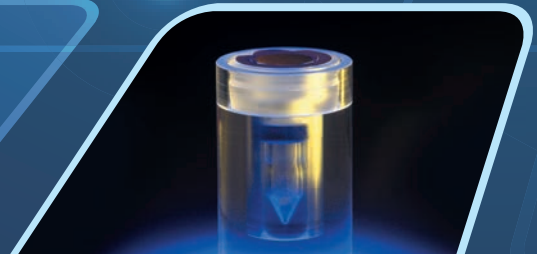
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

OFFICE OF THE INSPECTOR GENERAL
U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Semiannual Report To Congress

April 1, 2017–September 30, 2017



OIG VISION

OIG will identify the most critical risks and vulnerabilities in agency programs and 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:

From left to right:

Cybersecurity agent.

Valve for fire emergency.

Vial containing Y-90 microspheres used to treat liver cancers. *(Photo courtesy: Nordion)*

Nuclear reactor core.

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, 2017, to September 30, 2017.

Our work reflects the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse through the conduct of audits and investigations relating to NRC and Defense Nuclear Facilities Safety Board (DNFSB) programs and operations. The audits and investigations highlighted in this report demonstrate our commitment to ensuring integrity and efficiency in programs and operations at both agencies.

In addition to issuing several legislatively mandated audits and reports pertaining to agency information technology security and improper payment laws, my office issued reports intended to strengthen NRC's and DNFSB's technical and corporate management programs.

During this semiannual reporting period, we issued 20 program audit reports and analyzed 3 contract audit reports. As a result of this work, OIG made a number of recommendations to improve the effective and efficient operation of NRC's and DNFSB's safety, security, and corporate management programs. OIG also opened 24 investigations, and completed 24 cases. Four of the open cases were referred to the Department of Justice, and agency administrative action was taken on four cases.

OIG is 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 our ongoing commitment. My staff 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 diligence and commitment to the mission of this office.

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

Hubert T. Bell
Inspector General

NRC Headquarters complex.

CONTENTS

Resident Inspector 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

- In April 2016, the Nuclear Regulatory Commission (NRC) stopped leasing Government cell phones and instead entered into a contract with AT&T Mobility to purchase Android and iOS devices for up to 350 users. NRC property custodians are assigned responsibility for managing cellphones in the Space and Property Management System (SPMS), which is the official database used to track NRC property inventory assigned to various offices throughout the agency. OIG evaluated whether NRC's Government furnished cell phones are sufficiently managed to provide information security. The report makes four recommendations to improve NRC's management of Government phones.

- NRC and its licensees use the Probabilistic Risk Assessment (PRA) process to estimate the risk of potential accidents at nuclear power plants. PRA is a structured, analytical process for identifying potential weaknesses and strengths of plant designs and operations in an integrated fashion. NRC has a tool to estimate risk at nuclear power plants known as the Standardized Plant Analysis Risk (SPAR) Model Development Programs. During the period January 2016 through July 2016, NRC staff assessed alternatives to using SPAR models, including licensee PRA models. OIG's evaluation assessed NRC's process for piloting alternative risk modeling techniques, including analyzing costs, benefits, and feasibility of these alternatives. The report makes one recommendation to improve the process for assessing alternatives to using SPAR models.

- On June 8, 2017, the Senate Committee on Homeland Security and Governmental Affairs asked OIG to review NRC's processes and compliance with applicable legal standards for preserving certain electronic records as Federal records, and cooperation with congressional document requests, since January 20, 2017. In conjunction with answering the committee's six questions, OIG conducted an evaluation to assess NRC's compliance with applicable legal standards for preserving Federal records, specifically electronic communications for official agency business, since January 20, 2017. The report makes no recommendations as NRC has responded both to emerging technologies and to the requirements to preserve electronic records by establishing and revising policies and supporting implementation by all staff and senior leaders.

- NRC encourages members of the public to use Title 10, Code of Federal Regulations, Section 2.206 (10 CFR 2.206), Requests for Action Under This Subpart, as one method to bring issues to the agency's attention. Individuals may file a request under 10 CFR 2.206 to institute a proceeding pursuant to 10 CFR Section 2.202, Orders, to modify, suspend, or revoke a license, or for any other action as may be proper. NRC has not issued orders in response to any of the 38 10 CFR 2.206 petitions filed from FY 2013 through FY 2016. The audit objective was to determine whether NRC staff followed agency guidance

consistently in reviewing 10 CFR 2.206 petitions, and took steps to ensure appropriate information supports NRC decisions on 10 CFR 2.206 petitions. The report makes two recommendations to develop controls to ensure formal assessments are performed and are documented for future use, and clarify the criteria for reviewing and rejecting petitions.

- NRC issues certificates of compliance to approve the designs of (1) packages for transportation of radioactive material and (2) casks for spent fuel storage. Title 10 Code of Federal Regulations (10 CFR) Part 71 establishes the requirements for transportation of radioactive material package designs. 10 CFR Part 72 establishes the requirements for the issuance of certificates of compliance for spent fuel storage cask designs. The audit objective was to determine if NRC's processes for issuing certificates of compliance and reviewing 10 CFR Part 72.48 changes to licensee facilities, procedures or spent fuel storage casks provide adequate protection for public health, safety, and the environment. The report makes four recommendations to improve NRC's oversight for issuing certificates of compliance for radioactive material packages.

- Contract administration involves activities performed by agency officials after they award a contract. Contracting Officers (CO) administer NRC contracts and delegate specific contract administration responsibilities and technical supervision tasks to Contracting Officer's Representatives (COR), who are responsible for daily administration and technical direction of contracts during the period of performance. At the end of FY 2016, NRC had 43 COs and 644 CORs. From October 1, 2014, through September 30, 2016, NRC awarded 69 new contracts totaling $351.8 million. The audit objective was to assess the effectiveness of NRC's contract administration process and compliance with Federal and agency regulations. The report makes three recommendations to improve the effectiveness of management of contractor invoices and supporting documentation and to strengthen adherence to contract closeout procedures by CORs.

- On November 16, 2016, at 4:45 a.m., NRC's Network Operations Center identified that access was lost to key information technology (IT) services, including availability to the network, remote access, Internet, email and servers (file, print, and applications). Although the network outage was isolated to NRC headquarters, NRC's regional offices were also affected because they could not access centralized headquarters IT resources. Because of the outage, NRC excused headquarters employees for the entire workday on November 17, 2016, and for 2 hours on November 18, 2016, costing NRC an estimated $941,739 to grant employees administrative leave for this time. The Information Technology and Infrastructure Support Services (ITISS) contract provides NRC's IT services. The Global Infrastructure Development and Acquisition (GLINDA) contract will be the successor to ITISS beginning in early 2018. The objective was to evaluate the NRC network storage service interruption that occurred on November 16, 2016, and identify opportunities for improvement and solutions moving forward. This report makes four recommendations to improve NRC's processes, procedures, and operations under GLINDA.

- NRC's headquarters office Program Management, Policy Development and Analysis Divisions (PMDA) and regional office Divisions of Resource Management and Administration (DRMA) manage service delivery in corporate support areas. NRC has been proactive in identifying areas in which scarce program resources could be spent in the most economical and effective manner through external independent assessments. In addition, NRC established a Mission Support Task Force to identify opportunities to better optimize the expenditure of agency resources allotted to these programs. The audit objective was to determine if the activities performed by NRC's PMDA and DRMA programs produce the intended results from their operational processes in a manner that optimizes the expenditure of agency resources. The report makes one recommendation to optimize the use of resources and improve standardization and centralization throughout the agency.

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Adoption of cloud computing became Federal policy in 2010. A significant IT services contracting effort is underway at NRC, and several cloud applications have been recently deployed. The agency also is obtaining technical support for future cloud planning, acquisitions, and deployment. The audit objective was to assess whether NRC's adoption of cloud computing is adequately managed. The report makes two recommendations to develop guidelines to ensure that cloud services acquisitions rely on thorough project planning, and to train NRC information technology and acquisitions staff to manage new models of service delivery.

- From June 1, 2015, through May 31, 2016, NRC purchase card cardholders have spent approximately $3.5 million. The Government Charge Card Abuse Prevention Act of 2012 requires NRC to establish and maintain safeguards and internal controls for Government charge cards. It also requires OIG to conduct periodic risk assessments of the agency purchase card program to analyze the risks of illegal, improper, or erroneous purchases. The audit objective was to determine whether internal controls are in place and operating effectively to maintain compliance with applicable purchase card laws, regulations, and NRC policies. The report makes seven recommendations to improve the operational effectiveness of internal controls in the areas of documentation and program oversight.

- The *Federal Information Security Modernization Act of 2014* (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. OIG conducted an independent evaluation of NRC's implementation of FISMA 2014 at NRC's four regional offices and Technical Training Center and evaluated the effectiveness of agency information security policies, procedures, and practices as implemented in these locations. The reports made seven recommendations to strengthen information security.

- The Improper Payment Elimination and Recovery Act (IPERA), which amended the Improper Payments Information Act (IPIA), requires Federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. 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. The Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) established the Do Not Pay Initiative, which directs agencies to verify the eligibility 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 or Agency 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. The report made one recommendation to evaluate questioned costs identified under two NRC contracts.

- NRC participates in American Society of Mechanical Engineers (ASME) code committees as part of NRC's responsibilities under the National Technology Transfer Act of 1995. ASME is a non-profit professional organization that develops technical codes for the public and private sectors and includes a range of public and private sector employees. ASME codes are used in connection with technical standards for design, construction, and maintenance for commercial nuclear power plants. The audit objective was to assess NRC's oversight and compliance with applicable law, regulation, and policy relating to NRC employee participation in ASME code committees. The report made two recommendations to enhance oversight of NRC staff participation in ASME code committee activities.

- On March 22, 1975, a fire at the Browns Ferry nuclear power plant fundamentally changed how NRC addressed fire protection at nuclear power plants and shaped NRC's fire protection regulatory framework. Prior to the fire, NRC fire protection regulatory requirements were promulgated through General Design Criteria, Criterion 3, Fire Protection. Accordingly, all nuclear power plant licensees committed to plans outlining each plant's fire protection program, installed fire protection systems, and provided means to assure plants could shut down safely in the event of a fire. The audit objective was to assess the consistency of NRC's oversight of fire protection programs at operating nuclear power plants. The audit report makes recommendations to identify and implement best practices to enhance NRC's ability to apply appropriate regulatory requirements, licensing basis, and guidance documents to individual plants, and improve communication and knowledge transfer to benefit future inspections.

Defense Nuclear Facilities Safety Board Audits

- The Telework Enhancement Act of 2010 requires the head of each executive agency to establish and implement a policy under which employees shall be authorized to telework. The law defines telework as a work flexibility arrangement under which an employee performs the duties and responsibilities of his or her position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. The audit objectives were to determine (1) if DNFSB's telework program complies with applicable laws and regulations, and (2) the adequacy of internal controls over the program. The audit report makes three recommendations designed to strengthen DNFSB's telework program.

- DNFSB's enabling legislation authorizes it to assign staff to be stationed at any DOE defense nuclear facility to carry out the functions of the agency. DNFSB has used this authority to implement a Resident Inspector Program that serves a vital function in the agency's safety oversight of DOE's defense nuclear facilities. Employees in the program relocate to a DOE site with defense nuclear facilities and perform direct oversight of the safety of operations. At this time, there are 10 total resident inspectors, with 2 stationed at 5 DOE sites. The audit objective was to determine whether the Resident Inspector Program provides for the necessary onsite oversight of DOE defense nuclear facilities to adequately fulfill DNFSB's mission. The report made two recommendations to improve DNFSB's ability to develop and prepare candidates for the resident inspector position and increase agency transparency when determining which defense nuclear sites will have resident inspectors, along with the staffing of those sites.

NRC Investigations

- OIG conducted proactive investigations to evaluate the adequacy of two NRC Component Design Bases Inspections (CDBI), which are conducted to verify that nuclear power plant components are maintained within their design basis and monitor the capability of selected components and operator actions to perform their design bases functions. In March 2013—3 months after NRC conducted a CDBI at the St. Lucie nuclear power plant—a main stream isolation valve failed and caused a plant shutdown. In January 2015—7 months after NRC conducted a CDBI at the Pilgrim nuclear power plant—a safety relief valve failed to open upon operator demand during mitigation efforts related to a Loss of Offsite Power event affecting the plant.

- OIG conducted an investigation into an allegation that an NRC senior official harassed and retaliated against an employee for raising a safety concern by preventing the employee from completing the NRC Resident Inspector Development Program to become a resident inspector.

- OIG conducted an investigation into an allegation that an NRC senior official and two other employees made inappropriate verbal comments to licensee personnel during an informal review process pertaining to a senior reactor operator licensing examination at a nuclear power plant.

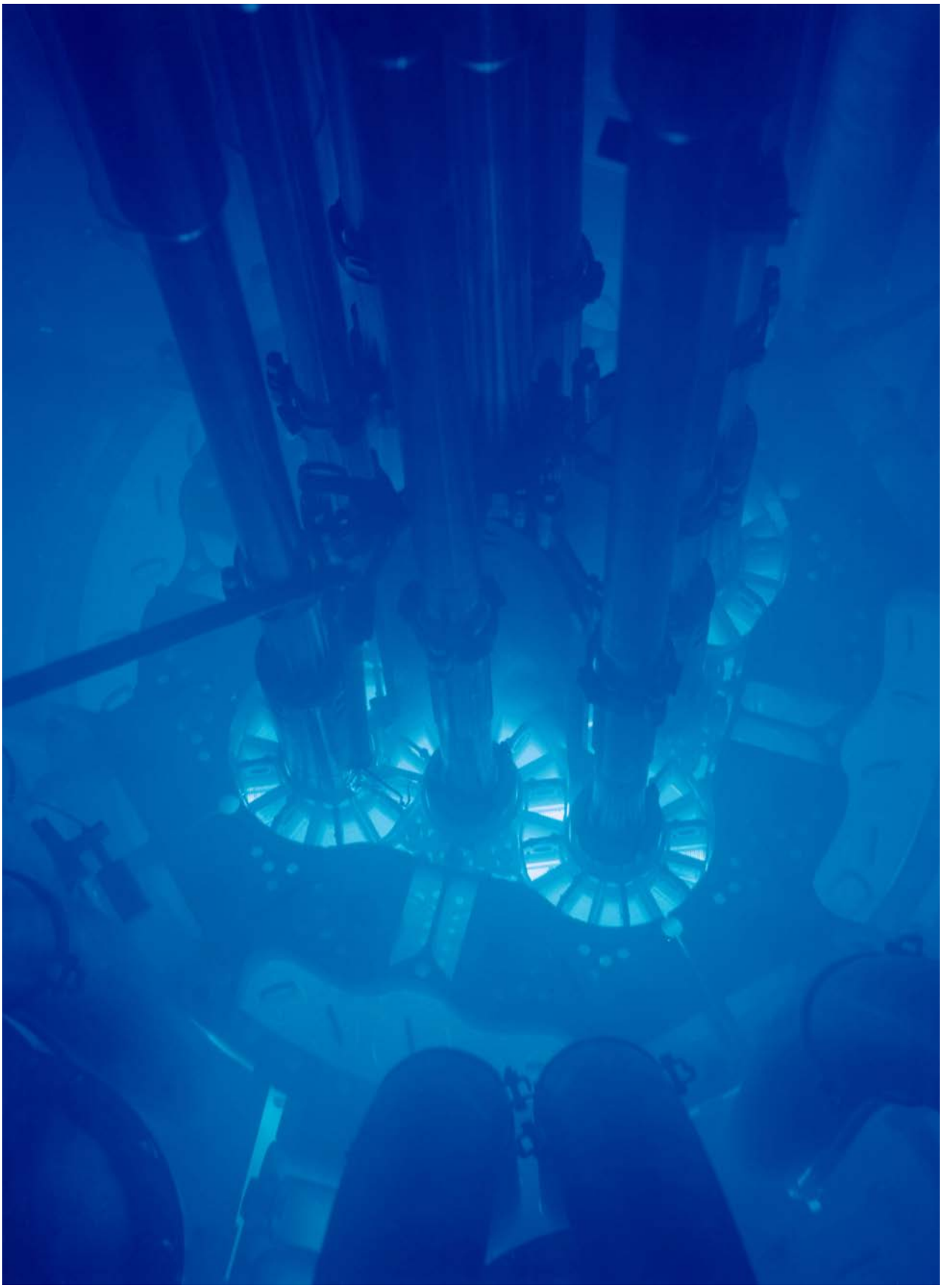
- OIG conducted an investigation into an allegation that an NRC senior official and another employee were running a charitable organization at NRC during official work hours. The NRC employees allegedly sent charity related emails using their NRC email accounts and some of these emails included language that directly or indirectly solicited donations for the organization.

- OIG conducted an investigation into an allegation that a former NRC employee had mishandled licensee proprietary information by taking the information out of the agency when the employee retired from Federal service and later transmitting the information back to NRC.

- OIG conducted an investigation into an allegation that during an NRC inspection meeting, an NRC senior official was limiting the scope of an inspection by informing licensee managers that the plant would receive only a certain number of inspection action items and that the NRC senior official had engaged in misconduct by striking an NRC licensee manager.

- OIG conducted an investigation into an allegation that NRC senior officials within a certain office were abusing their power by participating in off-site NRC inspections for the purpose of attaining frequent flyer miles and hotel points. In addition, according to the allegation, there was a "chilled work environment" within that NRC office and if an individual voiced a concern regarding unfairness or favoritism, that individual would be deliberately taken off an inspection and restricted from traveling

Fire equipment inspection at Calvert Cliffs nuclear power plant.



Nuclear reactor core.

OVERVIEW OF NRC AND OIG

NRC's Mission

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

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

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

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

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

OIG History, Mission, and Goals

OIG History

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

In response, Congress passed the landmark legislation known as the *Inspector General 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.

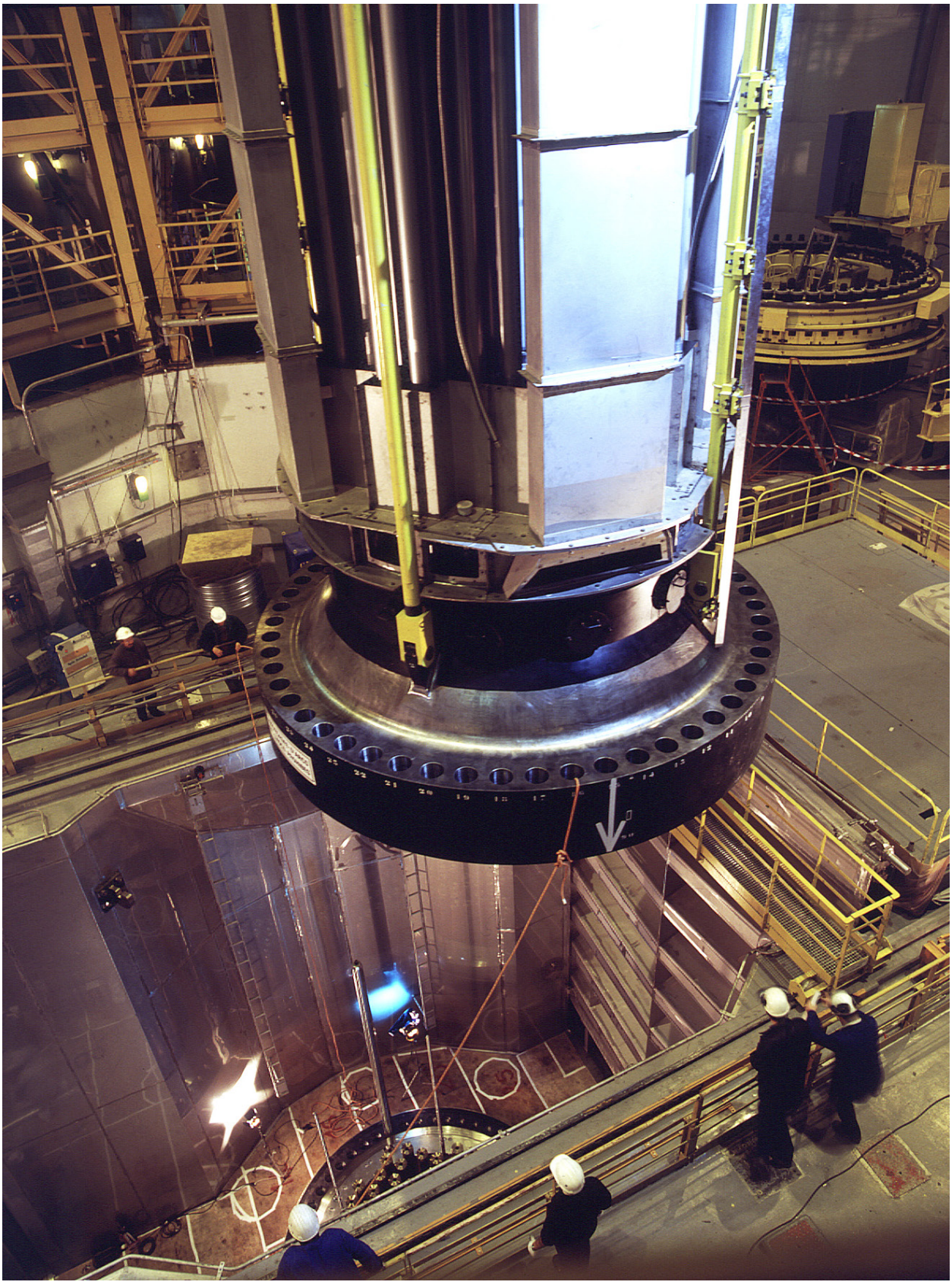
OIG is committed to ensuring the integrity of NRC programs and operations. Developing an effective planning strategy is a critical aspect of accomplishing this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, OIG developed a *Strategic Plan*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



Reactor core containment.

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 (MD), and makes recommendations to the agency concerning their impact on the economy and efficiency of agency programs and operations.

Regulatory review is intended to provide assistance and guidance to the agency prior to the concurrence process so as to avoid formal implementation of potentially flawed documents. 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, 2017 to September 30, 2017, OIG reviewed a variety of NRC and DNFSB documents including Commission papers (SECYs), Staff Requirements Memoranda, *Federal Register* Notices, Management Directives, Operating Procedures and statutes.

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

- Draft Management Directive and Handbook (MD) 12.5, NRC *Cybersecurity Progra*m. OIG stated that consistent with the independence provisions of the Inspector General Act, OIGis exempt from oversight by the Chief Information Officer. Further, that the MD did not appear to comply with Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

  OIG also noted that the following items addressed in the MD did not relate to cybersecurity and appeared to be outside the scope of the management directive: (1) Serves a significant role in planning, programming, and budgeting, has input to reporting requirements, management, governance, and oversight processes related to IT, (2) Approves the IT budget request for the agency and certifies that IT investments implement incremental development, as defined in capital planning guidance issued by OMB, (3) Approves all contracts or other agreements for IT or IT services, and (4) Approves all reprogramming of any funds made available for IT programs.

  Additional OIG comments suggested inclusion of the following references: Executive Order, EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," dated May 11, 2017, and Office of Management and Budget (OMB) documents M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, dated May 19, 2017.

- Draft MD 8.7, *Reactor Operating Experience Program*. OIG comments focused on the responsibilities descriptions for the Directors of the Offices of New Reactors and Nuclear Security and Incident Response suggesting that it would be appropriate to include the same statement in the section on the Director of Nuclear Reactor Regulation responsibilities as that for NSIR. OIG also suggested inclusion of additional definitions to explain the scope of industries intended to be within the scope of the MD.
- Draft MD 13.2, *Facility Management*. OIG comments focused on the need for additional clarification or standardization. Regarding the terms "NRC-controlled real property," "facilities occupied by NRC," "NRC-occupied facilities", and "NRC-occupied buildings," and whether these terms are to be used interchangeably.
- Draft MD 10.103, *Reduction in Force for Non-SES Employees*. OIG comments identified the need for clarification of terms including "Alternative actions" and "occupational level" and the provision of examples of multiple rating patterns and modal ratings as well as a sample Retention Register.

Other OIG Activities

Support of the Inspector General Community in Training

On April 6, 2017, Maryann Grodin, NRC OIG General Counsel, and Nancy Eyl, Assistant General Counsel to the Appalachian Regional Commission, addressed the Federal Audit Executive Council on the recently enacted Inspector General Empowerment Act. The presentation related the legislative history of the act, as well as relevant executive branch policy actions which lead to the extensive statutory revisions reflected in the act and primarily focused on the Acts numerous mandates. This interactive lecture also discussed broad and specific direction to IGs, and the agencies within which they function on expanded access, as well as required disclosures. Also enumerated were newly identified investigative and audit actions; and increased reporting authority and responsibilities.

The Council of Counsels to Inspectors General, a group of attorneys who serve as legal advisors in the Federal Inspector General community, sponsors a training program for law students working as summer interns in IG offices in the Washington, D.C., area. As part of the introductory session for this year's program, the NRC OIG General Counsel and the Assistant General Counsel to the Appalachian Regional Commission, provided a presentation for this program relating the concept and history of the Inspector General in the Federal Government. Topics discussed included the Inspector General Act and its statutory history and amendments, including the recently enacted IG Empowerment Act. The presentation conveyed the political and philosophical context of IG legal authority, and illustrated these concepts with examples from the IG community.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission* as of October 1, 2016 *(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-17-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC, http://www.nrc.gov/docs/ML16277A394.pdf*

NRC AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed nine financial and performance audits and evaluations, resulting in numerous recommendations to NRC management. These audits and evaluations are summarized below.

Audit Summaries

Evaluation of NRC's Management of Government Cell Phones

OIG Strategic Goal: Security and Corporate Management

In April 2016, NRC stopped leasing Government cell phones and entered into a contract with AT&T Mobility to purchase Android and iOS devices for up to 350 users. Currently 28 NRC property custodians are assigned responsibility for managing cellphones in the Space and Property Management System (SPMS), which is the official database used to track NRC property inventory assigned to various offices throughout the agency.

The Office of Administration (ADM) manages SPMS, and the Office of the Chief Information Officer (OCIO) plans and oversees the implementation of an Information Technology Security Program that enables access to agency resources from agency issued mobile devices such as smartphones. OCIO uses an application called MaaS360 to administer, manage, control and monitor smartphone activity and date usage. At the time of the evaluation, there were 347 users and 412 Government cell phones acquired from the mobility contract.

The objective was to evaluate whether NRC's Government furnished cell phones are sufficiently managed to provide information security.

Evaluation Results:

OIG did not identify weaknesses relative to Government furnished cell phone information security. However, the evaluation identified weaknesses in the management of Government furnished cell phones in the following areas:

Guidance and Training

Many of NRC's property custodians are unfamiliar with the process by which NRC's Government furnished cell phones are assigned and returned, or how to handle lost or stolen phones. Although Federal agencies are responsible for giving their employees the information and guidance they need to do their jobs, NRC guidance on cell phone management is inconsistent, and the agency does not consistently provide property custodians with guidance or training on cell phone management. Without properly training or instructing property custodians on how to handle cell phones, there is an increased risk that phones will be lost without NRC's awareness. Additionally, there is risk that end users will be provided with incorrect information about what to do if phones are lost or how to return phones when they are no longer needed.

Cell Phone Recordkeeping

NRC's Government furnished cell phone recordkeeping is inaccurate and inconsistent. NRC offices use one method for tracking inventory of Government furnished cell phones and a separate method for monitoring and management of smartphones. Without reconciling NRC's Government furnished cell phone records, there is a risk of improperly accounting for devices.

Rules of Behavior

Prudent business practices stress the importance of users periodically reviewing policies and procedures; however, NRC users are required to review the rules of behavior for all mobile devices only one time, which is the first time they are issued such an item. As a result, users may not be familiar with the rules of behavior, which could lead to misuse.

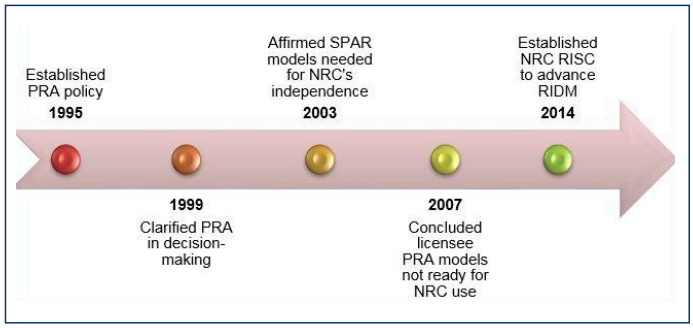
(Addresses Management and Performance Challenges #4 and #6)

Evaluation of Proposed NRC Modifications to the Probabilistic Risk Assessment Process

OIG Strategic Goal: Safety

NRC and its licensees use the Probabilistic Risk Assessment (PRA) process to estimate the risk of potential accidents at nuclear power plants. PRA is a structured, analytical process for identifying potential weaknesses and strengths of plant designs and operations in an integrated fashion. PRA considers accident scenarios to determine what can go wrong, the likelihood of occurrence, and the consequences for people and the plant.

NRC PRA Policy Developments



Source: OIG analysis based NRC data.

NRC's system for assessing risks of potential accidents at nuclear power plants is conducted using the Standardized Plant Analysis Risk (SPAR) model software program. NRC uses SPAR models to evaluate potential weaknesses and strengths of plant designs for each of the operating nuclear power reactors NRC regulates. SPAR models simulate accident sequence progression, plant systems and components, and plant operator actions.

The Three Mile Island accident in 1979 substantially changed the character of the analysis of severe accidents worldwide, and led to NRC establishing policy on the use of PRA methods.

An Office of Nuclear Reactor Regulation Risk Informed Steering Committee (RISC) evaluation team evaluated the potential for using licensee PRA models. The NRC RISC directed this effort because of concern about the annual cost of maintaining SPAR models. During the period January 2016 through July 2016, NRR staff led the

effort to evaluate the three following alternatives: (1) use licensee PRA models, which includes purchasing licensee software, (2) use licensee PRA results, and (3) continue using NRC SPAR models.

The NRC directed staff to stop evaluating the option of using licensee PRA results based on concerns that this option would compromise NRC's regulatory independence. Based on the preliminary cost benefit analysis and lack of industry interest, the NRC RISC decided that staff evaluation of the use of licensee PRA models in lieu of SPAR models for operations reactors should be terminated.

The evaluation objective was to assess NRC's process for piloting alternative risk modeling techniques including analyzing costs, benefits, and feasibility of these alternatives.

Evaluation Results:

Improved coordination and documentation of staff assessments would better support NRC's efforts to evaluate the costs, benefits, and feasibility of alternatives to its current risk modeling program (SPAR), such as using industry models. Although preliminary staff assessments show credible cost and feasibility limitations to adopting industry risk models, NRC has yet to document the results of this work and use it as the basis for a formal policy position. These actions are particularly important in the current regulatory climate, which emphasizes risk-informed decisionmaking. Moreover, better process management can help NRC more efficiently revisit SPAR alternatives if new cost data and feasibility solutions become available.

NRC's potential use of licensee PRA models as a regulatory tool could be a recurring matter of stakeholder interest in the coming years. Notably, the U.S. Senate Committee on Environment and Public Works asked NRC in December 2016 to describe the potential for using licensee PRA models and the agency actions (taken or planned) to address this potential opportunity. The Committee also requested periodic updates from NRC on PRA and other regulatory activities. Additionally, industry has also recently expressed interest in NRC's use of licensee PRA models.

The absence of a formal agency position explaining the reason NRC does not use licensee PRA models leaves the agency open to repeating previously completed data gathering and analysis. NRC would benefit from having an updated, formally documented, and verified evaluation so that, if the issue of using licensee PRA models arises again, there will be a readily accessible accurate, formal agency position on the subject.

(Addresses Management and Performance Challenge #1)

Evaluation of NRC's Management of Electronic Records

OIG Strategic Goal: Security and Corporate Management

On June 8, 2017, the Senate Committee on Homeland Security and Governmental Affairs asked OIG to review NRC's processes and compliance with applicable legal standards for preserving certain electronic records as federal records, and cooperation with Congressional document requests, since January 20, 2017. The Committee requested that NRC OIG provide responses to six specific questions. OIG evaluated the electronic records management in conjunction with its response to the committee's letter.

Evaluation Results:

NRC's records management provides effective information access by improving the completeness and accuracy of NRC records and information. Implementation of information and records management strategies allows timely and accurate capture, use, storage, and disposition of information, enabling NRC staff and stakeholders to access the information they need.

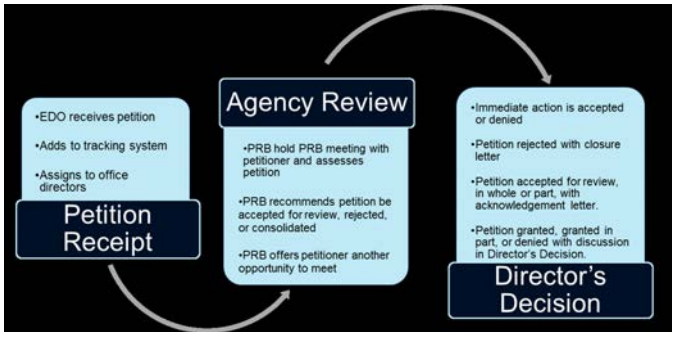
NRC has responded both to emerging technologies and to the requirements to preserve electronic records by establishing and revising policies and supporting implementation by all staff and senior leaders. The program relies on informed and motivated staff to achieve its goals. The agency must not only ensure that NRC information is secure as new technologies become available for records creation. NRC must also continue to be proactive to ensure that all agency staff use the available tools to comply with Federal mandates to manage the electronic records that document agency business.

(Addresses Management and Performance Challenges #4 and #6)

Audit of NRC's 10 CFR 2.206 Petition Review Process

OIG Strategic Goal: Safety

10 CFR 2.206 Petition Process



Source: OIG generated based on agency information.

NRC encourages members of the public to use Title 10, Code of Federal Regulations, Section 2.206, *Requests for Action Under This Subpart* (10 CFR 2.206), as one method to bring issues to the agency's attention. Any person may file a request by using 10 CFR 2.206 to institute a proceeding pursuant to 10 CFR Section 2.202 *Orders*, (10 CFR 2.202) to modify, suspend, or revoke a license, or for any other action as may be proper.

NRC's MD 8.11, *Review Process for 10 CFR 2.206 Petitions*, establishes procedures and timelines for the 10 CFR 2.206 review process, including roles and responsibilities. The Office of Nuclear Reactor Regulation, Division of Operating

Reactor Licensing, Special Projects and Process Branch oversees the 10 CFR 2.206 petition review process. The Executive Director for Operations assigns office directors petitions to review. Office directors and a petition manager establish Petition Review Boards (PRB) made up of cognizant management and staff and designate a chair for each Board. The PRB chair is responsible for ensuring appropriate review of all 10 CFR 2.206 petitions, and providing guidance for timely resolution of petitions. PRBs recommend to office directors whether petitions should be accepted for review, rejected, or consolidated.

Office directors are responsible for issuing a final Director's Decision and dispositioning the petition, which the Commission has an opportunity to review. NRC publishes *Federal Register* notices for petitions that meet the criteria for review and final Director's Decisions. NRC also publishes a status report of petitions under review and final Director's Decisions on completed petitions on NRC's public Web site.

NRC has not issued orders in response to any of the thirty-eight 10 CFR 2.206 petitions filed from FY 2013 through FY 2016. The lack of such actions could adversely affect the public's perspective on the effectiveness of the agency's 10 CFR 2.206 petition process.

The audit objective was to determine whether NRC staff follow agency guidance consistently in reviewing 10 CFR 2.206 petition, and take steps to ensure appropriate information supports NRC decisions on 10 CFR 2.206 petitions.

Audit Results:

Staff follow guidance for reviewing 10 CFR 2.206 petitions and providing supporting documentation for decisions. However, opportunities exist for NRC to improve consistency and increase public confidence in the agency's 10 CFR 2.206 petition process by ensuring (1) periodic assessments of the 10 CFR 2.206 petition process are performed, and (2) petition review and rejection criteria are clear.

Periodic Assessments of Process

NRC committed to periodically assess the 10 CFR 2.206 petition process to enhance its effectiveness, timeliness and credibility. However, NRC did not perform periodic assessments because it has not established management controls to ensure periodic assessments of the 10 CFR 2.206 petition process are performed.

Because NRC has not performed periodic assessments of the 10 CFR 2.206 petition process, NRC missed opportunities to enhance effectiveness, timeliness, and credibility of the process.

For example, NRC does not have a complete view of total time spent reviewing 10 CFR 2.206 petitions. Some staff expressed concern that too much time is required to complete administrative work such as setting up the PRB and public meetings. Staff and managers noted as petitions range in complexity, the amount of time spent reviewing petition varies. Some NRC staff explained that they spent more than 150 hours reviewing a single petition. Periodic assessments could have helped NRC better identify how resources are used and make informed decisions about resource allocation.

In addition, periodic assessments could have helped NRC establish more realistic

timeliness metrics for 10 CFR 2.206 petition reviews. During the audit, NRC staff informed OIG that MD 8.11 was undergoing a revision. Process changes resulting from this guidance revision without the benefit of periodic assessments might not achieve intended outcomes.

Petition Review and Rejection Criteria

Agency positions should be readily understood and easily applied. NRC staff have difficulty applying 10 CFR 2.206 petition review and rejection criteria because the criteria are not clear.

Staff difficulty applying 10 CFR 2.206 petition review and rejection criteria could result in accepting petitions that should be rejected and rejecting petitions that should be accepted. Additionally, some petitioners complained that the petition review and rejection process is inconsistent and biased against petitioners. Inconsistent and improper application of criteria could adversely affect public's opinion of NRC's regulatory consistency.

(Addresses Management and Performance Challenge #1)

Audit of NRC's Oversight for Issuing Certificates of Compliance for Radioactive Material Packages

OIG Strategic Goal: Safety

NRC issues certificates of compliance to approve the design of a (1) package for transportation of radioactive material or (2) cask for spent fuel storage. A transportation package includes the assembly of components necessary to ensure compliance with packaging requirements and the radioactive contents as presented for transport. A storage cask is a heavily shielded container, often made of lead, concrete, or steel, used for the dry storage of radioactive material.

The person or vendor who has been issued a certificate of compliance by NRC is called a certificate holder. A certificate holder or potential certificate holder is responsible for applying to NRC for approval of a new design, a revision or amendment to an existing design, or a renewal for an expiring certificate of compliance. Vendors with approved designs sell and lease packages or casks to NRC licensees authorized to use NRC approved packages or casks. These licensees are called certificate users.

The Office of Nuclear Material Safety and Safeguards (NMSS) is responsible for regulating activities to provide for the safe transportation of radioactive material packages and the safe storage and transportation of spent nuclear fuel. NMSS' Division of Spent Fuel Management (DSFM) within NMSS is responsible for reviewing and issuing certificates of compliance, and handling the regulatory, licensing, and inspection programs related to the transportation of radioactive material packages and the storage of spent nuclear fuel.

Title 10 Code of Federal Regulations Part 71 (Part 71) establishes the requirements for the transportation of radioactive material packages that apply to any holder or applicant for a transportation certificate of compliance. DSFM issues transportation certificates of compliance for a period of 5 years. 10 CFR Part 72 establishes the requirements for the issuance of certificates of compliance for spent fuel storage cask designs. DSFM issues storage certificates of compliance for a term not to exceed 40 years.

From October 2012 through February 2017, DSFM reviewed 227 applications under Part 71, divided into 3 types of reviews. There were 15 new cases, 71 renewal cases, and 141 amendments reviewed.

The audit objective was to determine if NRC's processes for issuing certificates of compliance and reviewing 10 CFR Part 72.48 changes provide adequate protection for public health, safety, and the environment.

Audit Results:

OIG found that NRC processes for issuing certificates of compliance are adequate; however, opportunities for improvement exist within NRC's internal processes. Specifically, NRC should (1) determine and provide the basis for an appropriate term for Part 71 certificates of compliance and (2) establish sufficient controls for Part 72.48 reviews.

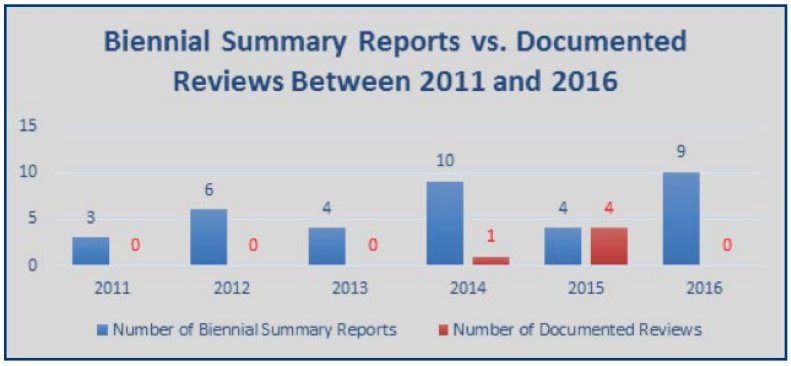
Part 71 Certificates of Compliance

Regarding the term for Part 71 (transportation) certificates of compliance, the agency is relying on a practice used by staff for years instead of a formal determination. NRC should regulate in a manner that clearly communicates requirements and ensures that regulations incorporate an assessment of safety significance or relative risk. However, NRC does not have documented regulatory and technical bases to support the aforementioned 5-year term. As a result, the agency is imposing a regulatory requirement without clearly assessing the importance to safety or the potential burden imposed on NRC staff and the certificate holders. NRC should regulate in a manner that clearly communicates requirements and ensures that regulations incorporate an assessment of safety significance or relative risk.

Part 72.48 Reviews

NRC staff are not following internal NRC procedural guidance for conducting Part 72.48 reviews. NRC management and staff are responsible for providing and following effective procedures to ensure implementation of agency policies. NMSS' primary guidance for Part 72 review—*Office Instruction-18*, *Part 72 Review Guidance*—states that project managers are expected to review, document, and communicate their review of 10 CFR 72.48 biennial summary reports within 30 days of receipt from the certificate holder. However, staff are not following agency guidance related to Part 72.48 procedures.

OIG staff searched ADAMS and located 36 certificate holder biennial summary reports submitted between 2011 and 2016. Of the 36 biennial summary reports submitted to NRC, only 5 reviews were documented and completed by NRC. None of the 5 completed reviews were placed in ADAMS within 30 days of completion as stipulated in *Office Instruction-18*. The audit team found the reviews were documented and placed in ADAMS an average of 2.5 years after the biennial summary reports were received.



NRC staff are not adhering to Part 72.48 procedures because there are insufficient internal controls to ensure consistent implementation of office policies. As a result, NRC may not detect Part 72.48 changes that should have been submitted as amendment requests.

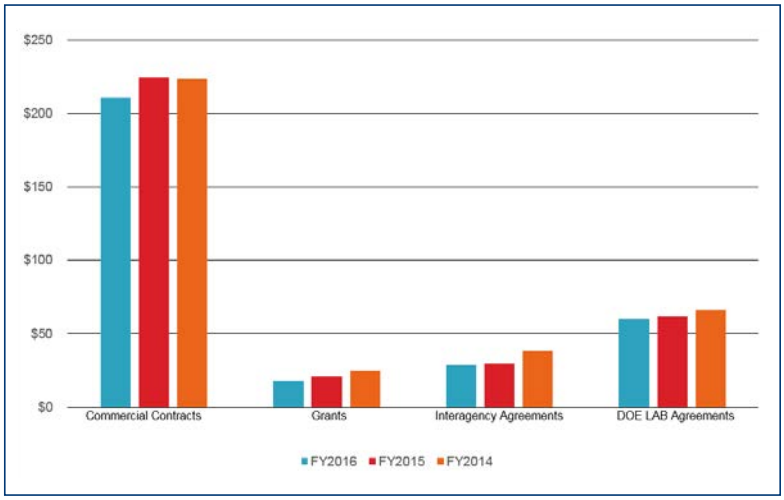
(Addresses Management and Performance Challenge #2)

Audit of NRC's Contract Administration Process

OIG Strategic Goal: Corporate Management

Contract administration involves those activities performed by agency officials after they award a contract. Contracting Officers (COs) administer NRC contracts. However, COs delegate specific contract administration responsibilities and technical supervision tasks to a Contracting Officer's Representative (COR). CORs are responsible for daily administration and technical direction of contracts during the period of performance. CORs review and reconcile invoices including verifying support for payment and collection. The COR is expected to maintain working contract files.

Fiscal Year 2016 Open Contract Obligations (in $ millions)



Contract administration is a key activity driver of NRC's strategic goals in increasing the economy, efficiency, and effectiveness of stewardship of government resources. At the end of FY 2016, NRC had 43 COs and 644 CORs. From October 1, 2014 through September 30, 2016, NRC awarded 69 new contracts totaling $351.8 million.

The audit objective was to assess the effectiveness of NRC's contract administration process and compliance with Federal and agency regulations. OIG retained RMA Associates, LLC, to conduct this performance audit

Audit Results:

The NRC process for contract administration generally complies with applicable laws, regulations, and policies. However, management oversight of the contract administration process should be improved in the following areas: (1) record retention for invoices and related supporting documentation should be improved, and (2) contract closeout initiation controls need strengthening.

Record Retention

NRC COs and CORs do not consistently record or archive contractual accounting records and supporting documentation within a centralized repository. Auditors sampled 2 contracts from a previous period along with 15 contracts during the period of FY15 through FY16 that obligated over $2.1 million to assess whether contract administration controls and compliance requirements were satisfied. Based on the contracts from FY15 through FY16, the following inconsistencies were found:

- NRC's CORs maintain invoices and supporting documentation at different locations. When there is a change in COR, invoices and supporting documentation maintained by the previous COR are not always given to the new COR.

- Of the 15 contracts reviewed for FY15 through FY16, six had insufficient, inadequate, or no documentation to support that proper, valid, and reasonable payments were made within the terms of the contract. For each of the 6 contracts, the current COR did not receive one or more types of documentation such as contractor receipts, logs and timesheets and the records could not be located for this audit.

Lack of supporting contract expense documentation within a central repository increases the likelihood of undetected contract fraud, waste, and abuse.

Contract Closeout

Contract closeouts are not being initiated in a timely manner. Auditors sampled 2 contracts from a previous period along with 15 contracts selected from the 69 contracts administered during the period of FY15 through FY16. Of those 15, 5 should have entered the closeout process. The performance period for these contract closeout samples had expired. However, the closeout initiation for one contract was incomplete and CORs had not initiated requests for closeout within the requisite 90 days for the other four. For two of those four contracts, initiation of closeout was more than 6 months behind schedule.

Contracts closeouts are not being initiated timely because NRC lacks prescriptive procedures for the COR to follow regarding final invoice submission. Implementing control procedures to strengthen adherence to contract closeout procedures will enable CORs to start closeout initiation procedures timely. According to NRC's Office of the Chief Financial Officer (OCFO), unliquidated obligations for commercial contracts from budget fiscal years 2007 through 2013 totaled approximately $3.5 million. Reducing unliquidated obligations increases funds the agency can use to support its mission.

(Addresses Management and Performance Challenge #6)

Evaluation of NRC's Network Storage Interruption

OIG Strategic Goal: Security

On November 16, 2016, at 4:45 a.m., the NRC's Network Operations Center identified that access was lost to key information technology (IT) services, including availability to the network, remote access, internet, email and servers (file, print, and applications). The network outage was isolated to NRC headquarters; however NRC's regional offices were also affected by the interruption. This resulted in NRC excusing headquarters employees for the entire workday on November 17, 2016, and for 2 hours on November 18, 2016. It cost NRC an estimated $941,739 to grant employees administrative leave for this time.

The Information Technology and Infrastructure Support Services (ITISS) contract provides NRC's IT services and is valued at more than $160 million as of June 2017. The ITISS contractor has one service provider—Dell Services Federal Government. The Global Infrastructure Development and Acquisition (GLINDA) contract will be the successor to ITISS beginning in September 2017.

The objective was to evaluate the NRC network storage service interruption that occurred on November 16, 2016, and identify opportunities for improvement and solutions moving forward.

Audit Results:

OIG evaluated the network storage interruption and its effect on agency operations, and identified opportunities for improvement in how NRC manages its IT services contract. OIG found weaknesses pertaining to the contract modification process, control of system architecture decisions, and the contract language and management.

Contract Modification Process

In 2015, NRC, without recognizing that it had done so, modified the ITISS contract disincentive fee from 5 percent to 2 percent. The modification occurred because of inadequate internal controls over contract modification. As a result, NRC will recover only $223,300 due to the network shutdown, when it could have recovered $558,266 had the disincentive fee remained unmodified. Improving internal controls over contract modification can prevent this type of error from occurring with other contracts, including the GLINDA acquisition.

Control of Storage System Architecture Decisions

NRC relinquished control of storage system architecture decisions to the contractor, contrary to the agency's guidance. NRC was not involved in the decisions because it lacked an office level policy requiring an evaluation of architecture to ensure it was meeting NRC's needs. Without such a policy in place, NRC may not be aware of the risks associated with the architecture selected by the contractor and the need to formulate a plan to mitigate those risks.

Contract Language and Oversight

OIG identified multiple issues with how the ITISS contract was written and overseen. These issues are related to the number and relative weight of the Service Level Requirements (SLR) included in the contract, and the lack of associated penalties.

Agency Lessons Learned Moving to GLINDA

NRC has learned from the ITISS contract experience. In the GLINDA acquisition, there will be a COR at the Blanket Purchase Agreement (BPA) level with CORs assigned to manage the BPA calls. This approach will allow more hands on monitoring and minimize failure, as long as the agency provides adequate guidance and support to those involved in managing the contract. The GLINDA acquisition will have standardized templates and appropriate breakdown of work for the CORs. Each COR at that BPA level will be delegated authority by the CO. However, none of this has been formalized into an overall contract governance plan. Additionally, NRC will also have an integrator who will be responsible for helping with the transition to the GLINDA acquisition, implementing the SLRs, and with processes and procedures. Given that the GLINDA acquisition will have multiple vendors, multiple CORs, and an integrator, it is imperative that NRC develop and implement a GLINDA acquisition governance plan.

(Addresses Management and Performance Challenge #4)

Audit of NRC's PMDA and DRMA Functions to Identify Program Efficiencies

OIG Strategic Goal: Corporate Management

Many NRC offices maintain corporate support through Program Management, Policy Development and Analysis (PMDA) Divisions or Divisions of Resource Management and Administration (DRMA). The PMDA function at NRC headquarters and the DRMA function at NRC regional offices manage service delivery in support areas. These organizations exist across NRC, and evolved to address individual office support needs depending on each office's specific mission and functions. They perform functions that are specific to their organization and common across all PMDA and DRMA supported offices.

For FY 2017, approximately 86 and 90 Full Time Equivalents (FTE) were dedicated to PMDA and DRMA activities respectively. Of the $181 million FY 2017 budget for the four regional offices, approximately $47 million or 26 percent, was for DRMA divisions. Also for FY 2017, of the $312.8 million headquarters program offices' budget, approximately $32.4 million or 10 percent was budgeted for PMDA divisions. NRC did not maintain this budget allocation information for PMDA and DRMA prior to FY 2017.

NRC is presently facing significant management and performance challenges such as tight and reduced budgets and realignment of program offices. To meet these program challenges, NRC must efficiently and effectively use its resources.

The audit objective was to determine if the activities performed by NRC's PMDA and DRMA programs produce the intended results from their operational processes in a manner that optimizes the expenditure of agency resources.

Audit Results:

NRC's PMDA and DRMA programs generally produce the intended results from their operational processes. NRC has been proactive in identifying areas in which scarce resources could be spent in the most economical and effective manner. For example, NRC established a Mission Support Task Force to identify opportunities to better optimize the expenditure of agency resources allotted to these programs.

However, agencywide policies and procedures pertaining to areas such as budget formulation are performed inconsistently. This occurred because NRC has not fully implemented all of the Mission Support Task Force Report recommendations designed to streamline and improve internal controls related to improving efficiency and effectiveness of PMDA and DRMA operations. While most of the Mission Support Task Force Report's 27 recommendations are scheduled to start during calendar year 2017, there are 2 recommendations that are not scheduled to start until calendar year 2018 and 1 not until calendar year 2019. As a result, NRC's internal controls may be compromised and policies and procedures may not be as effective and efficient as intended. Furthermore, there is increased potential for a wasting of resources, declining productivity and decreasing efficiency and effectiveness of NRC's administrative support operations.

(Addresses Management and Performance Challenge #6)

Audit of NRC's Adoption of Cloud Computing

OIG Strategic Goal: Security

Adoption of cloud computing became Federal policy in 2010. The policy prodded agencies to consolidate data centers, consider cloud services first in new acquisitions, use shared services, and adapt activities to new information technology (IT) service models. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources.

A significant IT services contracting effort is underway at NRC. Several cloud applications have been recently deployed. The agency also is obtaining technical support for future cloud planning, acquisitions, and deployment.

The audit objective was to assess whether NRC's adoption of cloud computing is adequately managed.

Audit Results:

NRC has not had a cohesive approach to cloud adoption. Federal and NRC guidance emphasize management's role in providing objectives, resources, and oversight for IT projects. However, until 2016, NRC management's focus on the agency's data centers substituted for an effective cloud strategy.

For example, NRC management committed to consolidating two older data centers into its new Three White Flint North data center. The decision was made without completing a cloud alternatives study that would have not only defined a basis for determining which options best met NRC's requirements, but also provided complete cost analysis of cloud and internal options.

The consolidation resulted in resources that are not scalable, rapidly provisioned, or shared. Further, it did not realize expected operating cost savings. Due to a lack of cost analysis in the beginning, it is not clear whether the project's modernization benefits were worth the additional cost, or whether the same benefits could have been achieved at a lower cost while also enabling the adoption of effective cloud solutions.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Purchase Card Program

OIG Strategic Goal: Corporate Management

NRC participates in the Governmentwide initiative of using purchase cards to pay for micro-purchases and acquisitions satisfying the Federal Strategic Sourcing Initiative. NRC instituted the purchase card program in 1994, with the issuance of the purchase card handbook.

The Government Charge Card Abuse Prevention Act of 2012 requires NRC to establish and maintain safeguards and internal controls for Government charge cards. It also requires OIG to conduct periodic risk assessments of the agency purchase card program to analyze the risks of illegal, improper, or erroneous purchases. OIG previously audited NRC's purchase card program in 2011, and issued *Audit of NRC's Purchase Card Program*, which identified opportunities for improvement in the areas of guidance, record keeping and oversight.

ADM is responsible for oversight of NRC's Purchase Card Program. ADM has a designated Agency Program Coordinator (APC) who is responsible for day-to-day program management. The APC provides oversight of the purchase card program and serves as the liaison between cardholders and Citibank. Additionally, OCFO has the responsibility of establishing the availability of funds, committing funds for the purchases of the Central Allowance Offices, and certifying the payment of the transaction to Citibank.

NRC's financial system, the Financial Accounting and Integrated Management Information System (FAIMIS), manages purchase card transactions. Cardholders and approving officials record the obligation and commitment for the purchase; attach supporting documentation; and reconcile, approve, and pay for the purchase in FAIMIS.

From June 1, 2015, through May 31, 2016, there were 4,120 purchase card transactions made by 77 NRC cardholders, who spent a total of approximately $3.5 million. Since the 2011, audit there was a substantial decrease in the number of cardholders from 160 to 77. Additionally, the average monthly purchases made under the purchase card program have decreased from approximately $519,000 to $292,000.

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

Audit Results:

Generally, NRC policies are in compliance with applicable purchase card laws and regulations. However, NRC internal controls are not always effective at maintaining compliance with Federal requirements and established NRC policies. The audit identified the need for improved controls relative to documentation and program oversight.

Regarding documentation, OIG found that cardholders do not consistently include supporting documentation in FAIMIS. Of the 286 sampled transactions reviewed during this audit, 163 contained incomplete or inadequate supporting documentation and the approving officials approved these transactions without reviewing the related supporting documentation in FAIMIS. The supporting documentation reviewed in FAIMIS and hardcopy were missing basic items on the purchase requisition such as management approval, funds approval, or adequate business justifications.

Regarding program oversight, the audit found opportunities for improvement related to the conduct of internal reviews of cardholder use, reconciliation of cardholder and approving official lists, and segregation of duties.

Purchase card internal control issues identified during this audit result in an increased risk for fraud, waste, and abuse of funds. By strengthening documentation of transactions in FAIMIS and improving oversight of the program, the agency will reduce risk and better safeguard its funds.

(Addresses Management and Performance Challenge #6)

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017 at NRC's Regional Offices and TTC

OIG Strategic Goal: Security

On December 18, 2014, the President signed the *Federal Information Security Modernization Act of 2014* (FISMA 2014), reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation must also include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's OIG or by an independent external auditor.

The NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for fiscal year (FY) 2017 at NRC's four regional offices and the Technical Training Center (TTC).

The objective was to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented in the respective locations.

Evaluation Results:

Region I, King of Prussia, PA—Region I's IT security program, including Region I IT security policies, procedures, and practices, is generally effective. However, a network vulnerability scan found vulnerabilities that require remediation.

Region II Atlanta, GA—Region II has continued to make improvements in its implementation of NRC's IT security program and practices for NRC IT systems since the previous evaluation in 2012. However, backups of Region II servers are not being performed.

Region III Lisle, IL—The Region III IT security program, including Region III IT security policies, procedures, and practices, is generally effective. However, an opportunity for improvement exists in regard to disseminating Region III procedures, notices, and divisional instructions.

Region IV Arlington, TX—The Region IV IT security program, including Region IV IT security policies, procedures, and practices, is generally effective. However, some regional policy guides are not up-to-date, Region IV backup procedures are incomplete and not up-to-date, and a network vulnerability scan found vulnerabilities that require remediation.

Technical Training Center Chattanooga, TN—The TTC IT security program, including TTC IT security policies, procedures, and practices, is generally effective. However, the TTC System Hardware and Software Inventory is incomplete and agency-managed laptops and standalone desktops are not authorized to operate in accordance with NRC policies, procedures, and processes

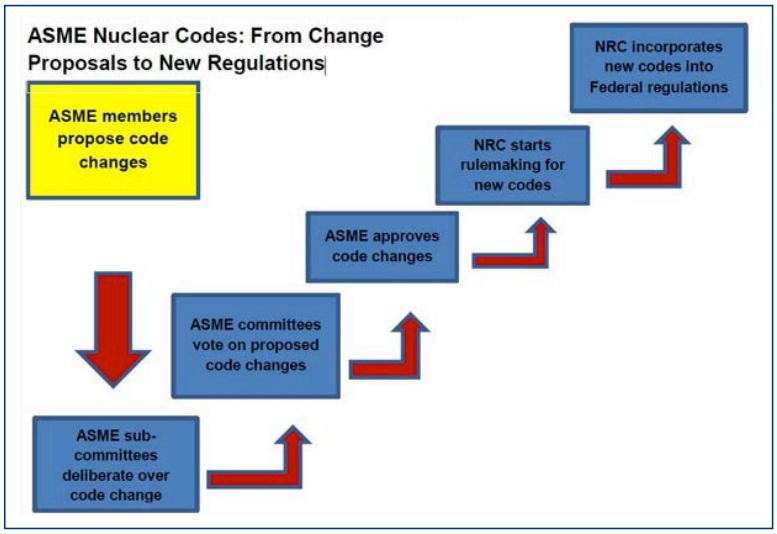
(Addresses Management and Performance Challenge #3)

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

OIG Strategic Goal: Safety

NRC participates in American Society of Mechanical Engineers (ASME) code committees as part of NRC's responsibilities under the National Technology Transfer Act of 1995. ASME is a non-profit professional organization that develops technical codes for the public and private sectors and includes a range of public and private sector employees. ASME codes are used in connection with technical standards for design, construction, and maintenance for commercial nuclear power plants.

ASME Code Development and Rulemaking Process



OIG analysis of ASME documentation and interviews with NRC staff.

NRC guidance for staff participation on ASME code committees is contained in NRC MD 6.5, *NRC Participation in Development and Use of Consensus Standards*. This guidance was recently updated October 28, 2016, and implementation of the changes is ongoing.

The ASME code development process begins when ASME committees are presented with proposed changes to ASME codes in 10 CFR 50.55a. The process ends either with a committee decision against making the changes, or a decision to incorporate the changes into ASME's code structure. If approved for publication by ASME, NRC may consider code changes for incorporation into the CFR through NRC's rulemaking process. ASME maintains official records of the ASME code development process in an online proprietary data system, which is accessible to the organization's members.

NRC's ASME code committee representatives interact with nuclear industry personnel during committee business, and must comply with Federal ethics laws and regulations, as well as NRC and ASME ethics policies. Additionally, the ASME

"balance of interest" policy aims to minimize conflicts of interest in technical or membership matters by preventing situations in which a single interest group could control action on a particular issue.

OIG undertook this work based on awareness of the potential lack of internal controls for managing committee participation in the areas of management oversight, monitoring, coordination, and guidance. OIG auditors also considered OIG Investigations' concerns regarding the potential for conflicts of interest with respect to NRC staff participation in ASME code committee meetings.

The audit objective was to assess NRC's oversight and compliance with applicable law, regulation, and policy relating to NRC employee participation in American Society of Mechanical Engineers Code Committees.

Audit Results:

NRC generally complies with applicable law, regulation, and policy pertaining to participation in ASME code committees. However, management oversight of staff participation could be improved by strengthening recordkeeping practices and internal controls for staff adherence to NRC ethics policies.

Recordkeeping Practices

Federal agencies are required to implement internal controls for effective information, communication, and monitoring. However, ASME code committee participation information is incomplete and staff use inconsistent methods for recording, communicating, and monitoring committee information. This has occurred because NRC has not yet finalized a plan for implementing recently revised guidance on NRC participation in standards organizations. Strengthened recordkeeping would support external reporting requirements, and enhance NRC's program management.

Conflict of Interest Controls

NRC ethics policy reflects Federal requirements for conflict of interest controls, such as training and financial disclosure reporting. However, most NRC staff representing the agency on ASME code committees do not file financial disclosure reports. This occurs because NRC policy governing ASME code committee participation does not include controls to verify staff compliance with conflict of interest policy. Financial disclosure reporting by ASME code committee representatives can help NRC better manage conflict of interest risk, and strengthen public confidence in the agency as a fair and impartial regulator.

(Addresses Management and Performance Challenge #6)

Audit of NRC's Fire Protection Oversight

OIG Strategic Goal: Safety

On March 22, 1975, a fire at the Browns Ferry nuclear power plant fundamentally changed how the Nuclear Regulatory Commission (NRC) addressed fire protection at nuclear power plants and shaped NRC's fire protection regulatory framework. Prior to the fire, NRC fire protection regulatory requirements were promulgated through General Design Criteria, Criterion 3, Fire Protection. Criterion 3 prescribed certain fire protection requirements associated with minimizing a fire's effect on equipment important to safety. Criterion 3 also required that fire protection systems should not impair equipment important to safety. Accordingly, all nuclear power plant licensees committed to plans outlining each plant's fire protection program, installed fire protection systems, and provided means to assure plants could shutdown safely in the event of a fire.

NRC staff at headquarters and regions oversee fire protection at operating nuclear power plants. NRC's Fire Protection Branch within the Office of Nuclear Reactor Regulation's Division of Risk Assessment performs safety evaluations associated with fire protection regulations, develops regulations and regulatory guidance, and supports application of the fire protection regulations at the regional level. Additionally, NRC inspectors provide oversight to plant fire protection programs through inspections.

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

Audit Results:

Opportunities exist for NRC to improve the consistency of fire protection oversight by ensuring (1) specific regulatory requirements for individual nuclear plants are clear to cognizant staff, and (2) documentation of inspection insights from discussions of issues that do not result in findings or violations.

Clarification of Regulatory Requirements

NRC staff have different views on licensee accountability to regulatory requirements because the applicability of specific regulatory requirements to individual plants is unclear. Fire protection regulatory requirements are made up of multiple safety evaluation reports, letters between NRC and licensees, and license amendments that reflect plant design changes that occur over time. NRC staff responsible for fire protection oversight have to determine which regulatory requirements apply to each individual plant based upon its unique and evolving licensing basis.

Differing views on the application of regulatory requirements could lead to inaccurate and inconsistent application of requirements and unreliable oversight. Additionally, staff time spent ascertaining which regulatory requirements apply to

specific plants can detract from time spent on direct inspection work. Together, these factors increase the risk of fire protection oversight lapses that could compromise plant safety. By clarifying applicability of various fire protection regulatory requirements for individual plants, NRC could strengthen safety oversight and promote public confidence in the agency's stated commitment to regulatory clarity, reliability, and efficiency.

Documentation of Inspection Issues

NRC is missing opportunities to capture inspection insights from fire protection inspection issues that do not result in findings or violations. Potential findings or violations identified by inspectors are sometimes resolved through discussions with licensees and NRC headquarters staff to clarify plant-specific requirements, and how conditions observed by inspectors relate to those requirements. NRC does not document inspection issues unless they pertain to findings or violations.

Because NRC does not document inspection issues unless they pertain to findings or violations, inspectors do not benefit from inspection insights that could enhance future fire protection inspections. Lacking such information, inspectors risk repeating work on issues that were resolved in previous inspections. During one triennial fire inspection observed by OIG, inspectors conceded they could spend several hours unnecessarily duplicating undocumented work from previous inspections, and contended that this happens routinely. Duplicative efforts detract from time and effort that could be spent more effectively addressing unexamined or unresolved safety issues. However, improved access to inspection insights could help future fire inspection teams plan and conduct their work more efficiently and effectively.

(Addresses Management and Performance Challenge #1)

Audits in Progress

Audit of NRC's Outreach and Consultation Practices with Federally-Recognized Native American Tribal Governments

OIG Strategic Goal: Safety

The United States has a unique relationship with Native American tribes as prescribed in the Constitution of the United States, treaties, and Federal statutes. As an individual regulatory agency, NRC recognizes that it has a "trust responsibility" to federally-recognized Native American tribes to adopt practices consistent with the fundamental principles contained in treaties, statutes, and executive orders. This special relationship requires Federal consultation with Native American tribes to be meaningful, in good faith, and entered into on a government-to-government basis.

The NRC staff has developed agencywide policy and guidance to ensure effective government-to-government interactions with Native American and Alaska Native Tribes and to encourage and facilitate Tribal involvement. It is NRC's expectation that all program and regional office outreach, consultation, and coordination practices will be consistent and adhere to the NRC's responsibilities and requirements.

The audit objective is to determine whether NRC fulfills its tribal outreach and consultation responsibilities and requirements.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Oversight of the National Materials Program

OIG Strategic Goal: Safety

The National Materials Program (NMP) is a term that has been used for many years to define the broad collective framework within which both NRC and the Agreement States carry out their respective radiation safety regulatory programs.

The focus of the NMP is the shared program activities between NRC and Agreement States and the ability of Agreement States to assume a greater proportional responsibility for the shared program activities. The scope of the NMP covers *Atomic Energy Act* materials, which are currently regulated by NRC and Agreement States.

Per NRC Commission direction, NRC and the Agreement States continue to collaboratively address materials issues within the constraints of available resources. Currently, there are 13 non-Agreement States and 37 Agreement States. Two of the non-Agreement States have submitted letters of intent to become Agreement States.

NRC has been developing and piloting the NMP for decades, which reflects the

evolving relationship between NRC and the Agreement States. NRC and Agreement States continue to be challenged with the ability to deal with the NMP environment that is constantly evolving to include changes in priorities for regulatory needs and fiscal conditions.

The audit objective is to determine if the NMP is an effective and efficient framework for carrying out NRC and Agreement State radiation safety regulatory programs.

(Addresses Management and Performance Challenge #2)

Audit of NRC's Special and Infrequently Performed Inspections

OIG Strategic Goal: Safety

NRC conducts baseline inspections at commercial nuclear power plants in support of the Reactor Oversight Process. Additionally, NRC may conduct special and infrequent inspections using criteria in Inspection Manual Chapter (IMC) 2515, Appendix C. These inspections may be implemented in response to events, to infrequent major activities at nuclear power plants, to evaluate emergent technical issues not related to licensee performance, to fulfill NRC's obligations under domestic interagency memoranda of understanding, or to implement the requirements of 10 Code of Federal Regulations (CFR) Part 75 for treaties between the United States and the International Atomic Energy Agency. These inspections are not part of the baseline or supplemental inspection program elements and Regional Administrator authorization is generally required for their implementation.

The audit objectives are to assess NRC's processes for (1) identifying conditions that warrant special and infrequent safety inspections at commercial power reactors under IMC 2515 Appendix C, and (2) conducting these inspections in accordance with agency guidance.

(Addresses Management and Performance Challenge #1)

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act (FISMA) for FY 2017

OIG Strategic Goal: Security

On December 18, 2014, the President signed the *Federal Information Security Modernization Act of 2014* (FISMA), reforming the Federal Information Security Management Act of 2002. FISMA outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. In addition, FISMA includes provisions

such as the development of minimum standards for agency systems, aimed at further strengthening the security of the Federal Government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

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

The evaluation objective is to conduct an independent assessment of the NRC's FISMA implementation for FY 2017.

(Addresses Management and Performance Challenge #3)

Audit of Security Over Research and Test Reactors

OIG Strategic Goal: Security

The NRC maintains an active oversight program of all research and test reactors which includes routine safety and security inspections and assessments. Research and test reactors are nuclear reactors primarily used for research, training, and development. They are licensed to operate at different maximum power levels and utilize various quantities and types of nuclear materials as fuel. The NRC requires research and test reactors to maintain security plans or procedures that are designed to detect, deter, assess and respond to unauthorized activities.

Most research and test reactors are at universities or colleges in the United States. The type and quantity of security measures in place at any given facility are "graded" depending on the potential for radiological release or exposure from the specific facility. Depending on the grade of the facility, individuals may not be required to be screened by metal or explosive detective devices prior to entry into a research and test reactor facility. Almost every research reactor has public education as a key element of its mission, and allows public tours of the facilities. Also, the use of dedicated armed guards varies among the research and test reactors. Most university research reactors rely on armed police officers, usually campus-based police officers for security protection.

The audit objective is to determine whether NRC provides adequate security oversight of research and test reactors.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Fiscal Year 2017 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, 2017. In addition, OIG will issue reports on NRC's

- Special Purpose Financial Statements.
- Condensed Financial Statements.
- Compliance with the *Improper Payments Elimination and Recovery Act of 2010.*

The audit objectives are to

- Express opinions on the agency's financial statements and internal controls,
- Review compliance with applicable laws and regulations,
- Review the controls in NRC's computer systems that are significant to the financial statements,
- Assess the agency's compliance with OMB Circular A-123, Revised, *Management's Responsibility for Enterprise Risk Management and Internal Control*, and
- Assess agency compliance with the *Improper Payments Elimination and Recovery Act of 2010.*

(Addresses Management and Performance Challenge #5)

Audit of NRC's Compliance With Standards Established by the Digital Accountability and Transparency Act (DATA) of 2017

OIG Strategic Goal: Corporate Management

The Digital Accountability and Transparency Act of 2014 (DATA Act) was enacted May 9, 2014, and requires that Federal agencies report financial and payment data in accordance with data standards established by the Department of Treasury and the OMB. The data reported will be displayed on a Web site available to taxpayers and policy makers. In addition, the act requires that OIG review statistical samples of the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality and accuracy of the data sampled and the use of the data standards by the agency.

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) identified a timing anomaly with the oversight requirements contained in the act and recommended that Inspectors General delay reports required by the Act. In the interim, CIGIE encouraged IGs to undertake DATA Act "Readiness Reviews" well in advance of the first November 2017 report. On November 30, 2016, OIG issued a

DATA Act readiness assessment report that concluded NRC demonstrated readiness to meet the requirements set forth in the DATA Act. OIG plans to provide Congress with the first required report in November 2017.

The audit objective is to assess the (1) completeness, timeliness, quality, and accuracy of FY 2017, second quarter financial and award data submitted by NRC for publication on USASpending.gov, and (2) NRC's implementation and use of the Government wide financial data standards established by OMB and Treasury.

(Addresses Management and Performance Challenge #5)

Audit of NRC's Decommissioning Financial Assurance Instrument Inventory

OIG Strategic Goal: Corporate Management

NRC Management Directive 8.12, *Decommissioning Financial Assurance Instrument Security Program*, provides guidance for ensuring that financial instruments, submitted as financial assurance for decommissioning by material licensees and fuel cycle licensees under Title 10, Code of Federal Regulations, fulfill their intent (i.e., providing reasonable assurance that financial resources for decommissioning will be available). The directive describes proper handling and safeguarding of financial instruments, and establishes requirements for the agency to perform an annual internal inventory[1] and a biennial external inventory[2] of the financial instruments. After verification, staff are required to prepare a report for management. These instruments are maintained in an NMSS safe to ensure proper protection.

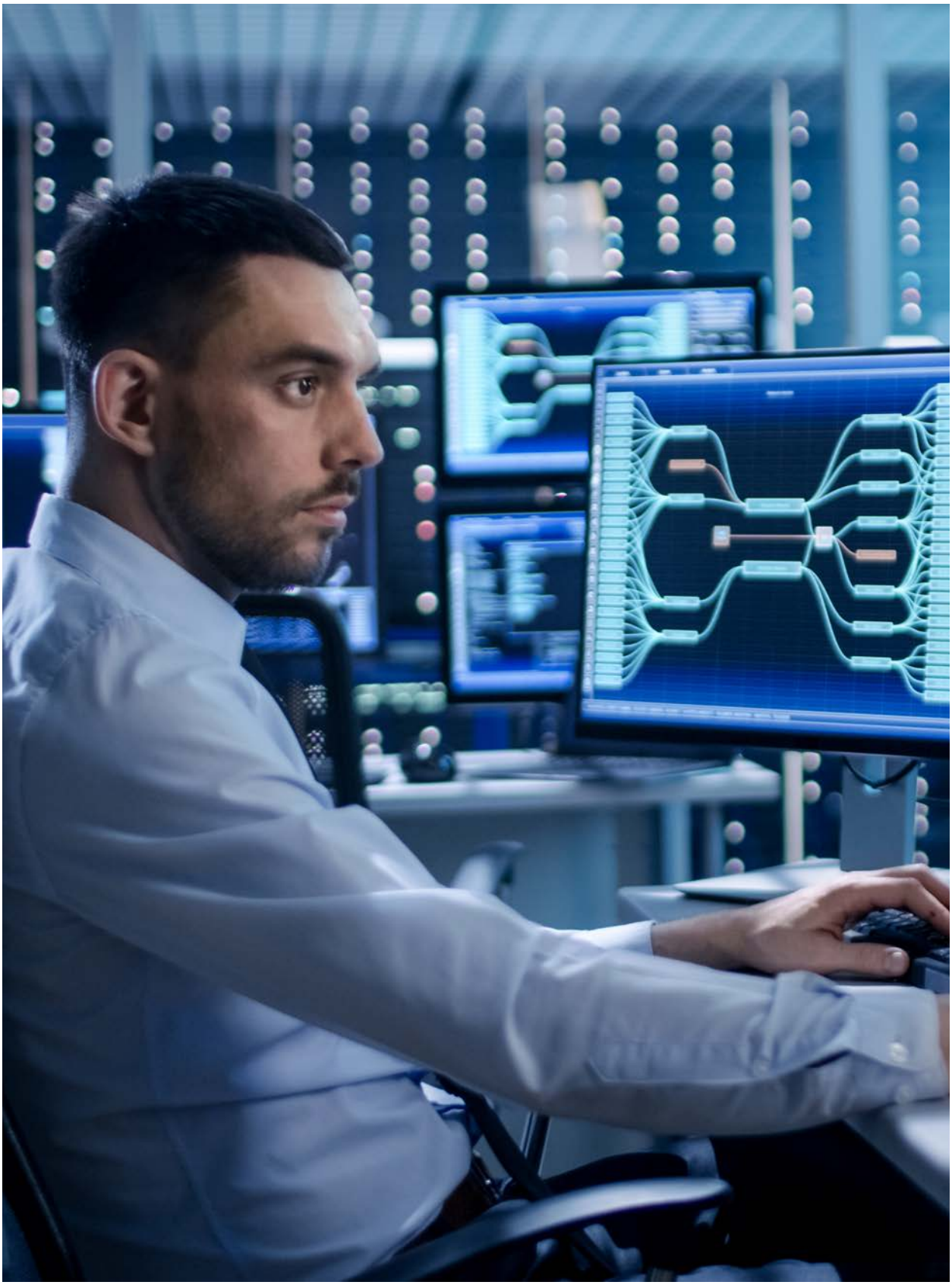
During OIG's *Audit of NRC's Decommissioning Funds Program* (OIG-16-A-16; June 8, 2016) OIG planned to verify the accuracy of the controlled list of original financial instruments maintained by NMSS. However, the safe containing the original financial instruments was broken and inaccessible, and OIG was not able to perform an independent inventory to verify information related to the financial instruments. NMSS' financial instrument control list (unaudited) reportedly contained 45 financial instruments valued at approximately $2.2 billion in decommissioning funds.

The audit objectives are to determine whether (1) NMSS' controlled list of financial instruments accurately accounts for the actual original financial instruments in the safe, and (2) the financial instruments are properly handled, safeguarded, and accurately inventoried in a timely manner.

(Addresses Management and Performance Challenge #5)

[1] *The annual internal inventory is conducted by the financial assurance instrument custodian in the Office of Nuclear Material Safety and Safeguards to evaluate 100 percent of the financial instruments in the safe.*

[2] *The biennial external inventory is conducted by the Office of Nuclear Reactor Regulation to evaluate 25 percent of the financial instruments in the safe.*



Cyber security agent.

NRC INVESTIGATIONS

During this reporting period, OIG received 127 allegations, initiated 22 investigations, and closed 24 cases. Of the 24 closed cases, 2 resulted in issued reports.

Investigative Case Summaries

NRC's Oversight of the St. Lucie Nuclear Power Plant Main Steam Isolation Valves and the Pilgrim Nuclear Power Plant Safety Relief Valve During Component Design Bases Inspections

Strategic Goal: Safety

OIG conducted two proactive investigations that evaluated the adequacy of two Component Design Bases Inspections (CDBI).

The purpose of a CDBI as identified in then-current Inspection Procedure (IP) 71111.21, Component Design Bases Inspection, is to verify that "plant components are maintained within their design basis" and to monitor "the capability of the selected components and operator actions to perform their design bases functions." The IP also notes that "[a]s plants age, modifications may alter or disable important design features making the design bases difficult to determine or obsolete, and that the NRC "risk assessment model assumes the capability of safety systems and components to perform their intended safety function." The inspection, in effect, verifies areas relating to the plant's safety systems, which are by definition rarely employed because their functions come into play only in unusual events, and so, lack ongoing performance measures. It was noted that in the 2017 revision, these purposes remain in force, with additional language emphasizing the effect of modifications.

NRC conducted a CDBI at St. Lucie in 2012, and 3 months after the inspection, in March 2013, a Main Steam Isolation Valve (MSIV) that was specifically inspected during the 2012 CDBI failed and caused a plant shutdown. NRC conducted a CDBI at Pilgrim in 2014, and 7 months later in January 2015, a Safety Relief Valve (SRV) failed to open upon operator demand during mitigation efforts for a Loss of Offsite Power (LOOP) event affecting the plant. A subsequent Special Inspection disclosed that the SRV in question, which was not inspected during the 2014 CDBI, was inoperable. However, an NRC Special Inspection Team disclosed that a second SRV, which had been inspected in the 2014 CDBI, had been inoperable since February 2013, when it had experienced a failure to open upon operator demand during a prior LOOP. This period of inoperability included the time period during which the 2014 CDBI was conducted.

Investigative Results:

OIG did not substantiate that the March 2013 MSIV failure and reactor trip at St. Lucie reflected a failure by NRC staff to conduct the December 2012 CDBI consistently with the requirements of the then-current revision of IP 71111.21. The component failure resulted from the licensee's extended power uprate-related installation of oversized internal parts that were not manufactured properly to meet their design, which was

not readily detectable during the CDBI. This led to the MSIV's inability to fully close, leaving a larger than designed-for portion of the valve disk exposed to steam flow with the plant in operation. This out-of-design exposure caused additional cumulative stress on the valve internals over a long-term period, eventually causing structural failure of an internal retaining pin and inducing the valve to close in an uncontrolled manner while the plant was in operation, resulting in a plant trip. The component failure did not prevent the component from reaching its safety position, but induced a plant shutdown directly related to the inoperability of the component. OIG identified a particular licensee post-installation testing procedure that, although not required to be reviewed in the CDBI, had it been included by the team in their sample of component attributes, could have detected the condition that led to the component failure.

OIG did not substantiate that the failure to detect the inoperability of the SRV at Pilgrim reflected a lack of adherence by NRC staff to the requirements of the then-current revision of IP 71111.21. The prolonged inoperability of the SRV was found to result from the licensee's interpretation of the February 2013 failure of the SRV to open on demand as an instrument problem rather than a problem with the component itself. The SRV's primary safety function was to open automatically at high pressures of approximately 1,000 pounds per square inch/gauge (PSIG) to reduce pressure and prevent system damage during emergencies where pressure could "spike" to high levels. The failures in both 2013 and 2015 were in opening upon operator demand at low pressures of 100 PSIG or below as a means to control pressure during a LOOP necessitated plant cooldown. Other systems and measures were available to accomplish this task and in fact were used during the incidents in question, notwithstanding that operability requirements do not distinguish between function at any point in the pressure range, and thus the unavailability of the SRV to operate at 100 pounds did constitute inoperability of the component. The licensee initiated a condition report documenting the February 2013 incident. However, this condition report was not sampled by the NRC staff during the CDBI, and was not required to be sampled under IP 71111.21.

(Addresses Management and Performance Challenge #1)

Alleged Retaliation by Regional NRC Senior Officials

Strategic Goal: Corporate Management

OIG conducted an investigation into an allegation that an NRC employee was being harassed and retaliated against by two NRC senior officials for raising a safety concern in 2014 regarding a female NRC resident inspector (RI) who fainted in approximately May 2014 in a containment unit (a heated environment) at a nuclear power plant. According to the NRC employee, two NRC senior officials were retaliating against the employee by preventing the employee from completing the Resident Inspector Development Program (RIDP) to become an NRC RI. Specifically, the NRC employee alleged that one of the NRC senior officials

retaliated against the employee by not allowing the employee to test before the Inspector Qualification Board (IQB) to become an RI even though the employee had completed all of the requisite requirements. It was also alleged that the same NRC senior official subjected the employee to participate in a practice qualification board even though no other person in RIDP was required to complete a practice board.

Investigative Results:

OIG did not develop any evidence that the NRC senior officials harassed or retaliated against the employee by engaging in activities to prevent the employee from becoming an NRC RI because the employee raised a safety concern in 2014. Also, OIG did not substantiate that the senior officials prevented the employee from completing the RIDP by not allowing the employee to take the test before the IQB. OIG found that other employees in the RIDP were required to participate in practice qualification boards, and that once the employee passed the practice boards, his/her current branch chief would recommend that person sit for the IQB. OIG found that neither of the two NRC senior officials were on the IQB for the NRC employee or that they attempted to influence the IQB. After the NRC employee tested and failed the final qualification board, the IQB recommended that the employee not be retested to become an RI.

(Addresses Management and Performance Challenge #6)

Inappropriate Communications Involving NRC Staff Pertaining to Reactor Operator Licensing Examination Process

Strategic Goal: Safety

OIG conducted an investigation into an allegation that an NRC senior official and two other NRC employees made inappropriate verbal comments relating to an informal review process involving a 2015 senior reactor operator licensing examination at a nuclear power plant. The alleged remarks were made during and after the informal appeal process. The allegation emphasized that the purported remarks were particularly indicative of bias against one of the applicants who sought review of the practical portion of the examination.

Reactor operator licensing examinations, which are plant specific and overseen by the NRC Region responsible for each given plant, consist of a written examination and an operating test that includes a plant walk-through and a practical test. NRC regulations provide applicants who fail either or both the written and/or the operating test the opportunity to appeal the failing result(s). Such applicants may choose either of two options: request an informal review by impartial NRC staff, usually drawn from headquarters or other Regions, or file a formal appeal to the NRC Atomic Safety and Licensing Board Panel.

Investigative Results:

OIG did not substantiate that NRC staff made any inappropriate remarks to the licensee, applicants, or review panel members during any portion of the examination and review process, and no evidence of bias was disclosed. The review process resulted in the reversal of two examination failures and the issuance of licenses to all applicants who had taken the 2015 senior reactor operator licensing examination at the nuclear power plant.

(Addresses Management and Performance Challenge #1)

Misuse of Government Time and Resources

Strategic Goal: Corporate Management

OIG conducted an investigation into an allegation that an NRC senior official and another NRC employee (the senior official's spouse) were running a charitable organization at NRC during official work hours. The NRC employees, cofounding members of the charitable organization, allegedly sent charity related emails using their NRC email accounts and some of those emails included language that directly or indirectly solicited donations. The emails were sent to NRC staff as well as individuals outside of the NRC.

Investigative Results:

OIG did not substantiate any misconduct by the NRC senior official. However, OIG found that the spouse (an NRC employee) spent anywhere from 1 to 3 hours a day conducting work on behalf of the charitable organization. OIG found that during a 5-year period, the NRC employee used the employee's Government computer to send approximately 150 emails related to the charitable organization. Approximately 14 of the emails included language that directly or indirectly solicited donations. NRC Office of the General Counsel staff advised OIG that the references to donations were not overt or direct; therefore, the emails may not have constituted a solicitation for a donation.

As a result of this investigation, OIG identified that while NRC MD 2.7, *Personal Use of Information Technology*, specifically prohibits NRC employees from using agency information technology to maintain or support a personal, private business, the MD lacks clarity in the following three areas:

- What constitutes de minimis use of Government IT resources for personal use and whether personal IT equipment may be used within Government office space to conduct a personal business activity?
- Is working on behalf of a charitable organization deemed a business activity?
- What constitutes a solicitation for charitable donations?

Because of the apparent need for improved clarity in MD 2.7, OIG requested NRC senior officials to address this issue.

(Addresses Management and Performance Challenge #6)

Leak of Proprietary Information by a Former NRC Employee

Strategic Goal: Security

OIG conducted an investigation into an allegation that a former NRC employee took licensee proprietary information from the NRC upon retiring from Federal service. The retired NRC employee later participated, as a public citizen, in NRC public conference calls. During a public conference call pertaining to a license amendment request, the former NRC employee transmitted to NRC via email the same proprietary licensee information taken from NRC when the employee retired.

Investigative Results:

OIG determined that the former NRC employee sent three pages of licensee information marked "proprietary" to NRC via email during a public conference call. The former NRC employee claimed that the three pages were sent from the employee's Government email account to his/her personal email account when the employee retired from NRC. The former NRC employee claimed not being aware that the document was proprietary. This matter was referred to the U.S. Department of Justice, which declined prosecution.

(Addresses Management and Performance Challenge #3)

Failure to Implement Relevant Inspection Procedures by NRC Region IV Manager

Strategic Goal: Safety

OIG conducted an investigation into an anonymous allegation that during an inspection meeting, an NRC senior official advised licensee personnel that NRC was limiting the scope of the inspection at the nuclear power plant. Specifically, the NRC official allegedly told licensee managers that the power plant would receive no more than 150 items in NRC's Confirmatory Action Letter (CAL) to the licensee. Also, according to the allegation, the NRC senior official had embarrassed and harassed a licensee manager during the inspection meeting by striking the manager in the head with rolled up papers in front of other plant management and staff.

Investigative Results:

OIG did not substantiate that the NRC senior official attempted to limit the number of action items in the NRC CAL to the licensee or that the NRC official engaged in misconduct by striking the plant manager with rolled up papers. Although the NRC senior official apologized to plant officials for unprofessional behavior toward the plant manager during the inspection meeting, the plant manager did not feel that the NRC senior official had acted unprofessionally.

(Addresses Management and Performance Challenge #1)

Abuse of Power in an NRC Office

Strategic Goal: Corporate Management

OIG conducted an investigation into an anonymous allegation that NRC senior officials within a particular office were abusing their power by taking unnecessary offsite inspections for the purpose of attaining frequent flyer miles and hotel points. In addition, the allegation reported there was a "chilled work environment" within the office and that if an individual voiced a concern regarding unfairness or favoritism, the individual would be deliberately taken off the inspection and restricted from traveling.

Investigative Results:

OIG did not substantiate any misconduct by managers within the NRC office. OIG found that an NRC senior executive requested office managers to participate in inspections so that they would be able to mentor and evaluate less experienced inspectors while conducting inspection activities at the site and, at the same time, gain experience in interacting with the vendors in person. Further, the particular office had gone through a workforce assessment, which identified internal issues, including travel assignments, mismanagements, and favoritism within the division. As a result of the assessment, the NRC office underwent an internal review process, including replacement of managers and modification of inspection assignment process, to address the concerns previously raised by the employees. In addition, OIG did not develop evidence of a chilled work environment within the office.

(Addresses Management and Performance Challenge #6)

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created the Defense Nuclear Facilities Safety Board (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 Department of Energy's (DOE) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. Since DOE is a self-regulating entity, DNFSB constitutes the only independent technical oversight of operations at the Nation's defense nuclear facilities. 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, 2016
(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-17-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board. http://www.nrc.gov/docs/ML1627/ML16277A414.pdf*

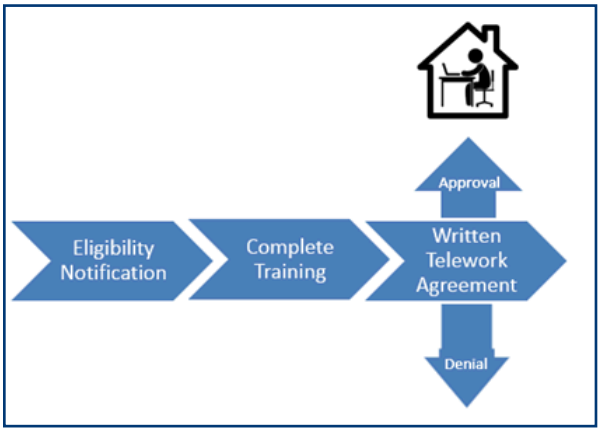
DNFSB AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed two performance audits and evaluations, resulting in numerous recommendations to DNFSB management. These audits and evaluations are summarized below.

Audit Summaries

Audit of DNFSB's Telework Program

Telework Approval Process



Source: Office of the Inspector General generated

The Telework Enhancement Act of 2010 (the act), enacted as Public Law 111-292, requires the head of each executive agency to establish and implement a policy under which employees shall be authorized to telework. The law defines telework as a work flexibility arrangement under which an employee performs the duties and responsibilities of his or her position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.

Employees are required to enter into written agreements with their agencies before participating in telework. The agreement outlines the telework arrangement decided upon by the employee and supervisor. DNFSB's directive and operating procedure contain general organizational guidance on the requirements, responsibilities, and procedures concerning the agency's telework program.

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

Audit Results:

DNFSB's telework directive and operating procedure do not fully address current agency practices, and implementation of internal controls needs to be strengthened. Federal guidance requires agencies to follow specific provisions related to its telework program and maintain effective internal controls over its program. However, while DNFSB staff are currently following Federal guidance in practice, the recently approved directive and operating procedure need to be updated to reflect DNFSB's current practices and Federal guidance. Specifically,

- DNFSB's process for telework denials is unclear because the directive and operating procedure are not consistent on this topic. The directive states that telework termination or denials cannot be grieved or appealed, while the operating procedure states that DNFSB employees have the right to appeal the termination of their telework arrangement.

- DNFSB's telework directive and operating procedure do not list information

technology security training as part of the telework requirements, or include completion of this training on the self-certification safety checklist.

In addition, DNFSB's implementation of policies, procedures, and internal controls for the telework program needs improvement. Specifically, DNFSB's official telework files are inconsistent and incomplete. OIG reviewed 116 telework files and discovered required documents were missing from many of the files.

Moreover, DNFSB's telework agreements are out of date and not regularly reviewed by supervisors or the telework managing officer. In accordance with the new operating procedure dated March 2017, telework agreements are supposed to be reviewed and updated annually.

As a result of not updating its policies, DNFSB risks potential (1) noncompliance with Federal guidance, (2) inconsistent application of the policy by supervisors, (3) inaccurate internal and external data reporting on telework, and (4) reduced Continuity of Operations (COOP) readiness.

(Addresses Management and Performance Challenge #3)

Audit of DNFSB's Resident Inspector Program

Congress created DNFSB to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's (DOE) defense nuclear facilities.

DNFSB's enabling legislation authorizes it to assign staff to be stationed at any DOE defense nuclear facility to carry out the functions of the agency. DNFSB has used this authority to implement a Resident Inspector Program that serves a vital function in the agency's safety oversight of DOE's defense nuclear facilities. Employees in the program relocate to a DOE site with defense nuclear facilities and perform direct oversight of the safety of operations. At this time, there are 10 total resident inspectors, with 2 stationed at 5 DOE sites.

Active Defense Nuclear Sites

Source: OIG Generated

The audit objective was to determine whether the Resident Inspector Program provides for the necessary onsite oversight of DOE defense nuclear facilities to adequately fulfill DNFSB's mission.

Audit Results:

DNFSB's Resident Inspector Program does provide the necessary onsite oversight of DOE defense nuclear facilities to adequately fulfill its mission; however, opportunities for improvement exist. Specifically, DNFSB should (1) create a formal, systematic process to develop and prepare candidates for the resident inspector position, and (2) create a formal, transparent process for annually determining which defense nuclear sites will have resident inspectors, along with the staffing of those sites.

Candidate Development Process

DNFSB is not always able to fill vacant resident inspector positions in a timely manner. Under the current Resident Inspector Program, a timely backfill for a vacant resident inspector position is impeded by the formal application process[3] and training requirements, as resident inspectors are expected to begin training 6 months before relocating to their first DOE defense nuclear site.

In addition to completing applicable pre-assignment training, the resident inspectors are expected to complete additional site-specific training in order to become acquainted with the site and maintain access to the site's facilities. One resident inspector commented that the training process is long and further believes that it takes a year to become effective as a new resident inspector. In addition, DNFSB's current contingency plan in cases of abrupt resident inspector departures is inefficient.

Although DNFSB should ensure continuity of needed skills and abilities, the agency does not have a formalized, systematic process for developing a pool of resident inspectors. As a result, DNFSB could face a gap in oversight at a DOE defense nuclear site.

Resident Inspector Assignments

DNFSB is not transparent in how it determines which defense nuclear sites will have resident inspectors. DNFSB should conduct operations transparently; however, there is no formal process for determining the number and location of resident inspectors.

DNFSB's resource planning process involves technical staff submitting an agency staffing plan to the Board members. The staffing plan must include, among other things, the number and location of resident inspectors stationed at DOE sites. The Board members then vote to approve or disapprove the recommended plan, thereby weighing in on maintaining the status quo or making changes to the number and location of resident inspectors. However, the Board members typically do not make the basis for their decisions to approve or disapprove the staffing plan transparent.

Several DNFSB staff (including resident inspectors) and DOE personnel do not know how DNFSB determines which DOE sites are assigned resident inspectors and the number of resident inspectors each site is assigned. DNFSB and DOE personnel speculated that it is based on tradition, the site's hazard level, and the amount of operational activity within the facilities at the various DOE sites. However, the Board usually does not make its decision making process or the rationale behind the current resident inspector configuration transparent to stakeholders.

Without a transparent process for determining the number and location of resident inspectors, DNFSB may lose stakeholder confidence.

(Addresses Management and Performance Challenges #2 and #4)

[3] *To qualify for the resident inspector position, one must submit a formal application and be a DN level III, IV, or V DNFSB employee. The candidate must also have a minimum of 2 years of direct experience at DNFSB headquarters with an overall performance rating of at least "Fully Successful."*

DNFSB AUDITS

Audits in Progress

Audit of DNFSB's Implementation of Its Governing Legislation

DNFSB is an independent organization within the executive branch chartered with the responsibility of providing recommendations and advice to the President and the Secretary of Energy regarding public health and safety issues at DOE defense nuclear facilities. In operation since October 1989, DNFSB reviews and evaluates the content and implementation of health and safety standards, as well as other requirements, relating to the design, construction, operation, and decommissioning of DOE's defense nuclear facilities.

DNFSB's Board consists of five members appointed by the President for staggered 5-year terms. In FY 2017, the Board is supported by almost 110 technical and administrative staff personnel and a current annual budget of approximately $29 million.

The Board has a variety of authorities and powers for interacting with DOE. These include: (1) conducting public hearings, (2) issuing subpoenas for the attendance of witnesses and production of evidence, (3) formally requesting information or establishing reporting requirements, (4) stationing on-site resident inspectors, and (5) conducting special studies. The Board and its staff annually conduct about 200 site visits with an average duration of 2-3 days. The Board communicates with DOE through trip reports, requests for information, other written correspondence, and meetings. The Board transmits a total of about 100 pieces of correspondence annually to senior DOE management at headquarters and field offices.

The audit objective is to review the role and structure of DNFSB to determine whether the Board is (1) operating in accordance with applicable laws and (2) whether the role and structure is effective to facilitate the agency's mission.

(Addresses Management and Performance Challenge #1)

Audit of DNFSB's Fiscal Year 2017 Financial Statements

Under the Chief Financial Officers Act, as updated by the Accountability of Tax Dollars Act of 2002 and the 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, 2017.

The audit objectives are to

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

(Addresses Management and Performance Challenge #3)

Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act for FY 2017

On December 18, 2014, the President signed the *Federal Information Security Modernization Act of 2014* (FISMA), which reformed the Federal Information Security Management Act of 2002. FISMA outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. In addition, FISMA includes provisions such as the development of minimum standards for agency systems, aimed at further strengthening the security of the Federal Government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security. FISMA provides the framework for securing the Federal Government's information technology including both unclassified and national security systems. All agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their security programs.

The evaluation objective is to conduct an independent assessment of DNFSB's implementation of FISMA for FY 2017.

(Addresses Management and Performance Challenge #2)

Audit of DNFSB's Compliance with Standards Established by the Digital Accountability and Transparency Act (DATA) of 2014

The Digital Accountability and Transparency Act of 2014 (DATA Act) was enacted May 9, 2014, and requires that Federal agencies report financial and payment data in accordance with data standards established by the Department of the Treasury and OMB. The data reported will be displayed on a Web site available to taxpayers and policy makers. In addition, the act requires that OIG review statistical samples of the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality and accuracy of the data sampled and the use of the data standards by the agency.

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) identified a timing anomaly with the oversight requirements contained in the act and recommended that IGs delay reports required by the act. In the interim, CIGIE encouraged IGs to undertake DATA Act "Readiness Reviews" well in advance of the first November 2017 report. On November 30, 2016, OIG issued a DATA Act readiness assessment report that concluded DNFSB demonstrated readiness to meet the requirements set forth in the DATA Act. OIG plans to provide Congress with the first required report in November 2017.

The audit objective is to assess the (1) completeness, timeliness, quality, and accuracy of FY 2017, second quarter financial and award data submitted by DNFSB for publication on USASpending.gov, and (2) DNFSB's implementation and use of the Government-wide financial data standards established by OMB and Treasury.

(Addresses Management and Performance Challenge #3)

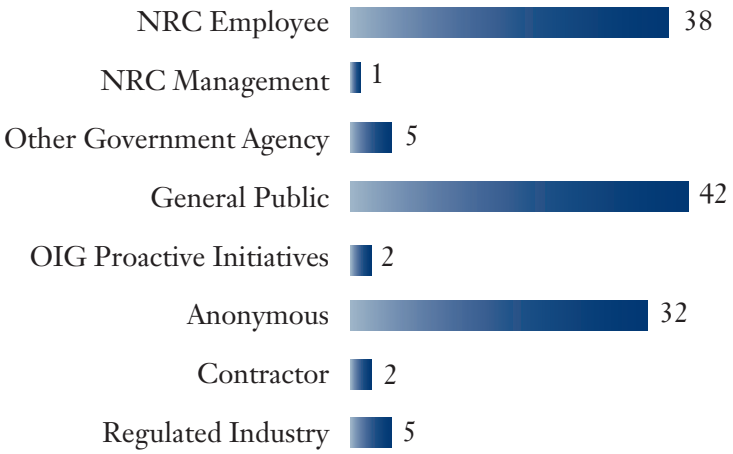
Nuclear power plant generator.

SUMMARY OF NRC OIG ACCOMPLISHMENTS AT NRC

April 1, 2017—September 30, 2017

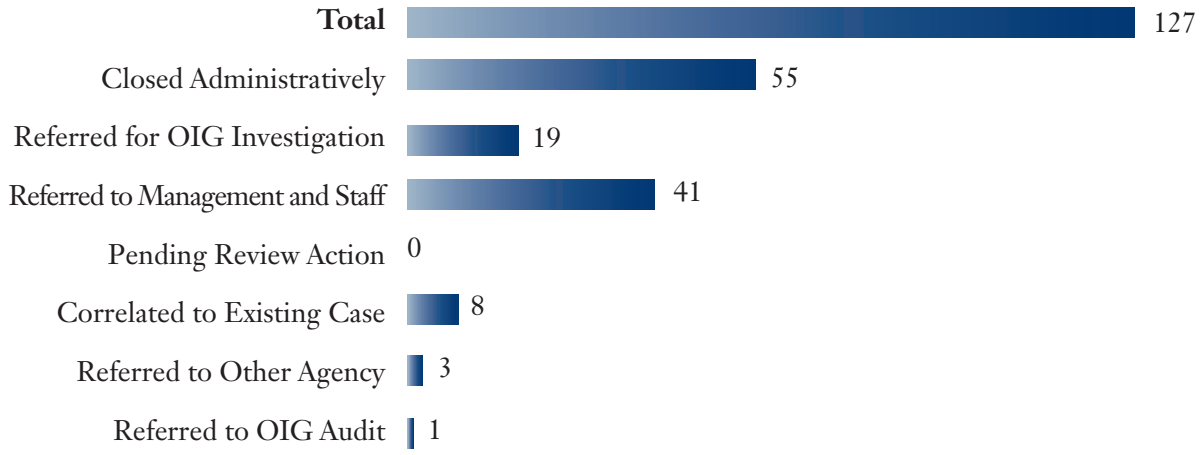
Investigative Statistics

Source of Allegations



Allegations resulting from the NRC OIG Hotline calls: 69 **Total: 127**

Disposition of Allegations



Status of Investigations

DOJ Referrals 8
DOJ Declinations 3
DOJ Pending 5
Criminal Informations/Indictments 0
Criminal Convictions 0
Criminal Penalty Fines 0
Civil Recovery 0
State and Local Referrals 0
Criminal Informations/Indictments 0
Criminal Convictions 0
Civil Penalty Fines 0
Civil Recovery 0
NRC Administrative Actions:
- Counseling and Letter of Reprimand 1
- Terminations and Resignations 1
- Suspensions and Demotions 2
- Other (e.g., PFCRA) 0

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued[4]	Cases in Progress
Conflict of Interest	0	1	0	0	1
Employee Misconduct	13	11	9	2	15
External Fraud	8	3	0	0	11
Internal Fraud	1	0	0	0	1
Management Misconduct	15	5	8	0	12
Miscellaneous	6	0	2	0	4
Proactive Initiatives	4	0	1	0	3
Technical Allegations	7	2	3	0	6
Theft	1	0	1	0	0
Total	**55**	**22**	**24**	**2**	**53**

[4] *Number of reports issued represents the number of closed cases where allegations were substantiated and the results were reported outside of OIG.*

NRC Audit Listings

Date	Title	Audit Number
09/21/17	Evaluation of NRC's Management of Government Cell Phones	OIG-17-A-27
09/21/17	Evaluation of NRC's Proposed Modifications to the Probabilistic Risk Assessment Process.	OIG-17-A-26
09/20/17	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2017—Region IV-Arlington, TX	OIG-17- A-25
09/13/17	Evaluation of NRC's Management of Electronic Records	OIG-17-A-24
08/22/17	Audit of NRC's 10 CFR 2.206 Petition Review Process	OIG-17-A-23
08/17/2017	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2017—Technical Training Center, Chattanooga, Tennessee	OIG-17-A-22
08/16/2017	Audit of NRC's Oversight for Issuing Certificates of Compliance for Radioactive Material Packages	OIG-17-A-21
08/16/2017	Audit of NRC's Contract Administration Process	OIG-17-A-20
07/27/2017	Evaluation of NRC's Network Storage Interruption	OIG-17-A-19
07/03/2017	Audit of NRC's PMDA and DRMA Functions to Identify Program Efficiencies	OIG-17-A-18
07/03/2017	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2017—Region I, King of Prussia, PA	OIG-17-A-17
06/20/2017	Audit of NRC's Adoption of Cloud Computing	OIG-17-A-16
05/31/2017	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2017-Region III, Lisle, IL	OIG-17-A-15
05/30/2017	Audit of NRC's Purchase Card Program	OIG-17-A-14
05/11/2017	Audit of NRC's Fiscal Year (FY) 16 Compliance with Improper Payment Laws	OIG-17-A-13
05/02/2017	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2017-Region II, Atlanta, GA	OIG-17-A-12
04/26/2017	Audit of NRC's Oversight of Employee Participation in American Society of Mechanical Engineers Code Committees	OIG-17-A-11
04/11/2017	Audit of NRC's Fire Protection Oversight of Operating Reactors	OIG-17-A-10

NRC Contract Audit Reports

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs (Dollars)	Unsupported Costs (Dollars)
09/08/16	**NUMARK ASSOCIATES, INC.** Independent Audit on NUMARK Associates, Inc. Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Years 2013, 2014 and 2015 NRC-HQ-12-C-42-0107 NRC-HQ-25-14-E-0004 NRC-HQ-25-14-E-0001	$0	$0
09/06/17	**BECKMAN & ASSOCIATES, INC** NRC-HQ-13-C-03-0032	$0	$0
9/11/17	**Qi Tech, LLC** Independent Audit Report on Qi Tech, LLC's proposed Amounts on Unsettled Flexibly Priced Contracts for FYs 2013 and 2014	$302,628	$0

Audit Resolution Activities

TABLE I

OIG Reports Containing Questioned Costs[5]

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[6]	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	0	0	0

[5] *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.*

[6] *In OIG's prior Semiannual Report to Congress (October 1, 2016, to March 31, 2017), OIG reported that a management decision was made. However, according to NRC management, the contractor provided additional documentation concerning the questioned costs and this information is being reviewed by NRC to determine if it is supportive of reducing the amount of questioned costs. This review shall be completed no later than December 31, 2017.*

TABLE II

OIG Reports Issued with Recommendations That Funds Be Put to Better Use[7]

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

[7] *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** **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 (SNM) inventories and validation of reported information. **Recommendation 3:** Document the basis of the approach used to risk inform NRC's oversight of MC&A activities for all types of materials licensees.	**OIG-03-A-15**

TABLE IV

Significant Revised Management Decisions

Date	Report Title	Number
4/7/2017	**Audit of the U.S. Nuclear Regulatory Commission's Implementation of 10 CFR Part 21, Reporting of Defects and Non-Compliance** April 13, 2016, the Commission approved the NRC staff's recommendation to eliminate rulemaking efforts related to 10 CFR Part 21, "Reporting of Defects and Noncompliance." After extensive work on this rule, staff concluded that there is not a basis for revising the rule itself, and that necessary changes can be achieved through clarification of the regulatory guidance for the rule. NRC quantified this resource reduction in terms of 1 staff Full Time Equivalent (FTE) and included this resource reduction in the formulation of the NRC FY 2017 Congressional Budget Justification. On May 2, 2017, OIG acknowledged that staff would discontinue the Part 21 rulemaking based on the Commission decision, recognized the ongoing staff efforts, and agreed that the proposed actions support the intent of the recommendation. OIG will close the recommendation upon review of the final regulatory guidance for implementing 10 CFR Part 21.	**OIG-11-A-08**

SUMMARY OF NRC OIG ACCOMPLISHMENTS AT THE DNFSB

April 1, 2017, through September 30, 2017

Investigative Statistics

Source of Allegations

DNFSB Employee 3

DNFSB Management 2

Allegations Received from NRC OIG Hotline: 4 **Total: 5**

Disposition of Allegations

Total 5

Referred for OIG Investigation 1

Pending Review Action 1

Closed Administratively 2

Referred to Other Agency 1

Status of Investigations

DOJ Referrals 1
DOJ Declinations 1
DOJ Pending 0
Criminal Informations/Indictments 0
Criminal Convictions 0
Criminal Penalty Fines 0
Civil Recovery 0
State and Local Referrals 0
Criminal Informations/Indictments 0
Criminal Convictions 0
Civil Penalty Fines 0
Civil Recovery 0
DNFSB Administrative Actions:
- Counseling and Letter of Reprimand 0
- Terminations and Resignations 1
- Suspensions and Demotions 0
- Other (e.g., PFCRA) 0

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued[8]	Cases in Progress
Employee Misconduct	1	0	0	0	1
Management Misconduct	4	2	0	0	6
Proactive Initiatives	2	0	0	0	2
Total	**7**	**2**	**0**	**0**	**9**

[8] *Number of reports issued represents the number of closed cases where allegations were substantiated and the results were reported outside of OIG.*

DNFSB Audit Listings

Date	Title	Audit Number
07/10/2017	Audit of DNFSB's Telework Program	DNFSB-17-A-06
06/05/2017	Audit of DNFSB's Resident Inspector Program	DNFSB-17-A-05

DNFSB AUDIT RESOLUTION ACTIVITIES

TABLE I

OIG Reports Containing Questioned Costs[9]

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

[9] *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[10]

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

[10] *A "recommendation that funds be put to better use" is a recommendation by the OIG that funds could be used more efficiently if DNFSB 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 DNFSB, 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.*

UNIMPLEMENTED AUDIT RECOMMENDATIONS

NRC Unimplemented Recommendations

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2003	Audit of NRC's Regulatory Oversight of Special Nuclear Materials	OIG-03-A-15	5/23/03	2	$0	NRC is authorized to grant licenses for the possession and use of special nuclear materials (SNM) and establish regulations to govern the possession and use of those materials. NRC's regulations require that certain materials licensees have extensive material control and accounting programs as a condition of their license. However, all license applicants, including those requesting authorization to possess small quantities of SNM, must develop and implement plans and activities that demonstrate a commitment to accurately control and account for radioactive materials. Licensees are also required to allow NRC to inspect the materials, controls, and premises where SNM and source materials are used or stored. Additionally, NRC requires that materials licensees report information to the Nuclear Materials Management and Safeguards System (NMMSS). NMMSS is a computer database managed by the U.S. Department of Energy (DOE) and jointly used with NRC as the national system for tracking certain private- and Government-owned nuclear materials. The audit objective was to determine whether NRC adequately ensures its licensees control and account for special nuclear material. The audit report made eight recommendations aimed at strengthening NRC's oversight of Special Nuclear Material. Agency management provided formal comments.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2010	Audit of NRC's Vendor Inspection Program	OIG-10-A-20	9/28/10	3	$0	NRC endeavors to protect the public health and safety and the environment by overseeing vendor compliance with NRC's regulations for assuring the integrity of domestic and global parts and services supplied to nuclear power reactors. Vendors manufacture a range of components such as fasteners, pumps, valves, and reactor vessels, as well as provide design, engineering, and construction services. While most vendors do not hold NRC licenses, they are nonetheless bound through contracts with licensees, applicants, or other vendors to comply with NRC's quality assurance regulations contained in Appendix B to Title 10, Code of Federal Regulations (10 CFR), Part 50 (Appendix B). Vendors are also required to comply with 10 CFR Part 21 (Part 21). NRC conducts reactive and routine inspections of vendors' implementation of Appendix B and Part 21 requirements. The audit objective was to assess NRC's regulatory approach for ensuring the integrity of domestic and foreign safety-related parts and services supplied to current or prospective nuclear power reactors. The audit report made ten recommendations aimed at strengthening NRC's approach to vendor inspection. Agency management agreed with the report.
2011	Audit of NRC's Implementation of 10 CFR Part 21, *Reporting of Defects and Noncompliance*	OIG-11-A-08	3/23/11	3	$0	NRC endeavors to protect the public health and safety and the environment through the regulation of the operating nuclear power plants in the United States. The *Energy Reorganization Act of 1974, as Amended, Section 206, Noncompliance*, provides the statutory basis for NRC guidance and regulations that pertain to reporting component defects in operating reactors. Specifically, it requires licensees operating nuclear power plants to notify NRC of defects in basic components that could cause a substantial safety hazard. NRC uses Title 10, Code of Federal Regulations, Part 21, *Reporting of Defects and Noncompliance* (Part 21) to implement the provisions of Section 206. The primary NRC office responsible for Part 21 implementation among licensees with operating plants is the Office of Nuclear Reactor Regulation. The audit objective was to determine if NRC's implementation of Federal regulations requiring reactor licensees to report defects contained in installed equipment is meeting the intent of the *Energy Reorganization Act of 1974, as Amended, Section 206,* Noncompliance. The audit report made five recommendations to improve NRC's implementation of Part 21. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2011	Audit of NRC's Shared "S" Drive	OIG-11-A-15	7/27/11	2	$0	The President of the United States has directed Federal agencies to promote information sharing with the public and improve the transparency of Government operations. Nevertheless, applicable laws and Government wide policies require NRC and other Federal agencies to protect some types of information against accidental or intentional disclosure. NRC staff process on agency networks a category of sensitive unclassified information unique to NRC called Sensitive Unclassified Non-Safeguards Information (SUNSI) on agency networks. NRC defines SUNSI as: "… any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal programs, or the personal privacy of individuals." The audit objective was to assess whether NRC effectively protects electronic documents containing Personally Identifiable Information and other types of SUNSI on NRC's shared network drives. The audit report made five recommendations to improve training, communication, coordination, and quality assurance controls to ensure SUNSI is appropriately managed. Agency management agreed with the report.
2012	Audit of NRC's Management of the Baseline Security Inspection Program	OIG-12-A-10	3/8/12	3	$0	NRC's baseline security inspection program is the agency's primary means for ensuring that nuclear power plants across the United States are protected in accordance with Federal Government regulations. The objective of this audit was to evaluate NRC's management of the baseline security inspection program, including specific program features such as the Significance Determination Process. The report made five recommendations to improve NRC's management of the baseline security inspection program. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2013	Audit of NRC's Process for Calculating License Fees	OIG-13-A-02	10/24/12	1	$0	The *Omnibus Budget Reconciliation Act of 1990* (OBRA-90), as amended, requires that NRC recover, through fees assessed to its applicants and licensees, approximately 90 percent of its budget authority [less amounts appropriated for waste incidental to reprocessing activities and amounts appropriated for generic homeland security activities ("non-fee items"). NRC assesses two types of fees to meet the requirements of OBRA-90—user fees and annual fees. First, user fees, presented in Title 10, Code of Federal Regulations (10 CFR), Part 170, under the authority of *the Independent Offices Appropriation Act of 1952*, recover NRC's costs of providing special benefits to identifiable applicants and licensees. Second, annual fees, presented in 10 CFR Part 171 under the authority of OBRA-90, as amended, recover generic regulatory costs not recovered through 10 CFR Part 170 fees. On an annual basis, NRC amends the licensing, inspection, and annual fees. Additionally, NRC publishes the annual Fee Rule in the Federal Register. The audit objective was to determine if NRC has established and implemented management controls to ensure that the license fee calculation process produces timely and accurate fees in accordance with applicable requirements. The audit report made four recommendations to further improve the license fee calculation process. Agency management agreed with the report.
2013	Audit of NRC's Safeguards Information Local Area Network and Electronic Safe	OIG-13-A-16	4/1/13	5	$0	NRC developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI) documents. SLES features two distinct components: a secure wireless Local Area Network (LAN) and an electronic safe (E-Safe) for SGI documents. The SGI LAN component is a network with a secure architecture and is dedicated for use in SGI data processing. The E-Safe component is a secure electronic data repository for SGI records. E-Safe users are able to create, capture, search, and retrieve data from this repository. The audit objective was to determine if SLES meets its operational capabilities and applicable security controls. The audit report made seven recommendations to improve the agency's SLES system. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2013	Audit of NRC's Budget Execution Process	OIG-13-A-18	5/7/13	1	$0	The U.S. Government requires Federal agencies to establish an effective funds control process to ensure funds are used only for the purpose set forth by Congress and that expenditures do not exceed amounts authorized. NRC's budget process consists of strategic planning; budget formulation; submission of the agency's budget to the Office of Management and Budget and Congress; approval of the budget by Congress; budget execution; and the reporting of budget and performance results. The budget execution phase refers generally to the time period during which the budget authority made through an appropriation remains available for obligation by NRC. NRC's task during the budget execution process is to spend appropriated funds to carry out its mission in accordance with fiscal statutes. Between fiscal years (FY) 2008 and 2012, NRC's budget appropriation ranged from $926.1 million to $1,066.9 million. The audit objectives were to determine whether (1) NRC maintains proper financial control over appropriated and apportioned funds to ensure compliance with applicable Federal laws, policies, and regulations and (2) opportunities exist to improve the budget execution process. The audit report made eight recommendations to improve the internal controls over the management of budget execution. Agency management agreed with the report.
2014	Audit of NRC's Oversight of Active Component Aging	OIG-14-A-02	10/28/13	2	$0	The *Atomic Energy Act of 1954*, as amended, and NRC regulations limit commercial nuclear power reactor licenses to an initial 40 years. Due to this selected period, some components may have been engineered on the basis of an expected 40-year service life. Components degraded due to aging have caused reactor shutdowns, failure of safety-related equipment, and reduction in the safety margin of operating nuclear power plants. Therefore, effective and proactive management of aging of components is a key element for safe and reliable nuclear power plant operation. NRC has established commercial nuclear power reactor industry requirements that exclude some components—referred to as active components—from a license renewal aging management review. Active components are those that perform their intended functions with moving parts or a change in state. According to NRC, active components are not subject to review as part of NRC's review of license renewal applications because of the existing regulatory process and existing licensee programs and activities. The NRC Office of Nuclear Reactor Regulation and the regional offices provide regulatory oversight of industry's active component aging activities. The audit objective was to determine if NRC is providing effective oversight of industry's aging component programs. The audit report made two recommendations to improve the agency's oversight of aging active component activities. Agency management provided formal comments to the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2014	Audit of NRC's Freedom of Information Act Process	OIG-14-A-17	6/16/14	1	$0	The Freedom of Information Act (FOIA) is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government. NRC's FOIA program is managed by the FOIA, Privacy, and Information Collections Branch (referred to in this report as the FOIA office) within the Office of Information Services, Customer Service Division. The FOIA process begins when the agency (1) receives—via mail, facsimile, or Internet—an incoming FOIA request, (2) assigns it a number, and (3) determines which NRC offices need to review their records to identify whether they have information pertinent to the request and sends a request to those offices. FOIA coordinators in responsive offices provide an estimate of the search, review, and duplication effort required to produce any documents identified as within the scope of the request. The audit objective was to determine whether the FOIA process is efficient and complies with the current laws. The audit report made nine recommendations to improve the efficiency of NRC's FOIA process. Agency management agreed with the report.
2015	Audit of NRC's Oversight of Spent Fuel Pools	OIG-15-A-06	2/10/15	2	$0	NRC is responsible for developing the regulatory framework, analytical tools, and data needed to ensure safe and secure storage, transportation, and disposal of spent nuclear fuel. For both operating and permanently shut down nuclear power plants in the United States, there are a total of 93 spent fuel pools that currently store spent fuel. Recent NRC staff studies demonstrating the safety of spent fuel pools and the safety of continued storage of spent fuel at reactor sites highlight the need to ensure the safety of pool operations for longer periods than originally envisioned. The audit objective was to determine whether NRC's oversight of spent fuel pools and the nuclear fuel they contain provides adequate protection for public health and safety, and the environment. The report made four recommendation to improve oversight of spent fuel pools. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Process for Ensuring Integrity in Scientific Research	OIG-15-A-08	2/10/15	1	$0	The Federal Government disseminates a variety of scientific information, including statistical information; information about health, safety, and environmental risks; and technical information it creates or obtains in the course of developing regulations. Scientific information is based on scientific research, analyses, and data performed to support the agency's work. Often, regulations are based on scientific, engineering, and economic analyses. Therefore, it is crucial that information disseminated by Federal agencies be objective, and have utility, quality, and integrity. To ensure information integrity, Federal agencies are required to adopt standards for information quality. These standards are set by the Office of Management and Budget (OMB). The Office of Regulatory Research plays a central role in the agency's information quality program because it leads peer review efforts of agency products. The audit objective was to determine whether NRC has controls in place to assure that scientific research is objective, credible, and transparent. The audit report made five recommendations to strengthen agency's information quality program. Agency management agreed with the report.
2015	Audit of NRC's Internal Controls Over Fee Revenue	OIG-15-A-12	3/19/15	4	$0	NRC is required by law to offset a substantial percent of its budget authority through fees billed to licensees and license applicants. NRC provides licensing services to agency licensees and license applicants. The agency recovers the costs to provide licensing services by invoicing licensees and applicants for staff time and contractor costs. Each fiscal year, NRC publishes a schedule of fees in 10 Code of Federal Regulations (CFR) Part 170 for licensing services directly provided to NRC licensees and applicants, and in 10 CFR Part 171 for annual fees billed to identifiable NRC license holders for generic regulatory costs not otherwise recovered through 10 CFR Part 170 fees. The audit objective was to determine whether NRC has established and implemented an effective system of internal controls over the recordation and reconciliation of fee revenue. The audit report made seven recommendations to improve internal controls over the recordation of fee revenue. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Regulatory Analysis Process	OIG-15-A-15	6/24/15	2	$0	The *Atomic Energy Act of 1954*, as amended (42 U.S.C. 2011), and Energy Reorganization Act of 1974, authorize NRC to develop regulations that licensees must follow to protect public health and safety and the environment, and to promote the common defense and security. NRC is authorized to establish by rule, regulation, or order, such standards and instructions to govern the possession and use of special nuclear, source, and byproduct material. NRC uses regulatory analyses to evaluate proposed rulemaking actions to protect public health and safety. NRC does not have a statutory mandate to conduct regulatory analyses, but voluntarily began performing them in 1976 to help ensure that its decisions to impose regulatory burdens on licensees are based on adequate information. The audit objective was to determine the adequacy of NRC's regulatory analysis process. The audit report made four recommendations to improve the regulatory analysis process. Agency management agreed with the report.
2015	Audit of NRC's Reactor Business Lines' Compliance with Agency Non-Financial Internal Control Guidance	OIG-15-A-16	6/25/15	1	$0	All Federal agencies are required to have internal controls in place for both financial and non-financial processes. Internal controls include activities to ensure that agency programs and processes work as intended. NRC has organized all programs, functions, and major activities into internal control areas referred to as business lines to provide a consistent framework for assessing internal control. A business line is a subdivision or component part of an agency program or administrative function that can be assessed for risks and allow for meaningful evaluation of internal control. The audit objective was to determine the extent to which NRC has developed effective reactor safety business line internal control processes for non-financial, programmatic activities. The audit report made three recommendations that will increase compliance with agency programmatic, non-financial internal control guidance. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Web-Based Licensing (WBL) System	OIG-15-A-17	6/29/15	2	$0	NRC's primary mission is to license and regulate the use of radioactive materials for civilian purposes to ensure adequate protection of public health and safety and the environment. NRC's recent Project Aim 2020 report noted that, although NRC accomplishes its mission, a lack of standardized processes is an obstacle to efficiency and agility. Deployed in 2012, NRC's Web-Based Licensing System (WBL) serves as an up-to-date repository of all NRC materials licenses, and as a Web-based license tool for NRC to manage the license process and information on NRC licensees. The incorporation of additional modules, such as for inspection and reciprocity tracking, ties various NRC oversight activities to the most up-to-date license information. The audit objective was to determine whether WBL meets its required operational capabilities and provides for the security, availability, and integrity of the system data. The audit report made four recommendations to improve NRC's use of WBL. Agency management agreed with the report.
2015	Audit of NRC's Management of Change	OIG-15-A-19	9/1/15	1	$0	As Federal budgets grow and shrink, as economic and environmental forces shape energy policy, and as legislative requirements wax and wane, the NRC's regulatory responsibilities—and the way it implements that oversight—will be subject to change. In just the past 5 years, NRC has undertaken several significant change initiatives. For example, in 2010, NRC initiated a "Transforming Assets into Business Solutions" effort with the goal of making NRC more effective and efficient by consolidating and improving business practices. Additional expected change awaits NRC as the result of "Project Aim 2020," which analyzes potential organizational changes to enhance NRC's ability to perform its mission in the future. Change management research and best practices demonstrate that many change initiatives fail because managers often skip steps needed to implement change or they make critical mistakes while implementing change. Change management literature also points to the importance of organizations to manage change efficiently and effectively to increase the likelihood that change occurs as intended. The audit objective was to assess the efficiency and effectiveness of NRC's management of change. The audit report made three recommendations to complete implementation of and promote the agency's change management framework and provide training to staff on the agency's approach to change management. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Evaluation of the Agencywide Document Access Management System (ADAMS) Functional and Operational Capabilities	OIG-16-A-06	11/30/15	3	$0	The Agencywide Documents Access and Management System (ADAMS) is NRC's repository for Official Agency Records. It has been in place since November 1999 and has to meet NRC's document management needs while also complying with Federal mandates for electronic recordkeeping and public access requirements. The Office of Information Services manages ADAMS and staff in headquarters and regional offices use ADAMS for their day-to-day mission activities. The public uses NRC's public site to access Web-Based ADAMS. The evaluation objective was to determine if ADAMS meets its required operational capabilities and adequately provides for functionality. The evaluation report made 13 recommendations addressing implementation of ADAMS' Records Manager module, improving ADAMS' search and retrieval functionality, and ensuring compliance with security standards and configuration management best practices. Agency management agreed with the report.
2016	Audit of NRC's Network Security Operations Center	OIG-16-A-07	1/11/16	3	$0	NRC's Network Security Operations Center (SOC) is responsible for securing the agency's network infrastructure and monitoring the network for suspicious activity. The SOC accomplishes this through the use of automated security tools, analysis of network activity data, and participation in incident response efforts. The SOC is primarily staffed by contractors working under the Information Technology Infrastructure Support Services contract. Robust SOC capabilities are particularly crucial given the sensitivity of the unclassified information processed on NRC's network, and the increasing volume of attacks carried out against Federal Government computer systems. The audit objective was to determine whether NRC's network SOC meets operational requirements, and to assess the effectiveness of SOC coordination with other organizations that have a role in securing NRC's network. The audit report made four recommendations to improve SOC performance and capabilities through better definitions of contract requirements and improving clarity in organizational roles and responsibilities. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of NRC's Personal Identity Verification (PIV) Card Access System	OIG-16-A-10	3/7/16	1	$0	The Personal Identity Verification (PIV) card is an identification card issued by a Federal agency that contains information unique to each employee and contractor. The main function of the card is to protect and to strengthen the security of both employees' and contractors' information and physical access to secured areas. NRC uses the PIV card to control physical access at its headquarters and its regional offices. Federal policies require agencies to swiftly revoke physical access rights at termination of employment. NRC must collect and destroy PIV cards from Federal employees and contractors upon termination. Additionally, some areas within NRC are restricted to certain individuals. Each restricted area has a designated representative who must maintain an up-to-date access list of individuals needing access. The audit objective was to determine whether NRC's PIV card access system meets its operational requirements, and to assess the effectiveness of the PIV system coordination among offices that have a role in securing NRC's physical access. The audit report made seven recommendations to improve the PIV card access system, reduce physical security risk across the agency, and ensure continued compliance with Federal regulations and guidance. Agency management agreed with the report.
2016	Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications	OIG-16-A-15	6/1/16	6	$0	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 resources. NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought after by potential adversaries. The NRC Office of Inspector General joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG assessed 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. NRC perimeter security services (e.g. , firewalls, intrusion detection/prevention systems) were configured to whitelist (i.e.,monitor only, not block) the scanning platforms/hosts identified in the agreed upon rules of engagement. The evaluation objective was to determine (i) the effectiveness of NRC's efforts to secure its publicly accessible Web applications, and (ii) whether NRC has implemented adequate security measures to reduce the risk of compromise to publicly accessible Web applications. The audit report made seven recommendations to improve the security of NRC's publicly accessible Web applications. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of NRC's Decommissioning Funds Program	OIG-16-A-16	6/8/16	2	$0	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 power reactor and material licensees to 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 audit report makes nine recommendations to improve internal controls related to decommissioning funds reviews and strengthen the agency's decommissioning funds review process. Agency management agreed with the report.
2016	Audit of NRC's Implementation of Federal Classified Information Laws and Policies	OIG-16-A-17	6/8/16	1	$0	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 objective was to assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed and effectively administered, and identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material. This report makes two recommendations to complete and fully implement current agency initiatives and to develop procedures and guidance to ensure effective records management and timely disposition and declassification of classified records at NRC. Agency management stated their agreement with the findings and recommendations in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	*Cybersecurity Act of 2015* Audit for NRC	OIG-16-A-18	8/8/16	1	$0	The *Cybersecurity Act* was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. Division N, Section 406, of 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. This audit report makes two recommendations to improve security over NRC's national security systems information systems, ensure compliance with Federal policies through development of agency wide policies and procedures over classified information systems, and maintain an agency wide inventory of national security systems. Agency management agreed with the report.
2016	Audit of NRC's Implementation of *Federal Managers' Financial Integrity Act* for Fiscal Year 2015	OIG-16-A-20	9/19/16	2	$0	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 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 Performance and Accountability Report. The audit report makes three recommendations to improve the effectiveness of NRC's process to assess internal control over program operations. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of NRC's Significance Determination Process for Reactor Safety	OIG-16-A-21	9/26/16	4	$0	The NRC Significance Determination Process (SDP) is used to determine the safety significance of inspection findings identified within the Reactor Oversight Process 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. The audit report made four recommendations to improve overall management of SDP workflow, clarify issue screening questions for inspection staff, and implement controls to ensure independent audits are performed and documented. Agency management agreed with the report.
2017	Independent Evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014* for Fiscal Year 2016	OIG-17-A-03	11/8/16	3	$0	The *Federal Information Security Modernization Act of 2014* (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of NRC's implementation of FISMA 2014 for fiscal year (FY) 2016. The evaluation objective was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA 2014 for FY 2016. The evaluation found three repeat findings from previous FISMA evaluations pertaining to continuous monitoring not being performed as required, and the NRC system inventory not being up-to-date. In addition, the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate. The evaluation report made five recommendations to improve NRC's implementation of FISMA. Agency management agreed with the report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Audit of NRC's Foreign Assignee Program	OIG-17-A-07	12/19/16	3	$0	Under the foreign assignee program, NRC invites peers from other nuclear safety regulators to obtain experience that would enhance safety programs and research programs worldwide, as well as promote exchange of technical information and expertise. Foreign assignees remain employees of the sponsoring regulatory or research organization in their home country. Approximately 80 foreign nationals have worked as assignees at NRC since 2005, representing 21 countries. The Office of International Programs has primary responsibility for the foreign assignee program and coordinates with other offices through the process of onboarding a foreign assignee and during the assignment. In recent years, assignees have worked in various offices at NRC headquarters and in NRC regional offices. The objective of this audit was to assess whether the NRC foreign assignee program provides adequate information security. The audit report makes three recommendations to develop a procedure for security planning during the process of onboarding and hosting a foreign assignee and to provide a secure, cost-effective email for the use of foreign assignees at NRC. Agency management agreed with the report.
2017	Audit of NRC's Oversight of Source Material Exports to Foreign Countries	OIG-17-A-08	2/16/17	5	$0	NRC's mission is to regulate the Nation's civilian use of nuclear materials to ensure protection of public health and safety, promote the common defense and security, and protect the environment. One of the agency's statutorily mandated responsibilities under the *Atomic Energy Act of 1954*, as amended, is to license the import and export of nuclear materials. Source material is often exported to be enriched and used as fuel for nuclear power plants across the world. As source material (uranium) could potentially be enriched to produce highly enriched uranium—the primary ingredient of an atomic weapon—tracking and accounting for the exports of source material are important to (1) ensure that it is used only for peaceful purposes, (2) comply with international treaty obligations, and (3) provide data to policymakers and other government officials. The audit objective was to determine the effectiveness of NRC's oversight of the export of source material. This audit report makes five recommendations to improve NRC's oversight of the export of source material through the creation of an export inspection program, clarification of specific NRC regulations related to exports, and creation of a qualification program for export licensing officers. Agency management did not entirely agree with the report and provided formal comments.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Audit of NRC's Oversight of Security at Decommissioning Reactors	OIG-17-A-09	2/22/17	3	$0	NRC regulates the decommissioning of commercial nuclear power plants. Decommissioning is the process used to safely remove a nuclear power plant from service and reduce residual radioactivity to a level that permits release of the property and termination of its license. NRC has rules governing power plant decommissioning that protects workers and the public during the decommissioning process. For example, NRC regulations require power plant licensees to establish, maintain, and implement an insider mitigation program. In addition, NRC has regulations for the management of worker fatigue. These regulations are designed to ensure licensees effectively manage worker fatigue and provide reasonable assurance that workers are able to safely and competently perform their duties. The audit objective was to determine whether NRC's oversight of security at decommissioning reactors provides for adequate protection of radioactive structures, systems, and components. The audit report makes three recommendations to clarify which fitness-for-duty elements decommissioning licensees must implement to meet the requirements of the insider mitigation program; and to establish requirements for a fatigue management program. Agency management stated their agreement with the findings and recommendations in this report.

Total unimplemented recommendations: 73

DNFSB Unimplemented Recommendations

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of the Defense Nuclear Facilities Safety Board's Information Security Program	DNFSB-16-A-02	10/28/15	1	$0	DNFSB is an independent organization within the Executive Branch that advises the President and the Secretary of Energy on public health and safety issues at Department of Energy (DOE) defense nuclear facilities. DNFSB reviews and evaluates the content and implementation of health and safety standards, as well as other requirements relating to the design, construction, operation, and decommissioning of DOE defense nuclear facilities. DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees. The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations. The audit report made three recommendations to improve DNFSB's information security guidance and Unclassified Controlled Nuclear Information access controls on its internal SharePoint site. DNFSB management stated their general agreement with the report.
2016	Audit of DNFSB's Process for Developing, Implementing, and Updating Policy Guidance	DNFSB-16-A-05	06/29/16	2	$0	In January 2015, a Government Accountability Office (GAO) 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. DNFSB has particularly 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 audit report made six recommendations to improve the processes for developing, implementing, and updating policy guidance. DNFSB management stated their general agreement with the finding and recommendations in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of DNFSB's Oversight of Nuclear Facility Design and Construction Projects	DNFSB-16-A-06	7/6/16	4	$0	Congress created DNFSB to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's (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 National Nuclear Security Administration. 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 audit report made five recommendations aimed at strengthening the efficiency and effectiveness of DNFSB's approach to oversight of defense nuclear facility design and construction projects. DNFSB management agreed with the recommendations, but elected to provide formal comments.
2016	*Cybersecurity Act of 2015* Audit for DNFSB	DNFSB-16-A-07	8/8/16	2	$0	The *Cybersecurity Act of 2015* was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States. Division N, Section 406, of 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. 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 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 personally identifiable information operated by or on behalf of DNFSB. The audit report made two recommendations to bring DNFSB into compliance with the *Privacy Act of 1974* and *E-Government Act of 2002*. DNFSB management stated their agreement with recommendations in this report.

Total unimplemented recommendations: 9

ADDITIONAL IG EMPOWERMENT ACT REPORTING

During this semiannual reporting period, OIG did not substantiate any instance of whistleblower retaliation, and there were no attempts by either NRC or DNFSB to interfere with OIG's independence.

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Document Access Management System
ADM	Office of Administration
AIGA	Assistant Inspector General for Audits
APC	Agency Program Coordinator
ASME	American Society of Mechanical Engineers
CAL	Confirmatory Action Letter
CDBI	Component Design Bases Inspection
CFR	Code of Federal Regulations
CIGIE	Council of Inspectors General on Integrity and Efficiency
CO	Contracting Officer
CoC	Certificate of Compliance
COR	Contracting Officer's Representative
DCAA	Defense Contract Audit Agency
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
DRMA	Division of Resource Management and Administration
DSFG	Dell Services Federal Government
DSFM	Division of Spent Fuel Management
FAEC	Federal Audit Executive Committee
FAIMIS	Financial and Accounting Integrated management Information System
FAR	Federal Acquisition Regulation
FASAB	Federal Accounting Standards Advisory Board
FedRamp	Federal Risk and Authorization Management System
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Integrity Act
FOIA	Freedom of Information Act
FPPS	Federal Personnel Payroll System
FSS	Facility Security Specialist
FY	Fiscal Year
GAO	Government Accountability Office
GLINDA	Global Infrastructure and Development Acquisition
IAM	Issue Area Monitor
IG	Inspector General
IGEA	Inspector General Empowerment Act
IMC	Inspection Manual Chapter
IP	Inspection Procedure
IPERA	Improper Payments Elimination and Recovery Act
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
IPP	Invoice Processing Platform
IT	Information Technology
ITISS	Information Technology Infrastructure Support Services
LAN	Local Area Network
LLRW	Low Level Radioactive Waste
LOOP	Loss of Offsite Power

MC&A	Material Control and Accounting
MD	Management Directive
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NFPA	National Fire Protection Agency
NMMSS	Nuclear Materials Management and Safeguards System
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	Nuclear Regulatory Commission
NRCAR	Nuclear Regulatory Commission Acquisition Regulation
NRO	Office of New Reactors
NRR	Office of Nuclear Reactor Regulation
OCHCO	Office of the Chief Human Capital Officer
OCFO	Office of Chief Financial Officer
OCIO	Office of the Chief Information Officer
OEDO	Office of the Executive Director for Operations
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIP	Office of International Programs
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Officer of Personnel Management
OWFN	One White Flint North
PAR	Performance and Accountability Report
PIV	Personal Identity Verification
PMDA	Program Management, Policy Development and Analysis
PRA	Probabilistic Risk Assessment
PRB	Petition Review Board
RES	Office of Nuclear Regulatory Research
RI	Resident Inspector
RIDM	Risk Informed Decision Making
RISC	Risk Informed Steering Committee
SDP	Significance Determination Process
SGI	Safeguards Information
SLES	Safeguards Information Local Area Network and Electronic Safe
SLR	Service Level Agreement
SNM	Special Nuclear Material
SOC	Security Operations Center
SPAR	Standardized Plant Analysis Risk
SPMS	Space and Property Management System
SRV	Safety Relief Valve
SRI	Senior Resident Inspector
SUNSI	Sensitive, Unclassified Non-Safeguards Information
TTC	Technical Training Center
TWFN	Two White Flint North
WBL	Web-Based Licensing
3WFN	Three White Flint North

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	10-28; 38-39; 42-44
Section 5(a)(2)	Recommendations for corrective action	10-28; 42-44
Section 5(a)(3)	Prior significant recommendations not yet completed	55
Section 5(a)(4)	Matters referred to prosecutive authorities	50, 57
Section 5(a)(5)	Listing of audit reports	51, 52, 58
Section 5(a)(6)	Listing of audit reports with questioned costs or funds put to better use	52
Section 5(a)(7)	Summary of significant reports	10-28; 35-40; 42-44
Section 5(a)(8)	Audit reports — questioned costs	53, 59
Section 5(a)(9)	Audit reports — Funds put to better use	54, 60
Section 5(a)(10)	Audit reports issued before commencement of the reporting period (a) for which no management decision has been made, (b) which received no management comment within 60 days, or (c) with outstanding, unimplemented recommendations, including aggregate potential costs savings	61-78
Section 5(a)(11)	Significant revised management decisions	55
Section 5(a)(12)	Significant management decisions with which OIG disagreed	none
Section 5(a)(13)	FFMIA section 804(b) information	none
Section 5(a)(14-16)	Peer review information	83
Section 5(a)(17)	Investigations statistical tables	49-50; 56-57
Section 5(a)(18)	Description of metrics	57
Section 5(a)(19)	Investigations of senior Government officials where misconduct was substantiated	none
Section 5(a)(20)	Whistleblower retaliation	none
Section 5(a)(21)	Interference with IG independence	none
Section 5(a)(22)(a)	Audits not made public	none
Section 5(a)(22)(b)	Investigations involving senior Government officials where misconduct was not substantiated and report was not made public	35-40

APPENDIX

Peer Review Information

Audits

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 investigative program was peer reviewed most recently by the Tennessee Valley Authority Office of Inspector General. The peer review final report, dated October 5, 2016, reflected that NRC OIG is in full compliance with the quality standards established by the Council of Inspectors General on Integrity and Efficiency and the Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority. These safeguards and procedures provide reasonable assurance of confirming with professional standards in the planning, execution, and reporting of investigations.

On July 12, 2017, NRC OIG issued a final report conveying the results of its peer review of the Federal Housing Finance Agency Office of Inspector General's investigative operations.

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

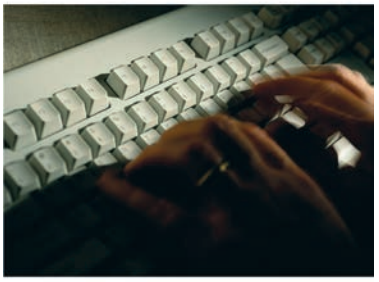
The Hotline Program provides NRC and DNFSB employees, other Government employees, licensee/utility employees, contractors, and the public with a confidential means of reporting suspicious activity concerning fraud, waste, abuse, and employee or management misconduct. Mismanagement of agency programs 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:

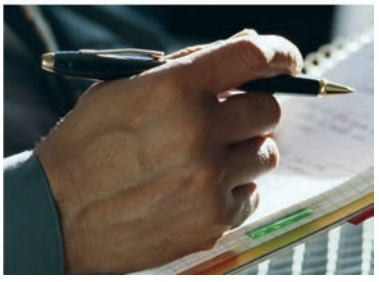
- Contract and Procurement Irregularities
- Conflicts of Interest
- Theft and Misuse of Property
- Travel Fraud
- Misconduct
- Abuse of Authority
- Misuse of Government Credit Card
- Time and Attendance Abuse
- Misuse of Information Technology Resources
- Program Mismanagement

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. 31, No. 1
October 2017

@NRCgov