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

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

Semiannual Report to Congress

April 1, 2016–September 30, 2016

OIG VISION

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

OIG MISSION

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

COVER PHOTOS:

Top: Turbine rotor for Vogtle 3 and 4 nuclear power plant construction site. (Courtesy Georgia Power)

Left: CA01 module is placed at the V.C. Summer site. (Courtesy South Carolina Electric & Gas Company)

Right: NRC Resident Inspector performs on-site inspection.

Bottom: NRC Construction Resident Inspector performs an inspection of reinforcing steel.

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, 2016, to September 30, 2016.

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

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

It was an active 6 months for my office in furtherance of its obligation to timely identify the most critical risks and vulnerabilities in NRC and DNFSB programs and operations to allow NRC and the DNFSB to take any necessary corrective action. The work highlighted in this report includes audits of NRC's significant determination process for reactor safety, oversight of 10 CFR 50.59, "Changes, test and experiments," decommissioning funds program, reactor oversight process, and the technical assistance request process. In addition, this report includes audits of DNFSB's process for developing, implementing and updating policy guidance, and oversight of nuclear facility design and construction projects.

During this semiannual reporting period, OIG issued 11 NRC and 3 DNFSB audit reports. As a result of this work, OIG identified vulnerabilities in, and made a number of recommendations to improve the effective and efficient operation of NRC's safety, security, and corporate management programs and those of the DNFSB. OIG also opened 25 investigations, and completed 23 cases. Three of the open cases were referred to the Department of Justice, and 39 allegations were referred to NRC management for action.

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

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

Hubert T. Bell
Inspector General

NRC Headquarters complex.

CONTENTS

Fire equipment inspection at Calvert Cliffs Nuclear power plant.

HIGHLIGHTS

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

NRC Audits

- A Technical Assistance Request (TAR) is a request for technical assistance from an NRC headquarters or regional office, or an Agreement State. These requests are generally sent to the Office of Nuclear Material Safety and Safeguards (NMSS) and involve issues related to nuclear materials. The process of sending these requests, along with receipt of the ensuing responses, constitute the TAR process. The purpose of the TAR process is to support NRC organizations external (and sometimes internal) to NMSS in the most efficient and effective manner. A TAR contains questions on subjects involving regulatory or policy interpretations, inspection findings, or a technical area in which NMSS possesses expertise or for which it has responsibility. The audit objective was to determine if NRC's TAR process facilitates effective and efficient responses and focused on TARs submitted by the regional offices to NMSS.

- NRC's Reactor Oversight Process (ROP) is a risk-informed, performance-based, tiered approach to assessing plant safety. Baseline inspections are the minimum level of inspection required to ensure plant safety and security, and are common to all operating nuclear plants. The baseline inspections focus on activities and systems that are risk significant. The audit objective was to assess the effectiveness of the ROP in discovery of plant performance issues. For the purposes of this audit, the assessment of the effectiveness of the ROP was limited to an analysis of how inspection procedures were written, understood, and performed by agency managers and inspection staff.

- OIG contracted with Willis Towers Watson to conduct the sixth Safety Culture and Climate Survey (SCCS) between November 23, 2015, and December 31, 2015. The survey response rate was 70 percent, which was sufficient to provide a reliable and valid measure of the current attitudes and perceptions of NRC employees. The objective of the SCCS was to identify areas of strength and opportunities for improvement pertaining to NRC's safety culture and climate and to benchmark against prior survey results. To appreciate the benchmark comparisons, it should be recognized that NRC was operating in a different environment and experienced significant organizational transformations since the 2009 and 2012 surveys. Specifically, in 2009, NRC was in the midst of the nuclear renaissance and experiencing significant organizational growth. Since 2012, NRC experienced changes in senior leadership, office reorganizations, and the implementation of agencywide initiatives such as Project AIM to rebaseline the organization. OIG expects the agency will use the survey data to develop and inform agencywide and office-specific action planning to address opportunities for improvement and to strengthen the agency's overall safety culture and climate.

- On July 22, 2010, the *Improper Payment Elimination and Recovery Act* (IPERA), which amended the *Improper Payments Information Act* (IPIA), was signed into law. IPERA directed the Office of Management and Budget (OMB) to issue implementing guidance to Federal agencies that are required to periodically review all programs and activities they administer to identify all programs and activities that may be susceptible to significant improper payments. In addition, IPERA also requires each agency to conduct recovery audits with respect to each program and activity of the agency that expends $1,000,000 or more annually, if conducting such audits would be cost-effective. On January 10, 2013, the *Improper Payment Elimination and Recovery Improvement Act* (IPERIA) was signed into law and established the *Do Not Pay Initiative*, which directs agencies to verify the accuracy of payments using databases before making payments. OMB guidance specifies that each agency's Inspector General should review agency improper payment reporting in the agency's annual Performance Accountability Report (PAR) or Financial Report, and accompanying materials, to determine whether the agency complied with IPERA. The audit objective was to assess NRC's compliance with IPIA, as amended by IPERA and IPERIA, and report any material weaknesses in internal control.

- NRC manages numerous publicly accessible Web applications to share nuclear information with licensees and the public. NRC's publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency information technology (IT) resources. NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought by potential adversaries. The NRC OIG has joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG will assess its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications. The objectives of the audit were to determine (1) the effectiveness of NRC's efforts to secure its publicly accessible Web applications, and, (2) whether NRC has implemented adequate security measures to reduce the risk of compromise for it's publicly accessible Web applications.

- NRC regulates the decommissioning of nuclear power plants, material sites, fuel cycle facilities, research and test reactors, and uranium recovery facilities, with the ultimate goal of license termination. NRC maintains strict rules governing nuclear power plant and material site decommissioning. These requirements were developed to protect workers and the public during the entire decommissioning process and after the license is terminated. Federal law and NRC regulations require that power reactor and material licensees establish or obtain a financial mechanism such as a decommissioning trust fund or a guarantee to ensure there will be sufficient money to pay for the facility's decommissioning. The audit objectives were to identify opportunities for program improvement, and determine the adequacy of NRC's processes for coordinating with licensees to address possible shortfalls.

- The *Reducing Over-Classification Act* of 2010 mandated that the Inspectors General of all Federal agencies with original classification authority perform at least two evaluations over proper use of classified information. The act found that over-classification of information negatively affects dissemination of information within the Government, increases information security costs, and needlessly limits stakeholder and public access to information. NRC OIG issued the first mandatory audit report in 2013. The report's recommendations have been implemented by NRC. This report represents the results of OIG's second mandatory review. The audit objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed and effectively administered, and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

- *The Cybersecurity Act* was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. The act requires that Inspectors General report on the policies, procedures, and controls to access covered systems. Covered systems are defined as a national security system, or a Federal computer system that provides access to personally identifiable information (PII). NRC uses three different types of national security systems to process and store classified information: standalone systems, subscriber systems, and shared service systems. Federal policy requires that classified information may only be stored, processed, or transmitted using systems that have been granted an NRC authorization to operate for classified information processing. The audit objective was to assess NRC's information technology security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to PII operated by or on behalf of NRC.

- NRC oversees nuclear power plant licensees' compliance with requirements stipulated in Title 10, Energy, Code of Federal Regulations, Section 50.59, "Changes, tests and experiments" (10 CFR 50.59). 10 CFR 50.59 establishes the conditions under which licensees may make changes to their facilities or procedures, and conduct tests or experiments, without prior NRC approval for a license amendment. When implementing the provisions of 10 CFR 50.59, licensees use a process, which involves applicability review, screening, evaluation, and documentation and reporting. In 2015, NRC staff estimated the number of licensee 10 CFR 50.59 implementation actions and found that for each operating reactor unit, licensees conduct approximately 475 screenings annually, from which result about 5 evaluations. This amounts to a combined total of about 49,000 screenings and evaluations per year. The audit objective was to assess the consistency and effectiveness of NRC's oversight of 10 CFR 50.59 implementation.

- *The Federal Managers' Financial Integrity Act* (FMFIA) requires Federal agencies, including NRC, to establish and maintain effective internal control over its operations to help accomplish its mission. FMFIA requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and

administrative control of each executive agency. Further, FMFIA requires that the head of each executive agency report annually to the President and Congress on their agency's compliance with FMFIA requirements. NRC updated Management Directive (MD) 4.4, *Internal Control*, in 2012 to comply with FMFIA. MD 4.4 established a uniform process for the agency to assess internal control that meets FMFIA requirements. The audit objectives were to (1) assess the NRC fiscal year (FY) 2015 compliance with FMFIA, and (2) evaluate the effectiveness of NRC's process to assess internal control over program operations, as reported in the Chairman's FMFIA Statement published in the agency's PAR.

- NRC's Significance Determination Process (SDP) is used to determine the safety significance of inspection findings identified within the Reactor Oversight Process (ROP) cornerstones of safety. NRC inspectors perform inspections at nuclear reactor sites to identify licensee failures to meet a regulatory requirement or self-imposed standard that a licensee should have met. The SDP consists of several steps and activities performed by agency staff and management to determine and categorize the significance of licensee performance deficiencies identified through inspections. The SDP also requires an independent audit of inspection findings to ensure significance determination results are predictable and repeatable. The audit objective was to assess the consistency with which NRC evaluates power reactor safety inspection findings under the SDP.

Defense Nuclear Facilities Safety Board Audits

- In January 2015, a Government Accountability Office audit noted the Defense Nuclear Facilities Safety Board (DNFSB) had few written policies. Subsequently in June 2015, DNFSB updated its directives program, including assigning roles and responsibilities for the drafting, issuance, and implementation of directives and supplementary documents. Particularly, DNFSB has increased its effort to establish directives and supplementary documents to support policies and procedures. The audit objectives were to (1) determine if DNFSB has an established process for developing, implementing, and updating policy guidance for staff; (2) determine if DNFSB implemented the recently issued operating procedures at the Board member level; and (3) identify any opportunities to improve these processes.

- The *Atomic Energy Act of 1954*, as amended, requires that DNFSB review the design and construction of new defense nuclear facilities to ensure the adequate protection of public health and safety during operation. DNFSB provides oversight of Department of Energy (DOE) defense nuclear facilities as well as those managed by the National Nuclear Security Administration (NNSA). DNFSB provides oversight of design and construction activities at the following sites: Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Nevada National Security Site, Pantex, Sandia National

Laboratories, Savannah River Site, Y-12 National Security Complex/Oak Ridge National Laboratory, Hanford, Idaho National Laboratory, and the Waste Isolation Pilot Plant. According to the DNFSB 2015 Annual Report to Congress, DNFSB is actively overseeing the design and construction of over a dozen new defense nuclear projects with a projected total cost exceeding $25 billion. The audit objective was to assess the efficiency and effectiveness of DNFSB's oversight of nuclear facility design and construction projects.

- The *Cybersecurity Act of 2015* was enacted on December 18, 2015, and designed to improve cybersecurity in the United States. The act requires that Inspectors General report on the policies, procedures, and controls to access "covered systems." Covered systems are defined as a national security system, or a Federal computer system that provides access to PII. DNFSB relies on the servicing organizations to properly protect the records, but must review the privacy impact assessment to determine whether they are using proper controls. The audit objective was to evaluate DNFSB's information technology security policies, procedures, practices, and capabilities as defined in the *Cybersecurity Act of 2015* for national security systems and systems that provide access to PII operated by or on behalf of DNFSB.

NRC Investigations

- OIG conducted three separate investigations involving NRC material licensees in Puerto Rico that falsely certified themselves as small business entities to receive reduced material license fees.

- OIG conducted an investigation into two incidents of network intrusion attempts into the resources connected to the NRC public facing Web site.

- OIG conducted an investigation regarding a notification by NRC that several senior NRC managers were targets of credential harvesting phishing emails.

- OIG conducted an investigation into an allegation that, in violation of NRC's ROP, an NRC senior manager instructed resident inspectors not to document Green findings at a plant if the plant places the findings in their corrective action program (CAP).

- OIG conducted an investigation into an allegation that NRC technical staff were prevented by their management from issuing a Request for Additional Information to an NRC licensee in connection with the financial condition of its nuclear plants.

- OIG conducted an investigation into an allegation that a DNFSB Board Member told a DNFSB employee not to share details relating to the operation of a pump at a DOE site with other DNFSB Board Members.

Spent fuel cask on rail transport.

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 news media reports of corruption took a toll on the American public's faith in its Government. The U.S. Congress knew it had to take action to restore the public's trust. It had to increase oversight of Federal programs and operations. It had to create a mechanism to evaluate the effectiveness of Government programs. And, it had to provide an independent voice for economy, efficiency, and effectiveness within the Federal Government that would earn and maintain the trust of the American people.

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

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

OIG Mission and Goals

NRC's OIG was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendment to the IG Act. NRC OIG's mission is to (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.**

Inspection of construction at V.C. Summer nuclear power station.

NRC OIG PROGRAMS AND ACTIVITIES

Audit Program

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

- **Survey phase**—An initial phase of the audit process is used to gather information, without detailed verification, on the areas and activities to be audited. 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 (DOJ) 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; the OIG audit program; the OIG Hotline; and OIG initiatives directed at areas bearing a high potential for fraud, waste, and abuse.

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

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

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

OIG General Counsel Regulatory Review

Regulatory Review

Pursuant to the *Inspector General Act*, 5 U.S.C. App. 3, Section 4(a)(2), OIG reviews existing and proposed legislation, regulations, policy, and implementing Management Directives, 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.

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

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

From April 1, 2016, to September 30, 2016, OIG reviewed a variety of agency documents including Commission papers (SECYs), Staff Requirements Memoranda, Federal Register Notices, Management Directives, regulatory actions, and statutes.

Comments provided on the most significant matters addressed during this period are described below:

Management Directive (MD) and Directive Handbook (DH) 7.*8*, *Outside Employment*. Provides guidance on the NRC policy that agency employees must receive written approval before engaging in certain nuclear industry related outside employment, in accordance with ethics regulation 5 CFR 5801.103.

The objective of this MD is to inform employees of outside employment that may be incompatible with their NRC employment. Specifically, it informs employees when prior approval to engage in outside employment is required, and identifies the NRC officials who are authorized to grant approvals necessary for employees to engage in this outside employment. OIG comments on the most recent revision to this important directive suggested additional clarification as to the deciding authority when there is a difference of opinion between Regional Counsel and headquarters Office of the General Counsel (OGC) in providing guidance, and that relevant ethics opinions be required as an attachment to employee requests for outside employment approval.

MD and DH 7.*10*, *Political Activity*. OIG suggested clarification that alleged violations of political activity laws and regulations are referred to the Office of Special Counsel (OSC) and that OIG provides coordination and liaison with the OSC and DOJ, as required, on application of the laws and regulations concerning prohibited political activity. OIG also noted the need to clarify that an NRC employee may report suspected violations of political activity laws and regulations to the OIG, which will coordinate and refer suspected Hatch Act violations to the OSC and to specify that OSC independently investigates alleged Hatch Act violations.

MD and DH *10.37*, *Position Evaluation and Benchmarks.* OIG provided detailed comments on technical aspects of position evaluation and benchmarks and observed that many of the benchmark positions were outdated and may not be suitable for accurate determination of grade levels of positions.

MD and DH *10.131*, *Protection of NRC Employees against Ionizing Radiation*. OIG noted that the described organizational responsibilities of the Director, Office of Nuclear Material Safety and Safeguards (NMSS), "Establishes standards for protection against ionizing radiation and provides technical oversight of the radiation safety programs to the NRC headquarters, regions, and the Technical Training Center," provided no description, even at a high level, of the framework or nature of this technical oversight, or a description of the oversight and criteria to be used by NMSS. OIG commented that a clearer description of the requirements and expectations for NMSS oversight of the agency's radiation safety programs would strengthen the consistency and effectiveness of internal controls in this important area.

MD and DH *4.1*, *Accounting Policy and Practices.* This MD was revised to reflect organizational changes for the Office of the Chief Financial Officer (OCFO) and the Office of the Chief Information Officer (OCIO) to comply with generally accepted accounting principles and standards, and align with other Federal financial requirements. OIG commented that the MD executive summary should include a reference to an OCFO Accounting Policy Manual in use at NRC and suggested a change of language in the guidance to state that accounting practices, "Provide timely and reliable accounting results using the accrual basis of accounting for: allocating resources; preparation and support of budget requests; recognizing the full cost of NRC programs, activities, and outputs; and controlling budget execution."

Other OIG Activities

The General Counsel to the Inspector General addressed OGC Honor Law Graduate attorneys as part of their agency orientation briefings. The OIG General Counsel provided information describing OIG, its history, statutory basis, implementing regulations, and relevant case law. In addition, the role of IG counsel, both at NRC and in the Federal community, were detailed and compared. The group discussed interaction protocols between agency attorneys and the OIG, including key interoffice connections in effecting the *Program Fraud Civil Remedies Act* (PFCRA) litigation and educational efforts related to whistleblower rights under the *Whistleblower Protection Enhancement Act*.

In August 2016, Mr. Stephen Dingbaum, OIG Assistant Inspector General for Audits (AIGA), retired after 42 years of distinguished Federal service. Mr. Dingbaum joined OIG as the AIGA in 2000. He continually guided his staff to focus on and assess areas that would enhance, strengthen, and promote greater economy and efficiency in agency programs and operations. As a result, many positive changes were made. Under Mr. Dingbaum's leadership, the audit staff received 16 awards from the Council of the Inspectors General on Integrity and Efficiency (and its predecessor organization) in recognition of outstanding audit work.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission* as of October 1, 2015 *(as identified by the Inspector General)*	
Challenge 1	*Regulation of nuclear reactor safety programs.*
Challenge 2	*Regulation of nuclear materials and radioactive waste programs.*
Challenge 3	*Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.*
Challenge 4	*Management of information technology and information management.*
Challenge 5	*Management of financial programs.*
Challenge 6	*Management of administrative functions.*

** For more information on the challenges, see OIG-16-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC, http://www.nrc.gov/docs/ML15274A142.pdf*

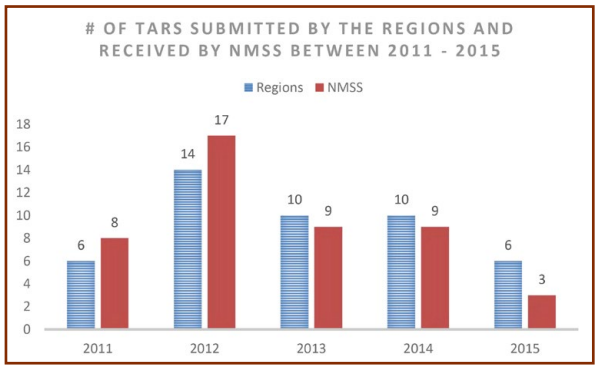
NRC AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed 11 financial and performance audits or evaluations, all of which are summarized here that resulted in numerous recommendations to NRC management.

Audit Summaries

Audit of NRC's Technical Assistance Request Process (TAR)

OIG Strategic Goal: Safety



Source: OIG analysis of TAR data from the regions and NMSS.

A TAR is a request for technical assistance from an NRC headquarters or regional office, or an Agreement State. These requests are generally sent to NMSS and involve issues related to nuclear materials. The process of sending these requests, along with receipt of the ensuing responses, constitute the TAR process.

The purpose of the TAR process is to support NRC organizations external (and sometimes internal) to NMSS in the most efficient and effective manner. A TAR contains questions on subjects involving regulatory or policy interpretations, inspection findings, or a technical area in which NMSS possesses expertise or responsibility.

The audit objective was to determine if NRC's TAR process facilitates effective and efficient responses. This audit focused on TARs submitted by the regional offices to NMSS.

Audit Results:

OIG found that NRC's TAR process facilitates effective responses; however, opportunities for improvement exist with regard to efficiency. Specifically, NRC should improve its communication and documentation associated with the TAR process.

NRC's TAR process requires the TAR requester to complete and submit a TAR request form. The request form includes a field where the requester must list previously completed TARs that have addressed similar issues. To locate previously submitted TARs, the TAR requester must search NRC's Agencywide Documents Access and Management System (ADAMS). However, TARs saved in ADAMS are often difficult to find. Furthermore, NMSS staff have not been profiling TARs in ADAMS in a consistent manner. Because TARs are missing from ADAMS and are not profiled consistently among each NMSS division, it is difficult for TAR requesters to search and locate completed TARs in ADAMS.

Additionally, OIG performed an independent verification of TAR records by cross referencing all TARS submitted by the regions to NMSS against those TAR records identified by NMSS as being submitted by the regions for the same time period. OIG's

verification confirmed that these records did not align. OIG also found an additional TAR in ADAMS that was not identified by NMSS or the regions.

Furthermore, some NRC staff indicated that the TAR process is not clear. Specifically, staff stated that NMSS does not always immediately acknowledge receipt of TARs or provide an estimate on how long it will take to complete a review and response to the TAR. Additionally, regional staff do not always know who TARs are assigned to at headquarters or what the TAR reviewer's strategy is for proceeding. Staff also opined that when a TAR requires additional input or review from OGC, the process can become even less timely and more convoluted.

These inefficiencies occurred because NMSS does not always adequately communicate with the regional offices and does not sufficiently document its TAR procedures. Additionally, there is no central location or TAR support site where all information relating to the TAR process, such as division procedures, TAR forms, TAR status logs, and points of contact, is stored. Lastly, involved offices do not have current, finalized TAR guidance to assist staff in navigating the TAR process. As a result, the TAR process can be untimely, which could consequently result in delays for processing licensees' licensing and decommissioning requests.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Reactor Oversight Process: Reactor Safety Baseline Inspection Procedures

OIG Strategic Goal: Safety

NRC's ROP is a risk-informed, performance-based, tiered approach to assessing plant safety. Baseline inspections are the minimum level of inspection required to ensure plant safety and security, and are common to all operating nuclear plants. The baseline inspections focus on activities and systems that are "risk significant."

The audit objective was to assess the effectiveness of the ROP in discovery of plant performance issues. For the purposes of this audit, the assessment of the effectiveness of the ROP was limited to an analysis of how inspection procedures were written, and understood and performed by agency managers and inspection staff.

Audit Results:

Opportunities exist to make baseline inspection procedures clearer for inspectors and managers performing and overseeing baseline inspections.

NRC staff and managers expressed difficulty distinguishing mandatory and discretionary activities in some baseline inspection procedures. Specifically, language in some inspection procedures include the terms "should" and "shall"; however, the context in which the terms are used is viewed as contradictory and confusing by involved staff, including inspectors.

OIG interviewed 41 staff and managers responsible for performing and overseeing inspections, and managing inspection procedures. Sixty-three percent acknowledged some inspection procedures were not clear. Furthermore, 63 percent of inspectors noted issues with inspection procedure clarity. Several inspectors also mentioned they rely on experience to judge which activities are mandatory and which are discretionary rather than solely relying on inspection procedures. Additionally, 37 percent of inspectors explained they view words such as "should" as indicating a mandatory activity while others view it as signaling a discretionary activity. Furthermore, a senior manager concluded inspectors in the regions and headquarters staff responsible for managing the inspection procedures do not always interpret inspection procedure mandatory and discretionary language the same way.

This occurred because NRC does not have controls in place to ensure clear and consistent language is used to differentiate mandatory and discretionary activities. As a result, there is potential for ineffective and inefficient use of agency resources as NRC inspectors may not perform activities deemed mandatory and instead perform unneeded discretionary activities. There is additional risk associated with how the agency is assured inspectors perform activities deemed mandatory in inspection procedures, given the varying interpretations of mandatory and discretionary language. NRC relies on completion of inspection procedures for assurance that each safety cornerstone has had an adequate assessment, and this assessment is a key input into NRC's assessment of whether nuclear reactor licensees operate safely.

(Addresses Management and Performance Challenge #1)

NRC Office of the Inspector General Safety Culture and Climate Survey: Executive Summary

OIG Strategic Goal: Safety and Corporate Management

OIG contracted with Willis Towers Watson to conduct the 6th SCCS between November 23, 2015, and December 31, 2015. Willis Towers Watson conducted the SCCS for approximately 3,670 NRC employees in the fall of 2015. The survey was provided to all permanent full-time and part-time employees. The survey response rate was 70 percent, which was sufficient to provide a reliable and valid measure of the current attitudes and perceptions of NRC employees.

The objective of the SCCS was to identify areas of strength and opportunities for improvement pertaining to NRC's safety culture and climate and to benchmark against prior survey results.

Survey Results:

To appreciate the benchmark comparisons, it should be recognized that NRC was operating in a different environment and experienced significant organizational transformations since the 2009 and 2012 surveys. Specifically, in 2009, NRC was in the midst of the nuclear renaissance and experiencing significant organizational growth.

Since the last survey in 2012, NRC experienced changes in senior leadership, office reorganizations, and the implementation of agencywide initiatives such as Project Aim to rebaseline the organization.

Successfully cultivating an engaged workforce and managing a culture and climate based on safety requires a great deal of time, resources, and effective leadership. Survey results identified strengths as well as opportunities for improvement.

Strengths were identified in the areas of Mission and Objectives, Supervision, and Training. More specifically, NRC's staff understand the mission, goals, and objectives of their work unit and feel that NRC prepares them for the work they do. In addition, staff feel they have the information they need to do their job and have development and growth opportunities.

NRC's three areas of greatest opportunity include Differing Views Processes, Empowerment and Respect, and Senior Management. Specifically, employees are concerned about using the Non-Concurrence Process and the Differing Professional Opinions Program due to potential negative consequences and have perceptions that management is not recognizing and respecting human differences and is not holding all employees to the same standards of ethical behavior. Moreover, participants do not have confidence in senior management and feel senior management does not provide a clear sense of direction.

(Addresses Management and Performance Challenges #1 through #6)

Audit of NRC's FY 15 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

On July 22, 2010, the IPERA was signed into law, which amended the IPIA. IPERA directed the OMB to issue implementing guidance to Federal agencies that are required to periodically review all programs and activities they administer and to identify all programs and activities that may be susceptible to significant improper payments. In addition, IPERA also requires each agency to conduct recovery audits with respect to each program and activity of the agency that expends $1,000,000 or more annually, if conducting such audits would be cost-effective.

On January 10, 2013, IPERIA was signed into law and established the *Do Not Pay Initiative*, which directs agencies to verify the accuracy of payments using databases before making payments. OMB guidance specifies that each agency's Inspector General should review agency improper payment reporting in the agency's annual PAR or Financial Report, and accompanying materials, to determine whether the agency complied with IPERA.

The audit objective was to assess NRC's compliance with IPIA, as amended by IPERA and IPERIA, and report any material weaknesses in internal control.

Audit Results:

Based on OIG's review of NRC's FY 2015 PAR and other documentation provided by the agency, OIG determined that the agency is in compliance with the requirements of IPIA. OIG also concluded that agency reporting of improper payments is accurate and complete.

(Addresses Management and Performance Challenge #5)

Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications

OIG Strategic Goal: Security

NRC manages numerous publicly accessible Web applications to share nuclear information with licensees and the public. NRC publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency IT resources. NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought by potential adversaries. NRC OIG has joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG will assess its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications.

The objectives of the audit were to determine (1) the effectiveness of NRC's efforts to secure its publicly accessible Web applications, and (2) whether NRC has implemented adequate security measures to reduce the risk of compromise for its publicly accessible Web applications.

Evaluation Results:

NRC has developed several policies, procedures, processes, and standards for ensuring NRC systems and applications are implemented in a secure manner, including guidance specific to the development of Web applications. However, the evaluation team found that NRC's efforts to secure its publicly accessible Web applications may not be effective and NRC has not implemented adequate security measures to reduce the risk of compromise for their publicly accessible Web applications. Specifically, the evaluation identified the following weaknesses:

- NRC does not have an inventory of publicly accessible Web applications.
- NRC cyber security standards are not current.
- NRC Web applications may not be compliant with NRC cybersecurity standards.

- Authorization to Operate the NRC Webcast Portal did not follow the NRC Risk Management Framework process.
- NRC's IT system decommissioning process needs improvement.

These weaknesses occurred, in part, because

- System owners are not required to identify whether any of the assets belonging to their system include publicly accessible Web applications.
- Some NRC cybersecurity standards were not updated.
- Confusion exists regarding which NRC office is responsible for ensuring adequate security measures are in place for contractor-operated systems.
- There is a lack of attention in determining how an internet protocal (IP) address space should be decommissioned or which inventories need to be updated.

As a result of these weaknesses, the security of NRC's publicly accessible Web applications is compromised.

(Addresses Management and Performance Challenges #3 and #4)

Audit of NRC's Decommissioning Funds Program

OIG Strategic Goal: Corporate Management

NRC regulates the decommissioning of nuclear power plants, material sites, fuel cycle facilities, research and test reactors, and uranium recovery facilities with the ultimate goal of license termination. NRC maintains strict rules governing nuclear power plant and material site decommissioning. These requirements were developed to protect workers and the public during the entire decommissioning process and after the license is terminated. Federal law and NRC regulations require that power reactor and material licensees establish or obtain a financial mechanism such as a decommissioning trust fund or a guarantee to ensure there will be sufficient money to pay for the facility's decommissioning. Although there are many factors that can affect nuclear reactor decommissioning costs, generally these costs range from $300-$400 million.

As of July 2015, there were 19 nuclear reactors, 15 complex material sites, 5 research and test reactors, 2 fuel cycle facilities, and 11 uranium recovery facilities in decommissioning.

The audit objectives were to identify opportunities for program improvement, and determine the adequacy of NRC's processes for coordinating with licensees to address possible shortfalls.

Audit Results:

The agency has adequate processes in place for coordinating with licensees to address possible decommissioning fund shortfalls. However, the audit identified multiple weaknesses in the agency's decommissioning funds review process. Specifically, NRC needs to (1) develop guidance on processing power reactor exemptions to reactor licensees, (2) re-evaluate the minimum decommissioning funding estimate formula, (3) strengthen user controls and guidance on conducting decommissioning financial assurance reviews, and (4) consistently document decommissioning financial assurance reviews for material licensees and inventory reviews of financial instruments.

These weaknesses exist because there are no objective criteria for determining the proper use of power reactor decommissioning trust funds and the agency has not established guidance detailing exemptions for reporting decommissioning costs. Consequently, if the agency continues using vague guidance to process decommissioning trust fund exemptions, it may reduce the availability of funds needed for radiological decommissioning. In addition, clarifying decommissioning trust fund regulations reduces the likelihood of licensees requesting and NRC processing unnecessary exemption requests. This will result in a more efficient, streamlined process.

(Addresses Management Challenge #5)

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

OIG Strategic Goal: Security

The *Reducing Over-Classification Act of 2010* mandated that the Inspectors General of all Federal agencies with original classification authority perform at least two evaluations over proper use of classified information. The act found that over-classification of information negatively affects dissemination of information within the Government, increases information security costs, and needlessly limits stakeholder and public access to information. NRC OIG issued the first mandatory audit report in 2013. The report's recommendations have been implemented by NRC. This report represents the results of OIG's second mandatory review.

The audit objectives were to (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed and effectively administered, and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material.

Audit Results:

NRC's implementation of Federal classified information laws and policies protects classified information. Document reviews of NRC classification actions reported from April 2013 through January 2016 revealed no systematic misclassification. However, there are opportunities for improvement of records management of

classified information within NRC. NRC lacks a cohesive approach to records management of classified information, which fosters inadequate understanding of and preparation for records management of classified information.

The lack of records management of classified information within NRC has prevented timely disposition and declassification. NRC has not reviewed classified records for disposition and declassification as required and is not prepared for mandatory reviews.

NRC staff has a backlog of hard copy classified information that requires processing. The agency has approximately 1,500 cubic feet of classified holdings in General Services Administration-approved containers issued across the agency and in security areas approved for the open storage of classified information. Some of the classified material relates to Atomic Energy Commission activities dating to the 1950s.

Additionally, classifiers are uncertain what is an agency record and do not understand how to manage their hardcopy and electronic files. These occurrences are reflected in NRC's 2015 self-inspection report, which noted that keeping drafts and duplicates after a classified document is completed is a "prevalent issue."

Lastly, records management within classified electronic information systems relies on individual approaches to file management. For example, one system user described careful organization of classified email and personal drive contents, but noted system owners do not limit storage volume or push users to cull their account files. File management is not a priority for most users. Individual approaches do not systematically capture classified electronic records and identify them for a scheduled review.

This occurred because of the agency's lack of a cohesive approach to records management. Consequently, misclassification and uncontrolled release of agency records, as well as inefficiency and reduced transparency within the agency's approach to records management may result.

(Addresses Management and Performance Challenges #3 and #4)

Cybersecurity Act of 2015 Audit for NRC

OIG Strategic Goal: Security

The *Cybersecurity Act* was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. The act requires that Inspectors General report on the policies, procedures and controls to access "covered systems." Covered systems are defined as a national security system, or a Federal computer system that provides access to PII. NRC uses three different types of national security systems to process and store classified information including standalone systems, subscriber systems, and shared service systems. Federal policy requires that classified information may only be stored, processed, or transmitted using systems that have been granted an NRC authorization to operate for classified information processing.

The audit objective was to assess NRC's information technology security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to PII operated by or on behalf of NRC.

Audit Results:

NRC's cybersecurity program has established policies and procedures to control access to its "covered systems." However, opportunities exist to strengthen the cybersecurity and physical security controls of NRC's national security systems.

OIG found that NRC has national security systems that were operating without the required authorizations to operate. Seven national security systems were identified, across multiple offices, as not having an authorization to operate. Additionally, four national security systems did not have an authority to use. Lastly, two laptops were identified as being used without an authorization to operate. However, the laptops are no longer being used and will be taken out of service.

This occurred because there is a lack of clarity in the agencywide policies and procedures over the systems and no integrated process across relevant offices. In addition, there is no agencywide inventory of the national security systems. As a result, classified information may be vulnerable or subject to unauthorized disclosure.

(Addresses Management and Performance Challenges #3 and #4)

Audit of NRC's Oversight of 10 CFR 50.59, "Changes, tests, and experiments."

OIG Strategic Goal: Safety

NRC oversees nuclear power plant licensees' compliance with requirements stipulated in Title 10, Energy, Code of Federal Regulations, Section 50.59, "Changes, tests and experiments" (10 CFR 50.59). 10 CFR 50.59 establishes the conditions under which licensees may make changes to their facilities or procedures, and conduct tests or experiments, without prior NRC approval for a license amendment. When implementing the provisions of 10 CFR 50.59, licensees use a process, which involves applicability review, screening, evaluation, and documentation and reporting. In 2015, NRC staff estimated the number of licensee 10 CFR 50.59 implementation actions and found that for each operating reactor unit, licensees conduct approximately 475 screenings annually, from which result about 5 evaluations. This amounts to a combined total of about 49,000 screenings and evaluations per year.

The audit objective was to assess the consistency and effectiveness of NRC's oversight of 10 CFR 50.59 implementation.

Audit Results:

NRC's processes for 10 CFR 50.59 oversight could be strengthened by coordinating communication of 10 CFR 50.59 guidance and process-related information. NRC staff having responsibilities for oversight of 10 CFR 50.59 implementation, including inspectors, and headquarters and regional staff do not always coordinate communication of 10 CFR 50.59 process-related information, including reports and requirements. Additionally, NRC's oversight of the 10 CFR 50.59 process could be strengthened by enhancing the agency's post-qualification 10 CFR 50.59 training to include recurring formal training.

These program weaknesses have occurred because NRC does not employ a well-structured approach for 10 CFR 50.59 process management and NRC's 10 CFR 50.59 training needs were based on the agency's immediate focus on addressing a San Onofre Nuclear Generating Station lessons learned training recommendation. As a result, NRC is risking the consistency and effectiveness of its 10 CFR 50.59 oversight. It is also missing the opportunity to enhance knowledge management and more cost-effectively address training needs by developing training that focuses on key oversight issues and emerging industry trends.

(Addresses Management and Performance Challenge #1)

Audit of NRC's Implementation of the Federal Managers' Financial Integrity Act for Fiscal Year 2015

OIG Strategic Goal: Corporate Management

FMFIA requires Federal agencies, including NRC, to establish and maintain effective internal control over its operations to help accomplish its mission. FMFIA requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency. Further, FMFIA requires that the head of each executive agency report annually to the President and Congress on their agency's compliance with FMFIA requirements. NRC updated MD 4.4, *Internal Control*, in 2012 to comply with FMFIA. MD 4.4 established a uniform process to assess internal control that meets FMFIA requirements.

The audit objectives were to (1) assess the NRC fiscal year 2015 compliance with FMFIA, and (2) evaluate the effectiveness of NRC's process to assess internal control over program operations, as reported in the Chairman's FMFIA Statement published in the agency's PAR.

Audit Results:

Overall, the agency complies with the requirements of the guidance related to the FMFIA Statement. However, the audit identified opportunities to improve the agency's implementation of the assessment of internal controls over program operations.

For example, the audit identified that NRC has not yet fully implemented MD 4.4, which is currently out-of-date. Additionally, NRC was not able to provide documentation to support the completion of all five steps of the MD 4.4 Five-Step Approach to Evaluate Programmatic Internal Control.

These programmatic weaknesses have occurred because of a lack of attention to revising, aligning, and implementing internal control guidance and processes. Specifically, NRC has not made revising and aligning programmatic internal control guidance a priority. An agency manager stated that MD 4.4 is out-of-date and the programmatic internal control chapter has been out-of-date since it was published. NRC staff and management stated that the guidance "veered" away from MD 4.4 and was replaced with annual memoranda from the Chief Financial Officer and Executive Director of Operations. However, these annual memoranda are not on the same hierarchical tier as MDs and thus not as authoritative. Additionally, agency officials could not produce internal control plans for all business and product lines, which is a required step under MD 4.4.

As a result, the NRC Chairman risks using unreliable information to support the annual internal control assessment process. Specifically, unclear and contradictory guidance for strategic planning, internal control, and quarterly performance reviews makes it more difficult to align these related oversight processes to enhance agency operations. Gaps in the information provided in the internal control plans make it difficult for the agency to track its progress in resolving internal control issues. Further, NRC's *Strategic Plan for Fiscal Years 2014-2018* states that NRC seeks to remain a model for regulatory effectiveness. As such, clear, effectively communicated, and consistently applied internal control guidance and processes are integral to implementing the agency's cross-cutting strategy of regulatory effectiveness in support of its safety and security goals.

(Addresses Management and Performance Challenge #5)

Audit of NRC's Significance Determination Process for Reactor Safety

OIG Strategic Goal: Safety

NRC's SDP is used to determine the safety significance of inspection findings identified within the ROP cornerstones of safety. NRC inspectors perform inspections at nuclear reactor sites to identify licensee failures to meet a regulatory requirement or self-imposed standard that a licensee should have met. The SDP consists of several steps and activities performed by agency staff and management to determine and categorize the significance of licensee performance deficiencies identified through inspections. The SDP also requires an independent audit of inspection findings to ensure significance determination results are predictable and repeatable. The audit objective was to assess the consistency with which NRC evaluates power reactor safety inspection findings under the SDP.

Audit Results:

The audit found programmatic weaknesses in NRC's SDP resource tracking, issue screening, and documentation of independent audits. With regard to resource tracking, NRC does not have complete information regarding time needed to complete various steps within the process. Although NRC plans to implement new SDP timeliness metrics and process enhancements, the agency has not regularly evaluated resources needed for SDP workflow and has not established or communicated clear expectations to staff and managers. Consequently, NRC could miss opportunities to identify and remedy SDP workflow problems. Regarding issue screening, the audit found that inspectors sometimes have difficulty determining whether issues should be categorized as minor or more-than-minor because issue screening instructions are unclear. As a result, staff might devote unnecessary resources to documenting minor issues, and risk inconsistent performance deficiency screening. Lastly, NRC lacks controls to ensure that independent audits of greater than Green findings are performed and documented. As a result, NRC risks misrepresenting agency performance in periodic self-assessments, and could miss opportunities to implement programmatic changes identified through independent audits.

(Addresses Management and Performance Challenge #1)

Audits in Progress

Audit of NRC's Fire Protection Oversight

OIG Strategic Goal: Safety

NRC requires every U.S. nuclear power plant to have a robust fire protection program to ensure that nuclear reactors operate safely. Plants can manage their fire safety with either a deterministic or a risk-informed, performance-based approach.

A 1975 fire at the Browns Ferry commercial nuclear reactor in Alabama prompted NRC, in 1979, to establish deterministic fire protection requirements. This approach stipulates that the plant's fire protection plan must outline the overall fire protection program and installed fire protection systems, as well as the means to ensure safe reactor shutdown in the event of a fire.

NRC modified its fire protection regulations, 10 CFR 50.48, "Fire protection," in 2004 to incorporate risk-informed, performance-based fire protection requirements contained in National Fire Protection Association Standard 805. The regulation allows plants to request exemptions to the 1979 or the 2004 standards if the plants can show special circumstances. NRC grants exemptions if they do not present an undue risk to health and safety and if other relevant requirements are met. NRC inspects fire protection programs at individual plants on a triennial basis.

The audit objective is to assess the consistency of NRC's oversight of fire protection programs at operating nuclear power plants.

(Addresses Management and Performance Challenge #1)

Audit of NRC's Oversight of Employee Participation in American Society of Mechanical Engineers Code Committees

OIG Strategic Goal: Corporate Management

NRC oversees the civilian use of nuclear power and materials to assure adequate protection of public health and safety and the environment. In pursuit of its mission, NRC designates select employees as authorized NRC representatives to American Society of Mechanical Engineers (ASME) code committees. These committees are composed of public and private sector personnel who collaborate to develop technical standards, some of which inform Federal regulations governing the commercial nuclear power industry.

Employees assigned to voluntary standards and professional organizations such as ASME must adhere to NRC and other Federal regulations to prevent conflicts of interest, misuse of Government position and resources, and actions that could directly and predictably affect the financial interests of that organization or members of that organization. Federal regulations and standards also require NRC to establish procedures to ensure employees serving on voluntary standards organizations and

professional organizations while on official duty adhere to ethical and other agency requirements.

The audit objective is to assess NRC oversight and compliance with Federal and NRC-developed regulations and rules for employee participation in ASME code committees.

(Addresses Management and Performance Challenge #6)

Audit of NRC's Oversight of Source Material Export to Foreign Countries

OIG Strategic Goal: Safety

Ensuring the effective oversight of source material export controls and associated processes is key to achieving the agency's mission to protect public health and safety and the environment. NRC regulations governing the import/export licensing process are provided in Title 10, Code of Federal Regulations, Part 110, "Export and Import of Nuclear Equipment and Material." NRC issues two types of licenses for the import and export of nuclear material: general licenses and specific licenses.

The NMSS Material Control and Accounting Branch is involved in oversight of the export and import of source material. The branch has responsibilities to facilitate the application of International Atomic Energy Agency safeguards and evaluates the adequacy of physical protection for export licensing reviews and retransfer requests. This branch works to enhance safeguards programs in other countries and promote nuclear non-proliferation. The branch also provides oversight and management of the U.S. National Accounting System for tracking transfers and possession of special nuclear material and it maintains a center of expertise for material control and accountability issues.

The audit objective is to determine the effectiveness of NRC's oversight of the export of source material and transfer of control of source material licenses.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Oversight of Low Level Radioactive Waste (LLRW) Disposal and Blending

OIG Strategic Goal: Safety

LLRW is typically produced at nuclear power reactors, hospitals, research facilities, and clinics from the use of nuclear materials for industrial and medical purposes. LLRW disposal occurs at commercially operated disposal facilities that must be licensed by either NRC or an Agreement State. LLRW is classified at the time of disposal in terms of the concentration of specific radioactive isotopes in the waste. Most LLRW (about 95 percent) has the lowest concentration and is Class A. Class B and Class C wastes may have higher concentrations.

Currently, there are four LLRW disposal facilities, all of which are licensed and regulated by Agreement States.

Blending of LLRW means mixing wastes of different concentrations to create product with more uniform and sometimes lower radionuclide concentrations. Blending higher activity and lower activity waste can lower the average concentration of radioactivity, making it suitable for disposal at more locations and at a lower cost. Disposal of LLRW is an expensive endeavor for licensees, and waste blending could be a cost-cutting solution. NRC's oversight of licensees is important to ensure that concentration averaging requirements for licensees result in the safe and effective disposal of both blended and non-blended LLRW.

The audit objective is to determine if the disposal and waste blending processes at disposal facilities are done safely and effectively.

(Addresses Management and Performance Challenge #2)

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016

OIG Strategic Goal: Security

The Federal Information Security Modernization Act of 2014 (FISMA) requires an independent evaluation of NRC's information security program and practices. 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 audit objective is to conduct an independent evaluation of the NRC's implementation of FISMA for FY 2016.

(Addresses Management and Performance Challenge #3)

Audit of Security Over Decommissioning Plants

OIG Strategic Goal: Security

The Security Oversight and Support Branch within the Office of Nuclear Security and Incident Response plans, coordinates, and manages the oversight activities for security at decommissioned power reactors. "Decommission" means to remove a nuclear facility from service and reduce residual radioactivity to a level that permits (1) release of the property for unrestricted use and termination of the license, or (2) release of the property under restricted conditions and termination of the NRC license. Nineteen nuclear reactors in the U.S. are undergoing decommissioning. Decommissioning begins when a licensee notifies NRC of its plans to permanently cease operations, and must be completed within 60 years of cessation of operations.

During decommissioning, the fuel is removed from the reactor, cooled in the spent fuel pool, and then placed in dry cask storage. As long as there is fuel onsite, a decommissioning power plant must continue to maintain a physical protection program that provides high assurance that the activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public. NRC provides oversight of licensee security programs at decommissioning nuclear power plants through an inspection program.

The audit objective is to determine whether the security inspection program provides adequate protection of radioactive structures, systems, and components at decommissioning reactors.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Foreign Assignee Program

OIG Strategic Goal: Security

NRC's Foreign Assignee Program was approved by the Commission in 1974 and began accepting assignees during the 1980s. Following background and biographical checks, an invitation is extended to a proposed assignee. NRC's Office of International Programs approves or disapproves the assignment to NRC and designates the NRC office to which the foreign assignee will be assigned.

Multiple NRC offices develop security plans specifying the security-related procedures, requirements, and restrictions for the assignee's NRC assignment. An information technology security plan covers computer configurations and connections.

In June 2015, NRC's Designated Approval Authority (DAA) approved a request to initiate a pilot program to allow foreign assignees access to NRC's Local Area Network (LAN). The DAA approval waived the background investigation

requirements for NRC LAN access as required by NRC Management Directives for the requested foreign assignee.

The audit objective is to assess whether the foreign assignee program provides adequate information security.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Managerial Cost Accounting Practices

OIG Strategic Goal: Corporate

NRC must be a prudent steward of its fiscal resources through sound financial management. Sound financial management includes the production of timely, useful, and reliable cost accounting information to support agency management. An effective cost accounting system assures full alignment of programs with outcomes in compliance with the *Statement of Federal Financial Accounting Standards No. 4*, Managerial Cost Accounting Concepts and Standards.

To be an effective tool for management decisionmaking, a cost accounting system requires an effective internal control process over data collected and its reporting functions. NRC is required to generate cost accounting information and use cost information to support managerial decisionmaking to provide accountability for decisions and to assure achievement of the best value for the agency's dollars.

The audit objectives are to determine whether NRC (1) is complying with the requirements of *Statement of Federal Financial Accounting Standards No. 4* and (2) has established an effective system of internal control over the production and use of cost accounting data and information.

(Addresses Management and Performance Challenge #5)

Audit of NRC's Purchase Card Program

OIG Strategic Goal: Corporate Management

The *Government Charge Card Abuse Prevention Act of 2012* (Charge Card Act), Public Law 112-194, requires all executive branch agencies to establish and maintain safeguards and internal controls for charge cards. OMB guidance requires each agency head to provide an annual certification that the appropriate policies and controls are in place or that corrective actions have been taken to mitigate the risk of fraud and inappropriate charge card practices. The annual certification should be included as part of the existing annual assurance statement under FMFIA (31 U.S.C. 3512(d)(2)). Under the *Charge Card Act*, Inspectors General are required to conduct periodic risk assessments of agency purchase card programs to analyze the risks of illegal, improper, or erroneous purchases. Status reports on Inspectors General

purchase card audit recommendations, if any, must be submitted to OMB by January 31, 2017, for compilation and transmission to Congress and the U.S. Comptroller General.

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

(Addresses Management and Performance Challenge #6)

Audit of NRC's FY 2016 Financial Statements

OIG Strategic Goal: Corporate Management

Under the *Chief Financial Officers Act* and the *Government Management and Reform Act*, OIG is required to audit the financial statements of the NRC. The report on the audit of the agency's financial statements is due on November 15, 2016. In addition, OIG will issue reports on NRC's

- Special Purpose Financial Statements.
- Implementation of FMFIA.
- Condensed Financial Statements.
- Compliance with IPERA.

The audit objectives are to

1. Express opinions on the agency's financial statements and internal controls.
2. Review compliance with applicable laws and regulations.
3. Review the controls in NRC's computer systems that are significant to the financial statements.
4. Assess the agency's compliance with OMB Circular A-123, Revised, "Management's Responsibility for Enterprise Risk Management and Internal Control."
5. Assess agency compliance with IPERA.

(Addresses Management and Performance Challenge #5)

Vogtle Unit 3 nuclear island containment with cooling tower in background. *Photo courtesy of Georgia Power*

NRC INVESTIGATIONS

During this reporting period, OIG received 117 allegations, initiated 25 investigations, and closed 23 cases. In addition, OIG made 39 allegation referrals to NRC management and 3 investigation referrals to the Department of Justice.

Investigative Case Summaries

False Claims of Small Business Entity Status by NRC Licensees

OIG Strategic Goal: Corporate Management

OIG proactively initiated three separate investigations involving NRC material licensees that submitted false claims of small business entity status. Licensees that certify themselves as small business entities are eligible to receive reduced material license fees. NRC requires companies seeking small business entity status to complete NRC Form 526 as part of the qualification process. Form 526 states that an NRC licensee that qualifies as a small entity under a specific size standard established by the NRC may pay a reduced annual fee by filing the required certification on NRC Form 526. To claim a reduced annual fee under size standard 1A on NRC Form 526, effective August 30, 2013, the company's average gross receipts must be $7.0 million or less over its last 3 completed fiscal years. Prior to August 20, 2013, the average was $6.5 million over the same period. NRC Form 526 also states that licensees that are subsidiaries of larger entities, including foreign entities, do not qualify as small business entities if the aggregate totals of the parent company are not within the guidelines of NRC Form 526.

Investigative Results:

OIG determined that one company in Puerto Rico applied and received small business entity status from the NRC for FY 2011 through FY 2015, which allowed the company to save a total of $31,400 in NRC licensee fees. However, the company's financial records and audited financial statements, from 2007 through 2015, revealed that the company never had gross receipts lower than $35.8 million. Therefore, the average gross receipts were above both the $6.5 and $7.0 million thresholds, failing to legitimately qualify the company as a small business entity under NRC standards. The company entered into a civil settlement agreement with the United States Attorney's Office (USAO), agreeing to pay the $31,400 owed to NRC, plus a $31,400 penalty, totaling $62,800.

OIG determined that a second company in Puerto Rico applied and received small business entity status from the NRC for FY 2014 through FY 2015, which allowed the company to save a total of $12,000 in NRC licensee fees. However, the company's financial records and audited financial statements, from 2010 through 2014, revealed that the company never had gross receipts lower than $29.7 million. Therefore, the average gross receipts were above the $7.0 million threshold, failing to legitimately qualify the company as a small business entity under NRC standards. The company entered into to a civil settlement agreement with the USAO, agreeing to pay $30,000 to settle the matter.

OIG determined that a third company in Puerto Rico applied and received small business entity status from the NRC for FY 2013 through FY 2015, which allowed the company to save a total of $19,600 in NRC licensee fees. However, the company's financial records and audited financial statements, from 2008 through 2014, revealed that the company never had gross receipts lower than $76.3 million. Therefore, the average gross receipts were above both the $6.5 and $7.0 million thresholds, failing to legitimately qualify the company as a small business entity under NRC standards. The company entered into to a civil settlement agreement with the USAO, agreeing to pay the $19,600 owed to NRC, plus a $19,600 penalty, totaling $39,200.

(Addresses Management and Performance Challenge #6)

Intrusion Attempts Into Resources Connected to the NRC Public Web Site

OIG Strategic Goal: Security

OIG initiated an investigation based on a review of network incident reports provided by the OCIO, covering May 2014 - April 2015. The OIG Cyber Crimes Unit (CCU) identified two incidents of network intrusion attempts into the resources connected to the NRC public facing Web site. The first incident occurred on May 20, 2014, and involved more than 3.7 million requests from a single Internet Protocol (IP) address to NRC public ADAMS. The second incident occurred between May 2 and May 27, 2014, when an unknown person attempted to compromise a database server, which was connected to an NRC public facing Web site. There was no known loss of data from either intrusion attempt and there is no indication that the attacks were successful.

In the May 20, 2014, incidents to NRC's Public facing Web site, the requests were in the form of thousands of variations of malicious requests made in a systematic manner across the public Web site. The requests appeared to utilize various types of exploits, such as password access and command execution. In the second incident, NRC reported that there were several unsuccessful access attempts directed against NRC public ADAMS from May 2 to May 27, 2014. The attempts were initially identified by the NRC Security Operations Center review of Intrusion Detection System logs. Further review of logs confirmed the intrusion attempts. Examination of the database server, event logs, and other logs confirmed that none of the attempted attacks were able to penetrate NRC public ADAMS. There was no indication of compromise.

Investigative Results:

CCU's review of the first incident determined that the IP that made more than 3.7 million requests to the NRC public facing Web site on a single day was registered to a company in Canada that rented "unmanaged" servers to its customers. This means that the company had only physical access to the server and could not access

the server's content (no root, administrator, or user access). CCU learned that most of its customers were resellers, renting an Internet infrastructure from the company in order to sell products to their own customers. No further information was available.

CCU's review of the second incident determined that the IP addresses were associated with TOR projects overseas. TOR is a free software for enabling anonymous communication. TOR directs Internet traffic through a free, worldwide, volunteer network consisting of thousands of relays to conceal a user's location and usage. Due to an inability to determine attribution, the CCU coordinated with the Federal Bureau of Investigation (FBI) on the results of this investigation for any action they deemed necessary.

(Addresses Management and Performance Challenge #5)

Credential Harvesting Phishing Email Affecting NRC Senior Managers

OIG Strategic Goal: Security

OIG conducted an investigation based on a notification from the NRC that several senior NRC managers were targets of credential harvesting phishing emails. On April 27, 2014, an unknown individual emailed an unknown number of recipients via Blind Carbon Copy with an email stating their "mailbox storage capacity has been surpassed" and providing a link that prompted users to input their login credentials. The original victim, a senior NRC manager who received the email, clicked on the link and provided his login credentials. Afterwards, the senior manager realized that the email might have been a phishing email and changed his password within 30 minutes of providing the login information. Between the time the manager provided his login information to the time he changed his password, over 2,000 emails were sent from the compromised email account to various recipients on the manager's contact list, both internal to NRC and external to other Government agencies. Another senior NRC manager clicked on the link sent from the original NRC victim and provided his login credentials.

Investigative Results:

OIG determined the individual who sent the email used a domain privacy service that lists proxy contact information in the *Who is* database instead of actual contact information. Entities utilize domain privacy service either to obscure their identity from others or prevent people who harvest emails and contact information from collecting information from the *Who is* database. The individual registered an overseas address. Because this phishing email appeared to have originated from overseas, further information was unavailable. CCU coordinated this investigation with the FBI for any action they deemed necessary.

(Addresses Management and Performance Challenge #5)

Concerns Regarding NRC Management Oversight Pertaining to Potential Inspection Findings

OIG Strategic Goal: Safety

OIG conducted this investigation based on an allegation that in violation of NRC's ROP, an NRC senior manager told resident inspectors not to document Green findings found at a plant if the plant (NRC licensee) places the findings into its CAP. NRC Inspection Manual Chapter 0612, "Power Reactor Inspection Reports," provides guidance on documenting power reactor inspections and findings. It states that a minor violation is a violation associated with a minor performance deficiency, does not warrant enforcement action, and is not normally documented in inspection reports. A Non-Cited Violation (NCV) is a finding that is characterized as Green (very low safety significance). Such findings are documented as violations, but are not cited in notices of violation, which normally require written responses from licensees. OIG's review of information contained in NRC's Digital City-Dynamic Web Page, for the 5-year time period of May 13, 2010, to May 13, 2015, identified that NRC Region II issued 855 Green NCVs, compared to 735 in Region I; 1,131 in Region Ill; and 1,539 in Region IV.

Investigative Results:

OIG could not substantiate whether or not the NRC senior manager instructed resident inspectors not to document Green findings. Although OIG found that some resident inspectors said the senior manager told them not to document Green findings under certain circumstances, other resident inspectors said they did not receive such instruction from the senior manager. In addition, a branch chief sought clarification from the senior manager. The senior manager maintained to OIG and the branch chief that he never told inspectors not to document Green findings; rather, his message was that in cases where inspectors could not decide whether a finding was minor or Green, to make a decision and move on. OIG noted that none of the resident inspectors who said the senior manager instructed them not to document Green findings under certain circumstances followed this instruction. OIG briefed NRC management concerning the apparent misunderstanding of guidance related to Green findings. As a result, OIG learned that NRC's Office of Nuclear Reactor Regulation is establishing new guidelines for determining what is minor or more than minor.

(Addresses Management and Performance Challenge #1)

NRC Management Directed Staff Not To Issue Request for Information Pertaining to Financial Assurance for Operation Costs

OIG Strategic Goal: Safety

OIG conducted this investigation in response to a congressional request to review an allegation that NRC technical staff were prevented from issuing a Request for Additional Information (RAI) to an NRC licensee, in connection with the financial condition of its nuclear plants.

Decommissioning is the safe removal of a nuclear facility from service and the reduction of residual radioactivity to a level that permits release of the property and termination of the license. NRC rules establish site-release criteria and provide for unrestricted and, under certain conditions, restricted release of a site. NRC also requires all licensees to maintain financial assurance that funds will be available when needed for decommissioning. Each nuclear power plant licensee must report to the NRC every 2 years the status of its decommissioning funding for each reactor or share of a reactor that it owns. The report must estimate the minimum amount needed for decommissioning by using the formulas found in 10 CFR 50.75, "Reporting and recordkeeping for decommissioning planning." Licensees may alternatively determine a site-specific funding estimate, provided that amount is greater than the generic decommissioning estimate. NRC staff perform an independent analysis of each of these reports to determine whether licensees are providing reasonable "decommissioning funding assurance" for radiological decommissioning of the reactor at the permanent termination of operation.

Per 10 CFR 50.33(f)(5), NRC may request that a currently operating reactor licensee provide information regarding its financial arrangements and status of funds. Specifically, the Commission may request an established entity or newly-formed entity to submit additional or more detailed information regarding its financial arrangements and status of funds if the Commission considers this information appropriate. One method available to NRC for seeking information from licensees is through an RAI. RAIs are typically issued by NRC when the staff is reviewing proposed licensing actions and needs additional information from the applicant. According to an NRC Office Handbook, the need for additional information relative to a particular licensing action or activity may be identified by the project manager (PM), but generally such a need is identified by the technical branch reviewer. In the latter case, the technical branch reviewer prepares the questions seeking the information and forwards the questions by memorandum to the PM. The PM reviews the questions and discusses any proposed modifications with the originator. The PM then prepares a letter to the affected organization with instructions for responding.

NRC issued an RAI to a licensee pertaining to information provided on the licensee's quarterly 10-K[1] Securities and Exchange Commission (SEC) filing about one of its nuclear power plants. The RAI asked the licensee to provide more detailed information to support NRC's financial qualification review. The RAI had been drafted by an NRC financial analyst who concurred on the draft as acting Branch Chief.

The licensee responded to its RAI with financial projections for the next 5 years. After reviewing this information, the NRC financial analyst was concerned about the financial data and its potential impact on other plants owned by the licensee; as a result, the financial analyst prepared a followup RAI and requested approval from the employee's manager. A draft RAI was provided to the NRC PM who had responsibility for matters pertaining to the licensee's plants. This time, however, after the PM informed the licensee about the draft RAI, the licensee contacted an NRC senior manager to express a concern and met with NRC senior managers about the draft RAI to convey his company's concerns that the followup RAI would have a negative impact on the company. A hold was subsequently issued by NRC managers to the staff on issuing the financial RAIs.

Investigative Results:

OIG could not substantiate impropriety in NRC management's direction to staff not to issue financial related RAIs to licensees, or that an NRC licensee improperly influenced NRC senior managers to make that decision. OIG found that an NRC supervisor, with support from his managers, directed staff to refrain from issuing financial RAIs until the process for issuing this type of request could be better defined and documented. OIG learned that most RAIs are issued by NRC when the staff is reviewing proposed licensing actions and needs additional information from the licensee to make a decision, and that there is a well-defined process for licensing-related RAIs. However, the financial RAIs that were halted by NRC management were unrelated to any licensing action, and it was not clear to the supervisor or his managers what would be done with responses from the licensee. OIG also learned that NRC issued two financial RAIs in the 3 months preceding the decision to postpone further RAIs; however, these were not reviewed by the supervisor, who had been on rotation at the time. OIG further determined that although a licensee representative telephoned the supervisor to express a concern about a draft RAI and requested a "drop-in" meeting to discuss the matter, the supervisor had documented his concerns clearly and shared them with his managers prior to this contact.

OIG found that in March 2015, NRC finalized guidance to staff describing NRC's authority for requesting financial information from licensees and various process aspects, including criteria to determine whether RAIs should be issued, criteria for evaluating information provided by licensees, and closeout and disposition following staff analysis of licensee responses to financial RAIs. OIG was advised by the agency that in July 2016, NRC staff evaluated the 2013 RAIs using the new guidance and concluded no further action was required on the RAIs, which are now considered closed by the staff.

(Addresses Management and Performance Challenge #1)

[1] *The annual report on Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. After it is filed, 10-K information is made available via the SEC Web site.*

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

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

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board* as of October 1, 2015 *(as identified by the Inspector General)*	
Challenge 1	*Organizational culture and climate.*
Challenge 2	*Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.*
Challenge 3	*Human capital management.*
Challenge 4	*Internal controls for technical and administrative/financial programs.*

** For more information on the challenges, see DNFSB-16-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing DNFSB. http://www.nrc.gov/docs/ML1527/ML15274A163.pdf*

DNFSB AUDITS

Audit Summaries

Audit of DNFSB's Process for Developing, Implementing, and Updating Policy Guidance

In January 2015, a Government Accountability Office audit highlighted that the DNFSB had few written policies. Subsequently, in June 2015, DNFSB updated its directives program, including assigning roles and responsibilities for the drafting, issuance, and implementation of directives and supplementary documents. Particularly, DNFSB has increased its effort to establish directives and supplementary documents to support policies and procedures.

The audit objectives were to (1) determine if DNFSB has an established process for developing, implementing, and updating policy guidance for staff, (2) determine if DNFSB implemented the recently issued operating procedures at the Board member level and (3) identify any opportunities to improve these processes.

Audit Results:

DNFSB has an established process for developing, implementing, and updating directives and supplementary documents for staff. DNFSB has also recently issued and implemented Board Procedures to guide Board Member processes. However, opportunities remain to further improve the management of DNFSB's directives program.

Specifically, the audit revealed that there is not a uniform awareness or understanding among involved staff of directive program guidance, including that which addresses timeliness and prioritization expectations for document creation and review. Furthermore, guidance does not address the role of OIG in the draft directive review process.

This occurred because DNFSB management has neglected to incorporate necessary controls and develop staff expertise to improve the directives program. As a result, DNFSB's ability to achieve its mission may be compromised while the less than optimal directives program may lead to possible knowledge drain and miscommunication among staff.

(Addresses Management and Performance Challenges #3 and #4)

Audit of DNFSB's Oversight of Nuclear Facility Design and Construction Projects

Congress created DNFSB to identify the nature and consequences of potential threats to public health and safety at DOE defense nuclear facilities. The *Atomic Energy Act of 1954*, as amended, requires that DNFSB review the design and construction of new defense nuclear facilities to ensure the adequate protection of public health and safety during operation. DNFSB provides oversight of DOE defense nuclear facilities as well as those managed by the NNSA. DNFSB provides oversight of design and construction activities at the following sites: Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Nevada National Security Site, Pantex, Sandia National Laboratories, Savannah River Site, Y-12 National Security Complex/Oak Ridge National Laboratory, Hanford, Idaho National Laboratory, and the Waste Isolation Pilot Plant.

According to the DNFSB 2015 Annual Report to Congress, DNFSB is actively overseeing the design and construction of over a dozen new defense nuclear projects with a projected total cost exceeding $25 billion. The audit objective was to assess the efficiency and effectiveness of DNFSB's oversight of nuclear facility design and construction projects.

Audit Results:

DNFSB oversees defense nuclear facility construction projects as evidenced in planning documents such as oversight plans and review agendas. However, DNFSB's approach to design and construction-specific oversight could be improved by systematizing and aligning organizational and staff-specific communications, roles, and responsibilities in construction oversight activities. The audit also identified misalignment between DOE/NNSA and DNFSB regarding identification and communication of significant safety issues.

These conditions potentially affect DNFSB's effectiveness and efficiency as an oversight body. Specifically, there is potential for

- Non-safety significant issues and safety significant issues to be prioritized equally.
- Risk that potentially affect safety significant issues will be overlooked as DNFSB staff could limit reviews based on personal experience and knowledge (instead of guidance).

- Previously closed issues to be re-opened.
- DNFSB resources not being used in the most effective and efficient way with respect to construction oversight activities.

DNFSB's non-systematic method for construction oversight also contributes to a diminishing confidence among its stakeholders who perceive DNFSB as contributing to cost overruns, project delays, or stoppages of nuclear facility construction projects.

(Addresses Management and Performance Challenge #2)

Cybersecurity Act of 2015 for DNFSB

The *Cybersecurity Act of 2015* was enacted on December 18, 2015, and designed to improve cybersecurity in the United States. The act requires that Inspectors General report on the policies, procedures, and controls to access "covered systems."

Covered systems are defined as a national security system, or a Federal computer system that provides access to PII. DNFSB relies on the servicing organizations to properly protect the records, but must review the privacy impact assessment to determine they are using proper controls. However, DNFSB does not review the privacy impact assessment for external organizations.

The audit objective was to evaluate DNFSB's IT security policies, procedures, practices, and capabilities as defined in the *Cybersecurity Act of 2015* for national security systems and systems that provide access to PII operated by or on behalf of DNFSB.

Audit Results:

DNFSB's cybersecurity program has established policies, procedures, and controls to access to its "covered systems." However, DNFSB does not comply with all requirements of the *Privacy Act of 1974* and the *E-Government Act of 2002*. Specifically, DNFSB does not

- Conduct required reviews of its systems of record.
- Review privacy impact assessments for external servicing organizations.

This is happening because of a lack of adequate internal policies to implement both the *Privacy Act of 1974* and *E-Government Act of 2002*. As a result, PII at DNFSB may be at risk of unauthorized disclosure.

(Addresses Management and Performance Challenge #2)

DNFSB AUDITS

Audits in Progress

Audit of DNFSB's FY 2016 Financial Statements

Under the *Chief Financial Officers Act*, as updated by the *Accountability of Tax Dollars Act of 2002* and OMB Bulletin 15-02, "Audit Requirements for Federal Financial Statements," OIG is required to audit DNFSB's financial statements. The report on the audit of DNFSB's financial statements is due on November 15, 2016.

The audit objectives are to

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

(Addresses Management and Performance Challenge #4)

Audit of DNFSB's Telework Program

The *Telework Enhancement Act of 2010* (the Telework Act), was enacted into law with the goal of ensuring that Federal agencies more effectively integrate telework into their management plans and agency cultures. The Telework Act defines telework as a work-flexibility arrangement under which an employee performs the duties and responsibilities of his or her position from an approved worksite other than the location from which the employee would otherwise work. The Telework Act establishes requirements for agencies when implementing their telework policies. The head of each executive agency needs to establish and implement a policy under which employees shall be authorized to telework. Also, employees must enter into written agreements with their agencies before participating in telework. Moreover, the head of each executive agency must ensure that employees eligible to telework and managers of teleworking employees receive training on telework before the employee enters into a written telework agreement. Currently, DNFSB has approximately 85 of 112 staff members participating in its telework program. Approximately six staff members are teleworking full-time.

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

(Addresses Management and Performance Challenge #3)

Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2016

FISMA requires an independent evaluation of DNFSB's information security program and practices. 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 DNFSB's implementation of FISMA for FY 2016.

(Addresses Management and Performance Challenge #2)

DNFSB INVESTIGATIONS

Investigative Summaries

Board Member Directs Omission of Safety Related Information

OIG conducted an investigation concerning an allegation that a DNFSB Board Member told agency staff stationed at a DOE site that he did not need to share details relating to the operation of a pump with other DNFSB Board Members. Upon learning of the allegation, a Board Member directed the staff member to include the information in his report because all Board Members needed to be aware of the issue. The DNFSB Board ultimately communicated this safety related issue to the DOE in writing.

Investigative Results:

OIG found no evidence to support that the Board Member directed the staff member to withhold safety related information from other Board Members. OIG learned that the staff member documented the safety related information pertaining to the pump in DNFSB weekly reports.

(Addresses Management and Performance Challenge #1)

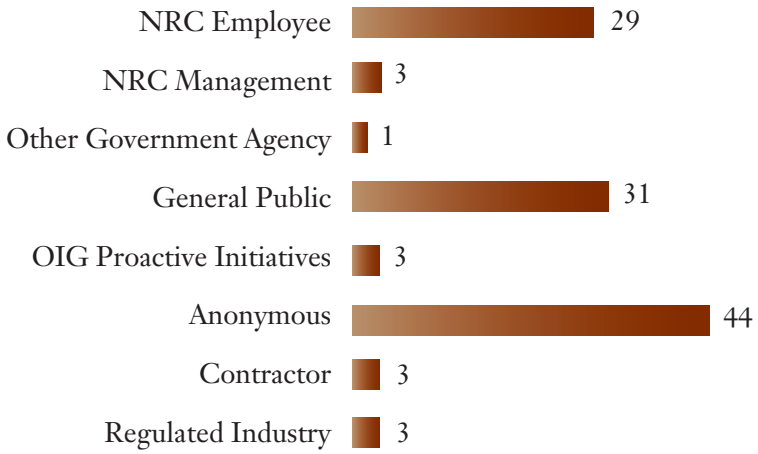
Cooling tower of Limerick Nuclear power plant. *Photo courtesy of Exelon Corp.*

SUMMARY OF NRC OIG ACCOMPLISHMENTS AT NRC

April 1, 2016, Through September 30, 2016

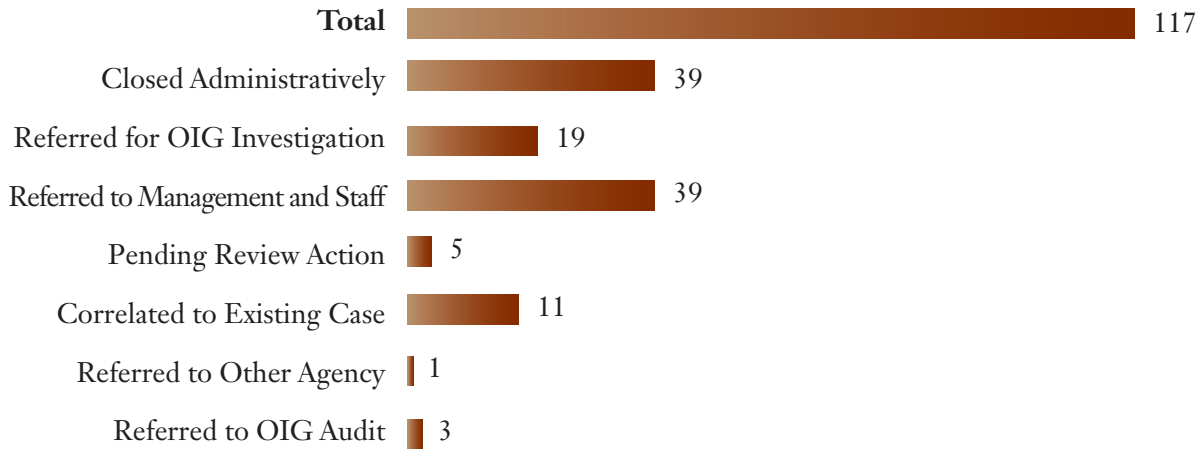
Investigative Statistics

Source of Allegations



Allegations resulting from the NRC OIG Hotline calls: 78 **Total: 117**

Disposition of Allegations



Status of Investigations

DOJ Referrals . . . 3
DOJ Acceptance . . . 1
DOJ Pending . . . 1
DOJ Declinations . . . 1
Criminal Convictions . . . 0
Criminal Penalty Fines . . . 0
Civil Recovery . . . 3
NRC Administrative Actions:
- Counseling and Letter of Reprimand . . . 1
- Terminations and Resignations . . . 0
- Suspensions and Demotions . . . 1
- Other (Letter from Chairman Review of Policy, and ADR) . . . 0

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

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Cases in Progress
Employee Misconduct	9	11	7	13
External Fraud	11	0	6	5
False Statements	1	0	0	1
Internal Fraud	1	0	1	0
Management Misconduct	11	9	4	16
Miscellaneous	4	4	3	5
Proactive Initiatives	5	0	2	3
Technical Allegations	7	1	0	8
Grand Total	**49**	**25**	**23**	**51**

NRC Audit Listings

Date	Title	Audit Number
09/26/16	Audit of NRC's Significance Determination Process for Reactor Safety	OIG-16-A-21
09/19/16	Audit of NRC's Implementation of the Federal Managers' Financial Integrity Act for Fiscal Year 2015	OIG-16-A-20
08/24/16	Audit of NRC's Oversight of 10 CFR 50.59, "Changes, test and experiments"	OIG-16-A-19
08/08/16	Cybersecurity Act of 2015 Audit for NRC	OIG-16-A-18
06/08/16	Audit of NRC's Implementation of Federal Classified Information Laws and Policies	OIG-16-A-17
06/08/16	Audit of NRC's Decommissioning Funds Program	OIG-16-A-16
06/01/16	Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications	OIG-16-A-15
04/29/16	Audit of NRC's FY 15 Compliance with Improper Payment Laws	OIG-16-A-14
04/15/16	NRC Office of the Inspector General Safety Culture and Climate Survey: Executive Summary	OIG-16-A-13
04/06/16	Audit of NRC's Reactor Oversight Process: Reactor Safety Baseline Inspection Procedures	OIG-16-A-12
04/06/16	Audit of NRC's Technical Assistance Request Process	OIG-16-A-11

NRC Contract Audit Reports

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs (Dollars)	Unsupported Costs (Dollars)
09/08/16	Southwest Research Institute Independent Audit Report on Southwest Research Institute's Proposed Amounts on Unsettled Flexibly-Priced Contracts or Subcontracts for FY 2011 NRC-02-06-018 NRC-02-06-021 NRC-02-07-006 NRC-03-09-070 NRC-03-10-066 NRC -03-10-070 NRC-03-10-078 NRC-03-10-081 NRC-04-10-144 NRC-41-09-011 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058	$0	$0

Audit Resolution Activities

TABLE I

OIG Reports Containing Questioned Costs[2]

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	$1,647,715	0
B.	Which were issued during the reporting period	0	0	0
	Subtotal (A + B)	1	$1,647,715	0
C.	For which a management decision was made during the reporting period:			
	(i) dollar value of disallowed costs	0	0	0
	(ii) dollar value of costs not disallowed	0	0	0
D.	For which no management decision had been made by the end of the reporting period	1	$1,647,715	0

[2] *Questioned costs are costs that are questioned by the 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[3]

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

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

TABLE III

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

Date	Report Title	Number
5/26/2003	**Audit of NRC's Regulatory Oversight of Special Nuclear Materials**	**OIG-03-A-15**
	Recommendation 1: Conduct periodic inspections to verify that material licensees comply with material control and accounting (MC&A) requirements, including, but not limited to, visual inspections of licensees' special nuclear material inventories and validation of reported information.	
	Recommendation 3: Document the basis of the approach used to risk inform NRC's oversight of material control and accounting activities for all types of materials licensees.	

SUMMARY OF NRC OIG ACCOMPLISHMENTS AT THE DNFSB

April 1, 2016, through September 30, 2016

Investigative Statistics

Source of Allegations

DNFSB Employee	0
General Public	0
Anonymous	1

Allegations Received from NRC OIG Hotline: 0 **Total: 1**

Disposition of Allegations

Total	**1**
Closed Administratively	0
Referred for OIG Investigation	1
Referred to Management and Staff	0
Pending Review Action	0
Correlated to Existing Case	0
Referred to Other Agency	0
Referred to OIG Audit	0

DNFSB Audit Listings

Date	Title	Audit Number
08/08/2016	Cybersecurity Act of 2015 Audit for DNFSB	DNFSB-16-A-07
07/06/2016	Audit of DNFSB's Oversight of Nuclear Facility Design and Construction Projects	DNFSB-16-A-06
06/29/2016	Audit of DNFSB's Process for Developing, Implementing, and Updating Policy Guidance	DNFSB-16-A-05

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ASME	American Society of Mechanical Engineers
CAP	corrective action program
CCU	Cyber Crime Unit
CFR	Code of Federal Regulations
DAA	Designated Approval Authority
DH	Directive Handbook
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FMFIA	Financial Managers' Financial Integrity Act
FISMA	Federal Information Security Management Act
FY	fiscal year
IG	Inspector General
IAM	Issue Area Monitor
IP	internet protocol
IPERA	Improper Payment Elimination and Recovery Act
IPERIA	Improper Payment Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
IT	information technology
LAN	Local Area Network
LLRW	low-level radioactive waste
MD	Management Directive
NCV	Non-Cited Violation
NNSA	National Nuclear Security Administration
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel (NRC)
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSC	Office of Special Counsel
NMSS	Office of Nuclear Material Safety and Safeguards (NRC)
NRC	U.S. Nuclear Regulatory Commission
PAR	Performance Accountability Report
PFCRA	Program Fraud Civil Remedies Act
PII	Personally Identifiable Information
PM	project manager
RAI	Request for Additional Information
ROP	Reactor Oversight Process
SCCS	Safety Culture and Climate Survey
SEC	Securities and Exchange Commission
SDP	Significance Determination Process
TAR	Technical Assistance Request
USAO	United States Attorney's Office

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	7–8
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	10–12; 14–21; 29–31; 36–38
Section 5(a)(2)	Recommendations for Corrective Action	10–21; 36–38
Section 5(a)(3)	Prior Significant Recommendations Not Yet Completed	49
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	44
Section 5(a)(5)	Information or Assistance Refused	None
Section 5(a)(6)	Listing of Audit Reports	45, 50
Section 5(a)(7)	Summary of Significant Reports	10–21; 29–34; 36–38; 41
Section 5(a)(8)	Audit Reports — Questioned Costs	47
Section 5(a)(9)	Audit Reports — Funds Put to Better Use	48
Section 5(a)(10)	Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made	None
Section 5(a)(11)	Significant Revised Management Decisions	None
Section 5(a)(12)	Significant Management Decisions With Which the OIG Disagreed	None

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

Section 989C.	Peer Review Information	53

APPENDIX

Peer Review Information

Audit

The NRC OIG Audit Program was peer reviewed by the Federal Communications Commission Office of Inspector General on September 17, 2015. NRC OIG received a peer review rating of "Pass." This is the highest rating possible based on the available options of "Pass," "Pass with deficiencies," and "Fail."

Investigations

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

OIG STRATEGIC GOALS

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

The NRC OIG Hotline

The Hotline Program provides NRC and DNFSB 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.

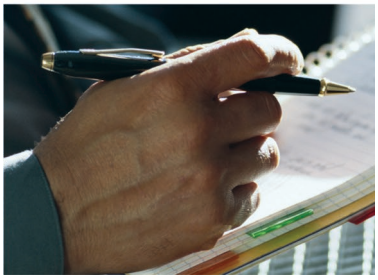
What should be reported:

- 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
TTY/TDD: 7-1-1, or 1-800-201-7165
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. 30, No. 1
October 2016

@NRCgov