmental reviews. A NEPA review may be initiated in response to a rulemaking, an application for a new license or certification, a license amendment, or a decommissioning plan submitted to the NRC. Generic EISs have been developed to guide staff in the areas of nuclear plant licensing renewal, decommissioning of nuclear facilities, and applications for in situ uranium recovery operations. Standard review plans support staff environmental reviews in other areas. Growing public concern over licensing issues such as reactor aging and spent fuel storage heightens the importance of successfully completing environmental reviews.

The audit objective is to determine whether NRC implements its environmental review and consultation responsibilities as prescribed by NEPA.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Oversight of Equipment Aging

OIG Strategic Goal: Safety

The U.S. fleet of commercial nuclear power plants is aging with an average age over 29 years. Additionally, approximately 90 percent of the 104 licensed plants have either received, are awaiting approval for, or intend to seek a 20-year license extension. This presents emergent challenges as previously unseen equipment failures occur. Aging failures can affect major components such as unit transformers, reactor coolant/recirculation pumps, and other large motors, and present material challenges, such as cracks in thermally treated components and related equipment degradation. Failures of these components can result in operating anomalies and degraded safety equipment, both affecting nuclear safety.

The audit objective is to determine if NRC is providing effective oversight of industry's aging component programs.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Support for Resident Inspectors

OIG Strategic Goal: Safety

The core of the NRC inspection program for nuclear power plants and fuel-cycle facilities is carried out by resident (onsite) inspectors. These inspectors provide an onsite NRC presence for direct observation and verification of licensees' ongoing activities. Generally, the NRC regions manage resident inspector assignments, which include at least two inspectors that are assigned to each site for a period of up to 7 years.

Resident inspector guidance stems from various sources. For example, for operating reactors, Inspection Manual Chapter 1202, *Senior Resident and Resident Inspector Site Turnover*, provides guidelines to ensure that resident inspectors new to a site have the necessary knowledge and site familiarity to successfully implement the reactor oversight process (including allegations and enforcement) and emergency response duties.

During the course of their assignment, the resident inspectors variously also require additional types of support for such areas as telecommunications, human resources, technical review, and legal counsel. Furthermore, the ability to communicate effectively and efficiently with the regional offices, NRC headquarters, and other resident inspectors is vitally important to their ability to meet the expectations of NRC management and the public.

The audit objectives are to evaluate the effectiveness of NRC support provided to the resident inspectors at nuclear power plants, fuel-cycle facilities, and construction sites.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Information Technology Governance

OIG Strategic Goal: Corporate Management

IT governance pertains to stewardship of IT resources in order to most efficiently and effectively attain agency vision, mission, goals, and objectives.

NRC has two IT governance boards – the *Information Technology/Information Management Board (ITB)* and the *Information Technology/Information Management Portfolio Executive Council (IPEC)*. The ITB is a review body created to make recommendations to the IPEC on the agency's IT architecture, perform portfolio analyses, and review technologies and standards. The IPEC is an executive management body established to provide strategic direction and to set fiscal year priorities, among other things. NRC also performs other types of management control activities that are overseen by these governance boards.

The audit objective will be to assess the effectiveness of NRC's current IT governance in meeting the agency's current and future IT needs.

(Addresses Management and Performance Challenge #5)

Audit of NRC's FY 2013 Financial Statements

OIG Strategic Goal: Corporate Management

Under the *Chief Financial Officers Act and the Government Management and Reform Act*, the 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 December 16, 2013. In addition, OIG will issue reports on:

- Special Purpose Financial Statements.
- Implementation of the *Federal Managers' Financial Integrity Act*.
- Summary of Performance and Financial Information.
- Agency compliance with the *Improper Payments Elimination and Recovery Act of 2010*.

The audit objectives are to:

- 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 OMB Circular A-123, Revised, *Management's Responsibility for Internal Control.*
- Assess agency compliance with the *Improper Payments Elimination and Recovery Act of 2010.*

(Addresses Management and Performance Challenge #6)

Audit of NRC's Process for Addressing Bankruptcy of Materials Licensees

OIG Strategic Goal: Safety

An NRC materials licensee's financial condition could affect its ability to control licensed material. Provisions of the *Atomic Energy Act* and regulations in 10 CFR require that NRC licensees notify NRC in the case of bankruptcy. These provisions are in place to assure that appropriate measures to protect the public health and safety have been or will be taken during a licensee's bankruptcy filing. These measures include:

- Maintaining security of licensed material and contaminated facilities.
- Assuring that licensed material is transferred only to properly authorized NRC or Agreement State licensees.

NRC's *Bankruptcy Review Team* was formed to review and act on bankruptcy notifications as they occur. NRC staff are then required to address any concerns identified that may impact public health and safety.

The audit objective is to determine if NRC has reasonable assurance that appropriate measures to protect the public health and safety have been or will be taken during bankruptcies involving byproduct, source, or special nuclear materials licensees.

(Addresses Management and Performance Challenge #1)

Audit of NRC's Use of the NEWFlex Program

OIG Strategic Goal: Corporate Management

NRC Employee Work Schedule Flexibilities (NEWFlex) is a program that offers expanded work schedule and additional credit hour options to help employees balance their work/life activities while at the same time assuring that each NRC office is able to execute its mission. This program is available to almost all NRC staff. NEWFlex is optional to employees, and the schedule is subject to supervisory approval. The program offers a flexible (variable) schedule that includes, but is not limited to, an extension of hours, schedules that can vary daily, and core hours. NEWFlex applies to employees while working at home, and supports the agency's telework initiative.

Each Federal agency must determine (1) whether to establish alternative work schedule programs; (2) how to administer the programs efficiently; (3) how to comply with the spirit of the President's memoranda of July 11, 1994, and June 21, 1996, on providing family-friendly work arrangements; and (4) how to ensure that the programs do not cause an adverse agency impact. Agencies wishing to establish flexible or compressed

work schedules permitted under 5 U.S.C. 6122 and 5 U.S.C 6127 do not need Office of Personnel Management approval.

The audit objectives are to assess (1) NRC's adherence to applicable laws and regulations, (2) the adequacy of NRC's internal controls associated with the program, and (3) whether the program adequately addresses unique situations such as drug testing, official travel, and other events.

(Addresses Management and Performance Challenge #7)

Audit of NRC's Full-Time Telework Program

OIG Strategic Goal: Corporate Management

The *Telework Enhancement Act of 2010* (Public Law 111-292), was signed into law on December 9, 2010. The act is a key factor in the Federal Government's ability to achieve greater flexibility in managing its workforce through the use of telework. Telework (1) is a strategy to improve Continuity of Operations to help ensure that essential Federal functions continue during emergency situations, (2) promotes management effectiveness when telework is used to target reductions in management costs and environmental impact and transit costs, and (3) enhances work-life balance, i.e., telework allows employees to better manage their work and family obligations. The law specifies roles and responsibilities for the Office of Personnel Management, General Services Administration, Office of Management and Budget, Department of Homeland Security, National Archives and Records Administration, and others to provide overall guidance to Federal executive agencies.

The term *telework* or *teleworking* refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of their position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. In practice, telework represents a work arrangement that allows an employee to perform work, during any part of regular, paid hours, at an approved alternative worksite such as home or a telework center. This definition of telework includes what is generally referred to as remote work, but does not include any part of work done while on official travel.

In the past, agencies have sometimes used the term remote to describe a work arrangement in which the employee resides and works at a location beyond the local commuting area of the employing organization's worksite or to describe a full-time telework arrangement. For reporting purposes, these employees should be included as teleworkers. While some agencies do permit full-time telework, it is not the norm. In fact, the act specifically identifies the following categories of part-time participation and requires that agencies report on the specific number of employees each year that telework:

- 3 or more days per pay period (denotes a biweekly pay period).

- 1 or 2 days per pay period.
- Once per month.
- On an occasional, episodic, or short-term basis (i.e., situational telework such as ad-hoc or unscheduled telework).

Specifically, with regard to program implementation of full-time telework, each agency's policies should identify whether full-time telework arrangements are allowable in the agency and, if so, aspects of the employment arrangement that could potentially change if an employee teleworks full-time (e.g., could there be consequences to locality pay, benefits, travel, reduction-in-force procedures, etc.).

The audit objectives are to determine (1) if NRC's telework program complies with applicable laws and regulations, and (2) the adequacy of internal controls over the program.

(Addresses Management and Performance Challenge #7)

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2013

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 IGs. In addition, FISMA includes new provisions such as the development of minimum standards for agency systems, aimed at further strengthening the security of 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 2013.

(Addresses Management and Performance Challenge #2)

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

OIG Strategic Goal: Safety

In March 2010, the Department of Energy (DOE) filed a motion with NRC to withdraw its license application for the Yucca Mountain high level waste repository. Subsequently, the former Chairman directed NRC staff to take actions to facilitate an orderly closeout of the Yucca Mountain review process, including documenting material reviewed to date for retention purposes and potential future review in accordance with agency policy.

It is the policy of the NRC that all official records made or received by the NRC in the course of its official business comply with the regulations governing Federal records management issued by the National Archives and Records Administration and the General Services Administration. Specifically, agency policy on the retention of records and information states that records are to be maintained and preserved as evidence of the NRC's organization, functions, policies, decisions, procedures, operations, or other activities…." Additionally, agency records are to be maintained in such a way that all information can be stored safely and retrieved easily when necessary…."

Given the uncertainty and public interest surrounding the issue of high-level waste storage, it is important that NRC maintain agency records related to the review of the Yucca Mountain high level waste repository DOE license application in accordance with Federal requirements and agency policy.

The audit objective is to determine if agency policy and procedures on document management provide reasonable assurance that documentation related to the review of the Yucca Mountain facility has been appropriately documented and retained.

(Addresses Management and Performance Challenge #4)

Investigations

During this reporting period, OIG received 100 allegations, initiated 39 investigations, and closed 35 cases. In addition, the OIG made 6 referrals to NRC management and 7 to the Department of Justice.

Investigative Case Summaries

Region IV's Potential Violation of the No Fear Act[25]

OIG Strategic Goal: Corporate Management

OIG conducted an investigation based on a number of allegations in an anonymous letter sent to Congress and the NRC Commission alleging that an NRC Region IV manager retaliated against regional staff for raising safety issues involving inspection activities at the Fort Calhoun Station nuclear power plant, concerning an onsite fire, and the adequacy of flood protection measures. It was further alleged that Region IV has a chilled workplace environment that dissuades inspectors from identifying safety issues that may be challenged by regional management.

Investigative Results:

OIG found that the Region IV manager supported the issuance of a yellow finding (substantial safety significance) rather than a red finding (high safety significance) regarding conditions relating to the 2011 fire based on specific technical concerns about the accuracy of a red characterization. Notwithstanding the manager's expressed views, a red finding was issued in this matter as a preliminary and a final finding. Additionally, OIG found that the manager raised concerns about the basis for a yellow finding concerning flood protection measures at the site. The resolution of the concerns resulted in a long delay in reporting the finding, but concluded with the manager supporting the yellow finding.

OIG found that despite staff assertions, there was no evidence that the manager altered or removed safety findings from inspection reports without the concurrence of the reporting inspector.

OIG also found that performance appraisals for Region IV risk analysts under the manager's supervision were downgraded in the 2009 performance year. There was no evidence that these downgrades were related to and in retaliation for raising safety issues. In a separate issue, evidence was developed that a Region IV reactor inspector received a performance downgrade following a disagreement with the manager over a 2009 inspection finding, and that the disagreement was a factor in the downgrade.

In addition, OIG found widespread concern among Region IV employees about interaction with the manager due to his interpersonal behavior. Employees did

[25] *The No FEAR Act provides for an environment where employees feel confident in coming forward to report possible violations of law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health and safety.*

distinguish the manager's interpersonal manner from his commitment to safety. However, OIG did find that negative perceptions of the manager's style created perceptions among some Region IV employees of a chilled workplace environment.

Further, OIG found that Region IV managers had been apprised of specific concerns from non-supervisory employees and branch chiefs about the manager's behavior, but that while some remedial measures were proposed, none included formal or documented performance counseling.

NRC Region III's Handling of a Pinhole Coolant Leak at Davis-Besse Nuclear Power Station, Oak Harbor, OH

OIG Strategic Goal: Safety

OIG completed an investigation into a congressional concern that the NRC Region III Public Affairs Officer (PAO) provided inaccurate and misleading information pertaining to a pressure boundary leak in a pipe at FirstEnergy's Nuclear Power Station, Davis-Besse, located in Oak Harbor, OH.

It was alleged that after FirstEnergy discovered "a pinhole coolant leak in a pipe weld while performing a walk down inspection of the plant," the PAO was quoted in a June 7, 2012, Bloomberg News article stating that the leak was below the NRC threshold for mandatory reporting. Further, it was alleged that the leak at Davis-Besse was not below NRC's threshold for mandatory reporting and Region III had publicly provided an inaccurate statement.

Additionally, the congressional concern included a disparity among statements made by NRC staff, the NRC Region III PAO, and FirstEnergy regarding cracking in Davis-Besse's shield building wall that was discovered by the licensee on October 11, 2011. The PAO and FirstEnergy publicly stated that the cracks were in an architectural or decorative element of the wall that had no structural significance; however, NRC staff later stated that the cracking in the shield building wall was in a structurally significant area of the wall.

Investigative Results:

OIG found that the Bloomberg News reporter misquoted the NRC Region III PAO in the June 7, 2012, news article concerning the need for the licensee to report to NRC the pressure boundary leak in the Davis-Besse pipe. OIG found that with the PAO's assistance, the Bloomberg News editor published another article on July 25, 2012, that corrected the June 7th article and accurately quoted the PAO in stating the plant was required to report the leak to the NRC.

With regard to the cracking of the shield building wall, OIG found that NRC's initial characterization of this incident was based on preliminary information

obtained from FirstEnergy. As more information became available to NRC, the agency revised its description of the cracking issue, and its later descriptions were therefore different than its earlier descriptions.

OIG also found that NRC inspected the Davis-Besse shield building cracking and NRC concluded that the cracking did not affect the ability of the shield building to perform its design function.

(Addresses Management and Performance Challenge #1)

Misuse of Transit Subsidy Benefit Program

OIG Strategic Goal: Corporate Management

OIG completed an investigation into allegations that an NRC employee used their Washington Metropolitan Area Transit Authority (Metro) Transit Subsidy Benefits Program (TSBP) funds to pay for parking for their privately owned vehicle. An initial review of the employee's Metro Transit Subsidy SmarTrip transaction history revealed there were several occasions where the employee paid for parking without reimbursing the money received from the TSBP.

Investigative Results:

OIG reviewed the NRC TSBP application (NRC Form 546) signed by the employee and approved by NRC on May 3, 2011. On the bottom of the NRC Form 546 is a certification block each applicant must read and sign. The certification block in part includes the following statement: "I will use the appropriate portion of my eligible monthly benefit for my actual monthly commuting cost by public transportation or eligible van pool." The NRC Form 546 indicated the employee would commute to the NRC using Metrorail from the New Carrollton Station to the White Flint Station, and return, 20 days per month, totaling $204.00 in monthly transit subsidy benefits. Both the NRC Form 546 and the NRC TSBP questions and answers state that the program benefits do not include parking.

OIG reviewed the employee's transit subsidy SmarTrip transaction history for the period January 2008 through mid-September 2011. The employee commuted by both Metrorail and by her privately owned vehicle during this time. The employee paid for parking on approximately 617 separate occasions, totaling $5,216.75. The employee deposited her own funds in the amount of $150.00 onto her SmarTrip card. After subtracting personal deposits, the total amount of potential TSBP funds misused was $5,066.75. The employee's service with the NRC was terminated in May 2013.

(Addresses Management and Performance Challenge #6)

Logon Credential Harvesting Using Google Spreadsheets

OIG Strategic Goal: Security

OIG completed an investigation into an allegation that an unknown individual(s) sent a spear phishing e-mail to approximately 215 NRC e-mail accounts containing a link to harvest NRC network user ID and passwords (credentials). The link in the e-mail went to a Google Doc spreadsheet asking users to "validate" their network credentials. At least 12 NRC users were identified as having clicked on the link and accessing the Google Doc spreadsheet page.

Investigative Results:

OIG investigative activity identified an account created in Malaysia for the sole purpose of sending the spear phishing emails. Additionally, it was determined 55 non-NRC issued user accounts were associated with other Federal Government agencies. OIG notified the other Federal Government agencies of the potential compromise of their users' accounts.

OIG was unable to conclusively identify the person(s) engaging in the spear phishing activities against the NRC. The investigation identified several suspects located in different foreign countries who may be participants in a scheme to fraudulently obtain network logon credentials from a variety of sources, including the U.S. Government, to send spear phishing e-mail messages. Investigative leads sent to these other countries resulted in no international law enforcement action being taken against the targets. As a result, OIG was unable to identify domestic targets who may be involved in the operation.

(Addresses Management and Performance Challenge #5)

NRC Handling of Contractor Award Process for Region I Contract

OIG Strategic Goal: Corporate Management

OIG completed an investigation initiated by a letter from Congress. The letter conveyed that a constituent, a former Small Business Administration (SBA) 8(a) business owner, alleged that NRC inappropriately awarded an SBA 8(a) contract that the alleger previously held to a different contractor to provide human resources support to NRC's Region I office.

Investigative Results:

OIG learned that the former contractor, a human resources consulting service contractor, had a contract with NRC from 2002 until 2012 to perform services for NRC's Region I office. The company was a participant in SBA's 8(a) Business

Development Program, a business assistance program for small disadvantaged businesses. Under the program, businesses owned and controlled by a "socially and economically disadvantaged individual" can receive sole-source contracts up to a ceiling of $4 million for goods and services. Participation is limited to 9 years and, after that time, neither the business nor the individual is eligible to participate again. OIG learned that on October 1, 2012, NRC awarded the NRC Region I contract to a a different 8(a) company, since the former contractor had graduated from the SBA 8(a) program and was not eligible to compete for the contractual services.

(Addresses Management and Performance Challenge #7)

Contract Irregularities Associated With Information Technology Contractor

OIG Strategic Goal: Corporate Management

OIG completed an investigation into an anonymous allegation that an NRC contractor was not providing IT infrastructure services and support mandated under its contract with NRC. According to the allegation, the NRC contractor was not providing printers, supplies, and maintenance that NRC desperately needed and was cutting costs by providing inexperienced personnel to work on the contract.

Investigative Results:

A review of the NRC contract disclosed that the contract is an indefinite delivery, indefinite quantity contract, containing firm-fixed-price and labor hours for IT infrastructure services and support, that was awarded to the contractor for the base period February 18, 2011, through February 17, 2014, with three option years ending on February 17, 2017. The contract supports the NRC IT infrastructure and provides NRC headquarters, regional offices, resident inspector sites, the NRC Technical Training Center, and mobile NRC users with the vast majority of needed IT services, including desktop and laptop computers, servers, office productivity software, e-mail, help desk, BlackBerry devices, network file storage, network printers, network management, IT operational security, data backup and recovery, and new technology integration.

OIG learned that under the firm-fixed-price and labor hours contract, the Government has a predetermined, agreed-upon price for a specific type of work, including labor and price for items. A firm-fixed-price contract is not subject to price adjustment on the basis of the contractor's cost experience in performing the contract, and it allocates to the contractor the maximum risk and responsibility for its performance cost and resulting profit or loss. Consequently, because this is a firm-fixed-price contract, NRC is not concerned about the salary of individuals who are supporting the contract as long as the contractor is providing individuals who can fulfill the contract requirements. The actual salary is between an individual employee and the contractor.

In addition, regarding the issue of whether the contractor personnel lacked experience in properly managing the contract, OIG found that early in the contract, NRC had issues with one of the contractor manager's level of experience. However, after this issue was brought to the attention of the contractor, the contractor replaced the manager and, since then, the contractor has done well in managing the contract.

OIG also found that the NRC contractor has been fulfilling the contract in a timely manner and that it has always delivered printers within the allotted time and the proper quantities.

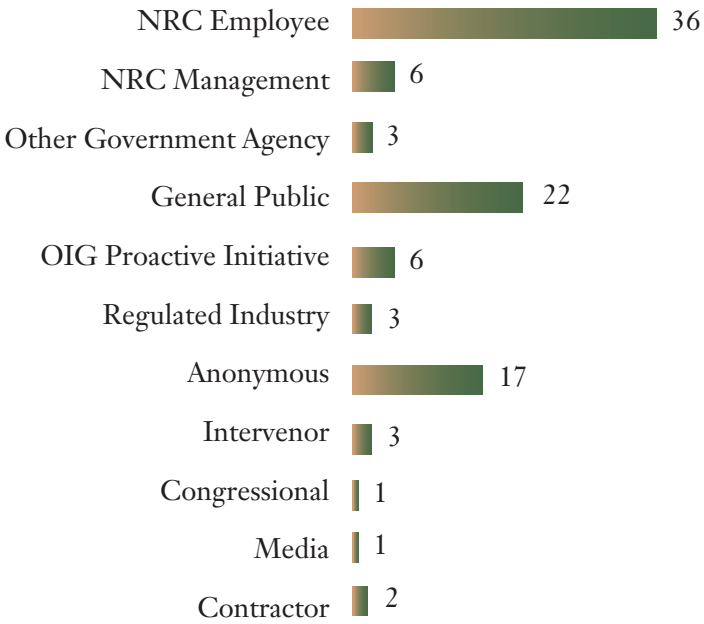
(Addresses Management and Performance Challenge #5)

Summary of OIG Accomplishments

April 1, 2013, through September 30, 2013

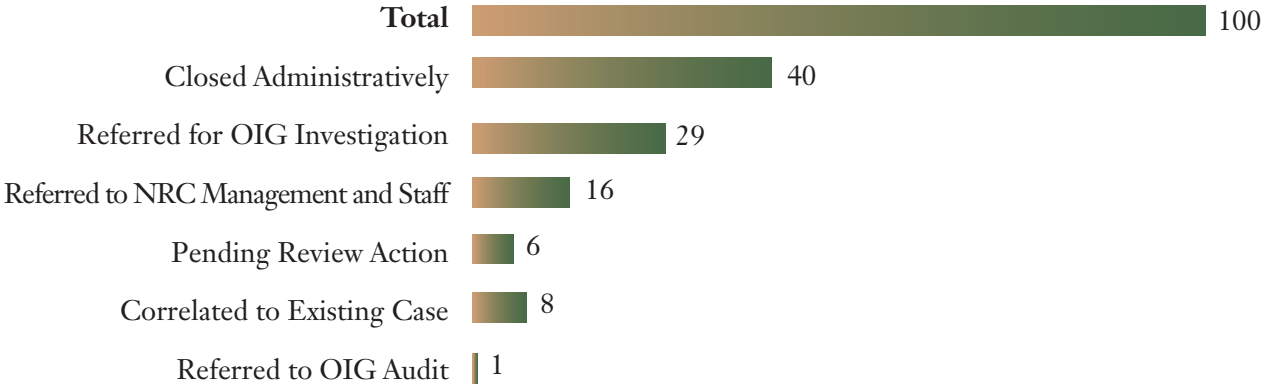
Investigative Statistics

Source of Allegations



Allegations resulting from Hotline calls: 47
Total: 100

Disposition of Allegations



Status of Investigations

DOJ Referrals 7
DOJ Acceptance 1
DOJ Pending 2
DOJ Declinations 7
Criminal Convictions 5
Criminal Penalty Fines $567,989.36
NRC Administrative Actions:
- Terminations and Resignations 1
- Suspensions and Demotions 3
- Other (Letter from Chairman) 1

State Referrals 1
State Declinations 1
State Accepted 0
PFCRA Referral 0
PFCRA Acceptance 0

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Cases in Progress
Employee Misconduct	27	19	17	29
Event Inquiry	2	0	0	2
External Fraud	6	1	1	6
False Statements	4	0	2	2
Management Misconduct	12	15	7	20
Miscellaneous	3	1	2	2
Proactive Initiatives	10	3	3	10
Technical Allegations	5	0	1	4
Theft	1	0	1	0
Whistleblower Reprisal	1	0	1	0
Grand Total	**71**	**39**	**35**	**75**

Audit Listings

Date	Title	Audit Number
04/01/2013	Audit of NRC's Safeguards Information Local Area Network and Electronic Safe	OIG-13-A-16
04/16/2013	Audit of NRC's Travel Charge Card Program	OIG-13-A-17
05/07/2013	Audit of NRC's Budget Execution Process	OIG-13-A-18
06/03/2013	Audit of NRC's Information Technology Readiness for Three White Flint North	OIG-13-A-19
08/20/2013	Audit of NRC's Compliance With 10 CFR Part 51 Relative to Environmental Impact Statements	OIG-13-A-20
09/12/2013	Audit of NRC's Implementation of Federal Classified Information Laws and Policies	OIG-13-A-21
09/12/2013	Audit of NRC's Ongoing Eligibility for Access Authorization	OIG-13-A-22

Contract Audit Reports

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs	Unsupported Costs
04/15/2013	**Dade Moeller & Associates, Inc.** Independent Evaluation of Dade Moeller & Associates, Inc. FY 2013 Provisional Billing Rates NRC-HQ-11-C-04-0012	0	0
09/04/2013	**Southwest Research Institute** Independent Audit of Southwest Research Institute's General Dollar Magnitude Cost Impact NRC-02-06-018 NRC-02-06-021 NRC-41-09-011 NRC-03-09-070 NRC-03-10-066 NRC-03-10-070 NRC-03-10-081 NRC-04-10-144 NRC-HQ-11 -C-03-0047 NRC-HQ-11 -C-03-0058	0	0
09/04/2013	**Southwest Research Institute** Independent Audit of Southwest Research Institute's FY 2011 Pre-Established Fringe Burden Rate for Provisional Billing Purposes NRC-02-06-018 NRC-02-06-021 NRC-41-09-011 NRC-03-09-070 NRC-03-10-066 NRC-03-1 0-070 NRC-03-10-081 NRC-04-10-144 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058	0	0

Audit Resolution Activities

TABLE I

OIG Reports Containing Questioned Costs[26]

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	1	$540,637	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	1	$540,637	0
D.	For which no management decision had been made by the end of the reporting period	0	0	0

[26] *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 Recommendations That Funds Be Put to Better Use[27]

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

[27] *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

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

Date	Report Title	Number
05/26/2003	Audit of NRC's Regulatory Oversight of Special Nuclear Materials **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.	OIG-03-A-15

TABLE IV

Summary of Audit Reports Without Management Decision for More Than Six Months

Date	Report Title	Number
7/12/2012	Audit of NRC's Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Process **Summary:** OIG made 10 recommendations to the Executive Director for Operations of which one is unresolved. **Recommendation 10:** Recommended that the Executive Director for Operations develop and implement a change management process to address future change in the ITAAC process that can create barriers to effective communication and coordination. **Reason Unresolved:** NRC staff stated agreement with the recommendation, yet the agency's actions do not meet the intent of OIG's recommendation. According to NRC staff, the Office of New Reactors (NRO) has incorporated the principals of change management in the tools and processes that facilitate and control ITAAC changes. OIG notes that this is not the same as the development and implementation of a change management process. NRC staff have recently stated that agency senior management are evaluating the implementation of an agency-level management system, which is expected to include a change management process. However, the agency has not provided to OIG any documentation or details that describes how this effort will be implemented. As a result, this recommendation remains unresolved. OIG expects to receive an updated response from NRC by March 7, 2014.	OIG-12-A-16

Abbreviations and Acronyms

3WFN	Three White Flint North
CFR	Code of Federal Regulations
DOE	Department of Energy
EIS	Environmental Impact Statement
E-Safe	electronic safe
FAIMIS	Financial Accounting and Integrated Management System
FISMA	Federal Information Security Management Act
FY	fiscal year
IAM	Issue Area Monitor
IG	Inspector General
IPEC	Information Technology/Information Management Portfolio Council
IT	information technology
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
ITB	Information Technology/Information Management Board
LAN	Local Area Network
MC&A	material control and accountablity
MD	Management Directive
Metro	Washinton Metropolitan Area Transit Authority
NEPA	National Environmental Policy Act of 1969
NEWFlex	NRC Employee Work Schedule Flexibilities
NRO	Office of New Reactors (NRC)
NRC	U.S. Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
OIG	Office of the Inspector General (NRC)
OMB	Office of Management and Budget
PAO	Public Affairs Officer
PSB	Personnel Security Branch (NRC)
ROD	Record of Decision
SBA	Small Business Administration
SGI	Safeguards Information
SLES	Safeguards Information Local Area Network System
SNM	special nuclear material
TSBP	Transit Subsidy Benefits Program

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
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	9-21, 29-34
Section 5(a)(2)	Recommendations for Corrective Action	9-21
Section 5(a)(3)	Prior Significant Recommendations Not Yet Completed	41
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	36
Section 5(a)(5)	Information or Assistance Refused	None
Section 5(a)(6)	Listing of Audit Reports	37
Section 5(a)(7)	Summary of Significant Reports	9-21, 29-34
Section 5(a)(8)	Audit Reports — Questioned Costs	39
Section 5(a)(9)	Audit Reports — Funds Put to Better Use	40
Section 5(a)(10)	Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made	42
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions With Which the OIG Disagreed	None
Section 989C.	Peer Review Information	45

Appendix

Peer Review Information

The OIG Audit and Investigative Programs undergo a peer review every 3 years.

Investigations

The NRC OIG Investigative program was peer reviewed most recently by the Corporation for National and Community Service Office of Inspector General. The peer review final report, dated September 16, 2013, reflected that the NRC OIG is in compliance with the quality standards established by the Council of the Inspectors General on Integrity and Efficiency and the Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority.

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.

Control panel at a nuclear power plant.

Construction progress at V.C. Summer Unit 3. *Photo courtesy of David Failla.*

OIG STRATEGIC 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.

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. 27, No. 1
October 2013