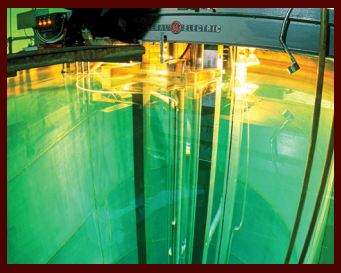
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Office of the Inspector General

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

SEMIANNUAL REPORT TO CONGRESS

October 1, 2017–March 31, 2018



OIG VISION

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

OIG MISSION

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

COVER PHOTOS:

From left to right:

Computer keyboard.
University of Wisconsin-Madison TRIGA Research Reactor.
Nuclear power plant hand scanner.
Low level waste disposal site.

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 October 1, 2017, to March 31, 2018.

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

In addition to issuing several legislatively mandated audits and reports pertaining to NRC and DNFSB information technology security spending data accuracy, management and performance challenges, and financial statements, we issued reports intended to strengthen NRC's oversight of decommissioning financial instruments, security of research and test reactors, and how effectively it manages personally identifiable information.

During this semiannual reporting period, we issued 13 program and financial audit reports and evaluations and, analyzed 2 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 safety, security, and corporate management programs. OIG also opened 20 investigations, and completed 15 cases. Three of the open cases were referred to the Department of Justice, and 47 allegations were referred to agency management for action.

NRC 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. I would like to acknowledge our auditors, investigators, and support staff for their commitment to the mission of this office.

Finally, our success would not be possible without the collaborative efforts between OIG staff and NRC and DNFSB staff to address OIG findings and implement corrective actions in a timely manner. I 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

Highlights . . . v
- Audits . . . v
- Investigations . . . ix

Overview of NRC and OIG . . . 1
- NRC's Mission . . . 1
- OIG History, Mission, and Goals . . . 2
  - OIG History . . . 2
  - OIG Mission and Goals . . . 3

NRC OIG Programs and Activities . . . 5
- Audit Program . . . 5
- Investigation Program . . . 6
- OIG General Counsel Regulatory Review . . . 7
- Regulatory Review . . . 7

NRC Management and Performance Challenges . . . 10

Audits . . . 11
- Audit Summaries . . . 11
- Audits in Progress . . . 19

NRC Investigations . . . 27
- Investigative Case Summaries . . . 27

Defense Nuclear Facilities Safety Board . . . 32

DNFSB Management and Performance Challenges . . . 33

DNFSB Audits . . . 34
- Audit Summaries . . . 34
- Audits in Progress . . . 38

DNFSB Investigations . . . 40
- Investigative Case Summaries . . . 40

Summary of OIG Accomplishments at NRC . . . 43
- NRC Investigative Statistics . . . 43
- NRC Audit Listings . . . 45
- NRC Audit Resolution Activities . . . 47

Summary of OIG Accomplishments at DNFSB . . . 50
- DNFSB Investigative Statistics . . . 50
- DNFSB Audit Listings . . . 52
- DNFSB Audit Resolution Activities . . . 53

Unimplemented Audit Recommendations . . . 55
- NRC . . . 55
- DNFSB . . . 79

Additional IG Empowerment Act Reporting . . . 82

Abbreviations and Acronyms . . . 83

Reporting Requirements . . . 86

Appendix . . . 87



Resident Inspector at Calvert Cliffs Nuclear power plant.

HIGHLIGHTS

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

NRC AUDITS

- As part of its regulatory function, NRC issues licenses for nuclear materials and regulates the decommissioning of material sites. Material licensees must provide financial assurance for decommissioning costs before they receive nuclear material or begin site operations. They must also maintain that funding throughout the duration of site operations. In June 2016, OIG issued an audit report on NRC's Decommissioning Funds Program. During that audit, OIG auditors were not able to examine the original financial instruments maintained by the agency because the safe containing the instruments was inaccessible. As a result, the audit had a scope limitation, which informed the decision to perform this audit. The audit objectives were to determine whether (1) NMSS' Inventory 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. The audit report made one recommendation to update guidance to reflect current practices.

- The *Atomic Energy Act of 1954*, as amended, Section 104.c, authorizes the licensing of utilization and production facilities useful in the conduct of research and development activities. The act also stipulates that the Commission should impose only such minimum amount of regulation sufficient to promote the common defense and security and to protect the health and safety of the public while permitting conduct of widespread and diverse research and development. NRC licenses 31 currently operating research and test reactors (RTRs), which contribute to research in diverse fields such as physics, medicine, archeology, and materials science. RTRs use a limited amount of radioactive material in their diverse designs and all are designed to be inherently safe and resistant to unintentional or intentional mis-operation. The audit objective was to determine whether NRC provides adequate security oversight of research and test reactors. OIG found that NRC's security oversight of research and test reactors takes into account the mission of permitting research while ensuring that licensee activities promote secure operations. Therefore, OIG made no recommendations.

- On July 6, 2017, OIG identified and accessed an employee's bank account information on a personal check that was scanned and saved to the agency's shared "S" drive. After finding that the sensitive information was not protected by access controls, OIG reviewed the shared "S" drive for Personally Identifiable Information (PII) and identified a folder dated 2011, which had 35 subfolders for several offices in the agency. Of the 35 subfolders, 17 contained PII without appropriate access controls. The objective was to assess how NRC effectively manages and protects PII stored

on the shared "S" drive in accordance with Federal regulations. This report made four recommendations to improve NRC's procedures and process for managing and protecting PII stored on the shared "S" drive.

- The Chief Financial Officers Act of 1990, as amended, requires the Inspector General (IG) or an independent external auditor, as determined by the IG, to annually audit NRC's financial statements in accordance with applicable standards. In compliance with this requirement, OIG retained Acuity Consulting, Inc., to conduct this annual audit. The audit included, among other things, obtaining an understanding of NRC and its operations, including internal control over financial reporting; evaluating the design and operating effectiveness of internal control and assessing risk; and testing relevant internal controls over financial reporting. The audit also examined, on a test basis, evidence supporting the amounts and disclosures in the financial statements, assesses the accounting principles used, and evaluates the significant estimates made by agency management as well as the overall financial statement presentation. The resulting report contained unmodified opinions on the agency's financial statements and internal controls and did not identify any instances of non-compliance regarding the agency's compliance with laws and regulations.

- Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Governmentwide data definition standards issued by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury). Treasury displayed spending data on the USAspending.gov Web site. A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAO) were required to provide assurance over the quality of the data submitted and begin reporting fiscal year 2017 second quarter data for public display by May 2017. The DATA Act also requires OIGs to submit this audit report to Congress and the public. The audit objective was to assess (1) the completeness, timeliness, quality, and accuracy of FY 2017 second quarter financial and award data submitted for publication on USAspending.gov and (2) NRC's implementation and use of the Governmentwide financial data standards established by OMB and Treasury. This report made two recommendations to improve NRC's documentation of policies and procedures for the SAO assurance statement, and to improve the agencies policies and procedures governing Broker[1] submission warning messages.

[1] *A key component of the reporting framework laid out in the DATA Act Schema is the DATA Act Broker, a system of software applications designed to standardize data formatting and assist reporting agencies in validating data prior to submitting it to Treasury. Treasury developed the broker using a process that emphasizes frequent user feedback so that changes can be incorporated into the prototype early and often.*

- 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 OIG or by an independent external auditor. OMB requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool. The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017. This report made seven recommendations to improve the agency's implementation of FISMA 2014 requirements.

  In addition, OIG issued a report summarizing the findings and recommendations of all OIG FISMA 2014 evaluations conducted during FY 17 (at headquarters, the four regional offices, and the Technical Training Center); the summary report does not offer any additional recommendations.

- In accordance with the Reports Consolidation Act of 2000, the Inspector General identified what he considered the most serious management and performance challenges facing NRC as of October 1, 2017. These management and performance challenges are directly related to NRC's mission areas (i.e., commercial nuclear reactors and nuclear materials), security, information technology and information management, financial programs, and administrative functions. OIG's work in these areas indicates that while program improvements are needed, NRC is continually making progress to address OIG recommendations and improve the efficiency and effectiveness of its programs. This report contained no recommendations.

DEFENSE NUCLEAR FACILITIES SAFETY BOARD AUDITS

- The Accountability for Tax Dollars Act of 2002 requires the IG or an independent external auditor, as determined by the IG, to annually audit DNFSB's financial statements to determine whether the agency's financial statements are in accordance with applicable standards. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management as well as evaluating the overall financial statement presentation. The objective of a financial statement audit is to determine whether the audited entity's financial statements are free of material misstatement. The auditors expressed an unmodified opinion on the agency's FY 2017 and FY 2016 financial

statements and an unmodified opinion on DNFSB's internal controls over financial reporting, and found no reportable instances of noncompliance with laws and regulations. Therefore, no recommendations were made.

- Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Governmentwide data definition standards issued by the OMB and the Department of the Treasury. Spending data are displayed on the USAspending.gov Web site. A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAOs) are required to provide assurance over the quality of the data submitted and begin reporting fiscal year 2017 second quarter data for public display by May 2017. The DATA Act also requires OIGs to submit this audit report to Congress and the public. The audit objective was to assess the (1) completeness, timeliness, quality, and accuracy of fiscal year 2017 second quarter financial and award data submitted for publication on USAspending.gov, and (2) DNFSB's implementation and use of the Governmentwide financial data standards established by OMB and Treasury. The audit report makes a recommendation to improve DNFSB's documentation of policies and procedures for the SAO statement of assurance, and to improve DNFSB's internal policies and procedures governing submissions under the DATA Act.

- 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 OIG or by an independent external auditor. OMB requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool. The evaluation objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017. The evaluation report made seven recommendations to improve DNFSB's implementation of FISMA 2014.

- In accordance with the Reports Consolidation Act of 2000, the Inspector General identified what he considered the most serious management and performance challenges facing DNFSB as of October 1, 2017. These management and performance challenges are directly related to DNFSB's organizational culture and climate, security, administrative functions, and technical programs. This report contains no recommendations to imporve DNFSB's implementation of FISMA 2014.

NRC INVESTIGATIONS

- OIG conducted an investigation into an allegation that a former NRC Branch Chief, now employed at a nuclear power plant (NPP), was working on the same issues at the NPP that he was assigned while working at the NRC, potentially a violation of ethics rules. Further, it was alleged that an NRC Division Director was having private discussions with licensee executives regarding NRC issues that should have been coordinated with NRC licensing staff.

- OIG conducted two investigations into alleged employee misuse of agency-issued computers. One investigation was based on a reported concern regarding the employee's unusual after-hours activity at NRC headquarters. The other investigation was initiated based on agency network logs that indicated the employee was attempting to visit various sexually explicit Web sites.

- OIG conducted an investigation into an allegation that someone was impersonating an NRC official to obtain citizens' personal information (and money) in exchange for alleged grants from the NRC. The unknown individual(s) communicated with the citizens via text through Facebook Messenger. In reviewing the information, OIG identified that an individual, claiming to be "Larry Mankel," had created a Facebook page that contained photographs of a U.S. Congressman.

- OIG conducted an investigation into an allegation that an NRC senior official committed time card fraud when he instructed an employee to work from home for approximately 4 months, instead of using sick leave, due to a family medical issue.

- OIG conducted an investigation into an allegation that an NRC employee was sexually harassed by an NRC manager.

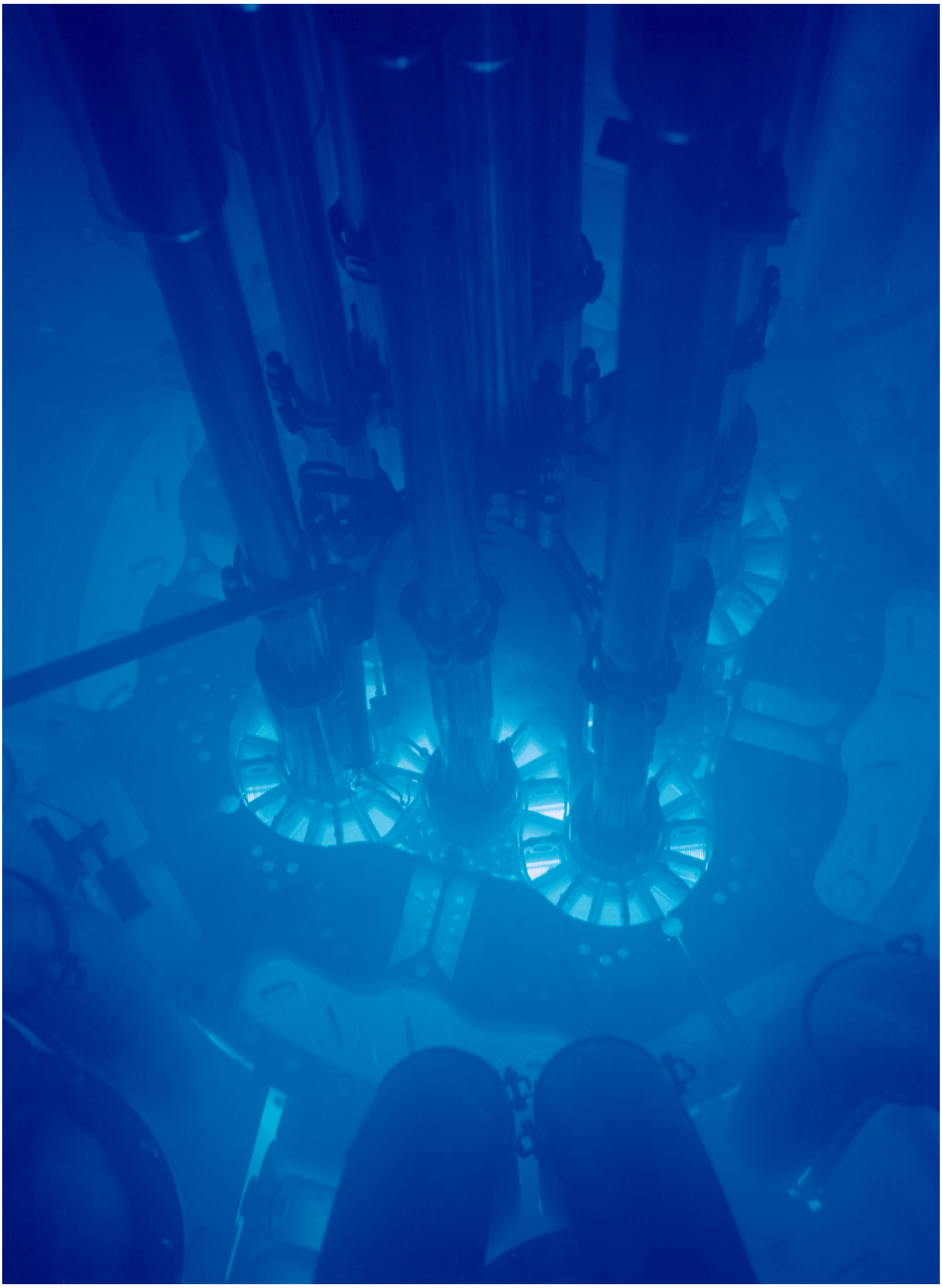
DNFSB INVESTIGATIONS

- OIG conducted an investigation into an allegation that the former Acting General Counsel had acted in an unethical manner by providing misleading information to the Board, which in turn was to be provided to the Government Accountability Office (GAO), in response to a GAO audit recommendation.

- OIG conducted an investigation into an allegation that DNFSB mismanaged an effort to procure a Correspondence Management System software program that could have been developed with existing software tools at a lower cost to the Federal Government.



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.

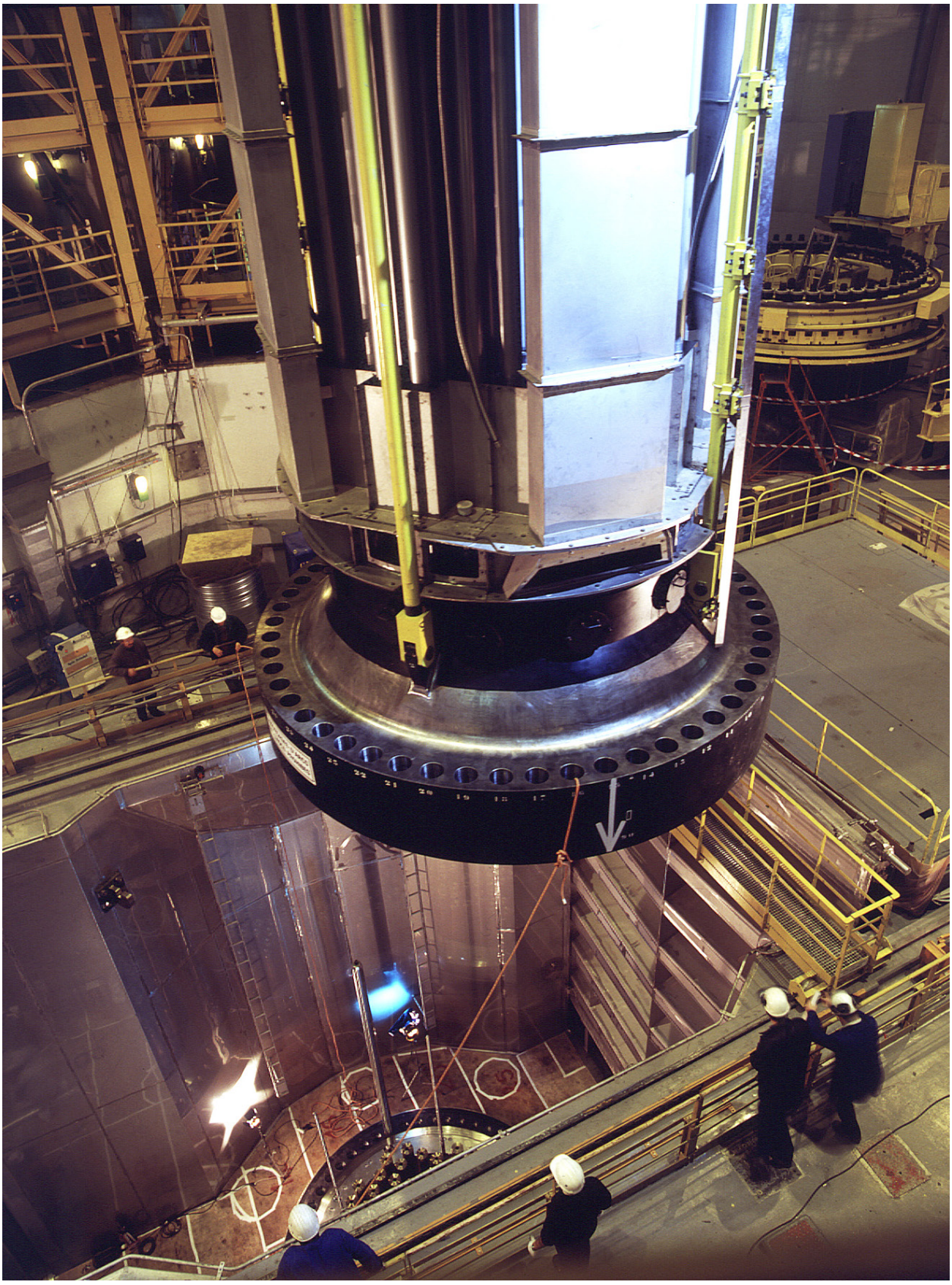
OIG is committed to ensuring the integrity of NRC programs and operations. Developing an effective planning strategy is a critical aspect of accomplishing this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, OIG developed a Strategic Plan that 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 – An initial phase of the audit process is used to gather information on the agency's organization, programs, activities, and functions. An assessment of vulnerable areas determines whether further review is needed.

- Fieldwork – Detailed information is obtained to develop findings and support conclusions and recommendations.

- Reporting – The auditors present the information, findings, conclusions, and recommendations that are supported by the evidence gathered during the survey and fieldwork 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 – 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 and contractors, interfacing with the Department of Justice on OIG-related criminal and civil matters, and coordinating investigations and other OIG initiatives with Federal, State, and local investigative agencies and other OIGs. Investigations may be initiated as a result of allegations or referrals from private citizens; licensee employees; NRC employees; Congress; other Federal, State, and local law enforcement agencies; OIG audits; the OIG Hotline; and OIG initiatives directed at areas bearing a high potential for fraud, waste, and abuse.

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

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

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

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 October 1, 2017, to March 31, 2018, OIG reviewed a variety of agency documents including Commission papers (SECYs), Staff Requirements Memoranda, and Federal Register Notices, Management Directives, Directives, Operating Procedures and statutes.

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

NRC

- Overall, draft revision to Management Directive and Handbook (MD) 8.13, "Reactor Oversight Process [ROP]," provided a clear and succinct description of the purpose, objectives, and responsibilities for execution of the agency's reactor oversight program. OIG comments focused on clarification of terms to aid in application of the cited provisions. Also, one comment identified an issue related to descriptions of NRC's objectives in several listed areas associated with Reactor Safety where the term "adequate" was used instead of the generally accepted phrase "adequate protection" in its description of the NRC's objective related to assessing the actions of the licensee's emergency plan. We also offered substantive advice with regard to the section on "Changes to the ROP," suggesting changing the use of the word "should" in the process of identifying changes that need Commission approval. OIG's comment pointing out that if Commission approval for important changes to the ROP is to be a process requirement, then the more appropriate action word would be "shall."

- Revised MD and Handbook 5.6, "Integrated Materials Performance Evaluation Program (IMPEP)," reflects the merger and revision of the Agreement State Policy Statement and incorporates recommendations from two working group reports. OIG comments focused on evaluation frequency, noting that the NRC reviews, through the IMPEP process, the performance of the NRC and Agreement State materials programs on a periodic basis. The schedule for conducting each review is developed by the Office of Nuclear Material Safety and Safeguards (NMSS). IMPEP reviews of the NRC and Agreement State materials programs are typically scheduled every 4 years; however, IMPEP reviews may be extended to 5 years if the materials program has had two consecutive IMPEP reviews with all indicators found satisfactory. The interval between IMPEP reviews may be shortened due to performance weaknesses and at the direction of the Management Review Board (MRB), based on the review team's recommendation, or other information obtained during the MRB meeting or review period. We commented that although IMPEP assesses three of NRC's regional offices, it does not review headquarters. Therefore, in the Handbook, "regional offices (I, III, and IV)" should be added after NRC to correctly identify the offices reviewed.

- Additional clarification was suggested for Draft MD and Handbook 10.49, "Student Loan Repayment Program." Specifically, Directive Section I.C. (d) and Section I.C. (e) appeared contradictory. I.C.(d) provides, "An employee who fails to complete the period of employment established under a service agreement is indebted to the Federal Government and must reimburse the NRC for all student loan repayment benefits received (not on a pro rata basis) for any service agreement not completed. However, Section I.C. (e) indicates, "An employee who is involuntarily separated for reasons other than misconduct or unacceptable performance or transfers to another Federal agency without a break in service, is not indebted to the Federal Government if his or her service with the NRC terminates before the date specified in the service agreement." As written, it was not clear that "involuntary" pertains to the word "transfers." We suggested that if "involuntary" applies to both parts of the sentence, reword I.C. (e) to state: "An employee who is involuntarily separated or who is transferred to another Federal agency without a break in service for reasons other than misconduct or unacceptable performance, is not indebted to the Federal Government if his or her service with the NRC terminates before the date specified in the service agreement."

- With regard to Draft MD and Handbook 10.51, "Recruitment, Relocation, and Retention Incentives," OIG suggested that Section II.A.3 of Handbook 10.51 offer either (1) clarifying information or (2) a referral to a source with clarifying information on the "mileage test for permanent change-of-station moves." Section II.A.3 states, "If an employee does not meet eligibility criteria to receive regular relocation benefits (e.g., the employee's new duty station does not meet the mileage test for permanent change-of-station moves, which is different than the relocation incentive mileage test), then he or she …would… not be eligible for a relocation incentive." Without clarifying information, it is difficult for the reader to reconcile this section with the preceding section, II.A.2, which states, "In most cases, an employee must be

relocating to a worksite 50 miles or more from the worksite of the position held immediately before the move." OIG noted it would be helpful for NRC staff to have access to sufficient information to reconcile these two paragraphs.

DNFSB

- For DNFSB draft Directive -125.1, "Telework Program," OIG suggested a change on Page 3, section 6 (Requirements), subsection B., to change "absent without permission" to "Absence without leave (AWOL)," so as to be consistent with Office of Personnel Management terminology.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission* as of October 1, 2017 *(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-18-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC, https://www.nrc.gov/docs/ML1729/ML17291A011.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. Most of these audits and evaluations are summarized below.

AUDIT SUMMARIES

Audit of NRC's Decommissioning Financial Assurance Instrument Inventory

OIG Strategic Goal: Corporate Management

As part of its regulatory function, NRC issues licenses for nuclear materials and regulates the decommissioning of material sites. Material licensees must provide financial assurance for decommissioning costs before they receive nuclear material or begin site operations. They must also maintain that funding throughout the duration of site operations.

In June 2016, OIG issued an audit report on NRC's Decommissioning Funds Program. During that audit, OIG auditors were not able to examine the original financial instruments maintained by the agency because the safe containing the instruments was inaccessible. As a result, the audit had a scope limitation which informed the decision to perform this audit.

The audit objectives were to determine whether (1) the Office of Nuclear Material Safety and Safeguards Inventory 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.

Audit Results

NRC properly safeguards the original signed decommissioning financial instruments in a fire-proof safe; however, opportunities for improvement exist in the following areas:

- The Inventory List contains incomplete information and does not accurately account for the financial instruments in the safe. For example, auditors found that several financial instruments had missing or inaccurate dollar amounts on the Inventory List and many of the instruments were missing or had inaccurate issuance dates. OIG also identified four licensees with inadequate financial assurance in the safe, and three folders where the license had been terminated.

- NRC's evaluations of financial instruments are inconsistently documented and there is no requirement for followup to ensure identified discrepancies are corrected. None of the supporting documentation provided to OIG auditors indicated what steps were completed or what, if any discrepancies were identified. Consequently, OIG could not follow up to determine if identified discrepancies were corrected because there was no documented support showing specific detail of the discrepancies.

- There is no filing methodology to ensure files are consistently organized. Auditors found inconsistent filing methods, duplicative an inaccurate entries on the inventory list, and no hardcopy of the inventory list in the safe.

These weaknesses occurred because agency guidance related to oversight of the financial instruments is outdated and does not reflect actual practices, segregation of duties is not maintained, and there is no detailed procedural guidance for office evaluations. As a result, there is an increased risk documents will not be timely identified to draw upon the financial instrument needed to fund the standby trust in an efficient and effective manner. Subsequently, this could result in a potential delay in funding availability for decommissioning.

(Addresses Management and Performance Challenge # 5)

Audit of NRC's Security Oversight of Research and Test Reactors

OIG Strategic Goal: Security

The *Atomic Energy Act of 1954*, as amended, Section 104.c, authorizes the licensing of utilization and production facilities useful in the conduct of research and development activities. The act also stipulates that the Commission should impose only such minimum amount of regulation sufficient to promote the common defense and security and to protect the health and safety of the public while permitting conduct of widespread and diverse research and development.

NRC licenses 31 currently operating Research and Test Reactors (RTR), which contribute to research in diverse fields such as physics, medicine, archeology, and materials science. RTRs use a limited amount of radioactive material in their diverse designs and all are designed to be inherently safe and resistant to unintentional or intentional mis-operation.

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

Audit Results:

NRC's security oversight for RTRs is designed to meet the requirements established in the AEA to provide regulations, guidance, and oversight for RTR licensees as they conduct research activities. Oversight is structured around the risks associated with the strategic significance of the special nuclear material, a licensee may possess and is designed to be site-specific. The RTR Oversight Branch within NRC's Office of Nuclear Reactor Regulation has taken steps to increase effectiveness, even as security requirements have changed with the threat environment. However, the oversight program is dynamic and will require continued balancing of resources going forward.

(Addresses Management and Performance Challenge # 3)

Evaluation of NRC's Shared "S" Drive

OIG Strategic Goal: Security

OIG has issued two reports, in June 2006 and July 2011, that identified issues with NRC's protection of Personally Identifiable Information (PII). However, on July 6, 2017, OIG identified and accessed an employee's bank account information on a personal check that was scanned and saved to the agency's shared "S" drive. After finding that the sensitive information was not protected by access controls, OIG reviewed the shared "S" drive for PII and identified a folder dated 2011, which had 35 subfolders for several offices in the agency. Of the 35 subfolders, 17 contained PII without appropriate access controls.

The objective was to assess how NRC effectively manages and protects PII stored on the shared "S" drive in accordance with Federal regulations.

Evaluation Results:

This evaluation identified two opportunities for improvement on how NRC manages and protects PII stored on the shared "S" drive.

NRC staff store PII on the shared "S" drive without adding appropriate access controls because NRC guidance and annual PII training do not provide specific procedures and training on how to effectively protect PII stored on the shared "S drive."

Additionally, NRC management is required to review the agency shared "S" drive to identify and eliminate PII at least annually. However, NRC has not reviewed the shared "S" drive for PII since 2011 because NRC management has not applied the necessary resources to perform this effort.

As a result, PII stored on a shared "S" drive without safeguards may be compromised or vulnerable to unauthorized disclosure, thereby putting individuals at risk of identity theft.

(Addresses Management and Performance Challenge # 3)

Results of the Audit of the United States Nuclear Regulatory Commission's Financial Statements for FY 2017

OIG Strategic Goal: Corporate Management

The Chief Financial Officers Act of 1990, as amended, requires the IG or an independent external auditor, as determined by the IG, to annually audit NRC's financial statements to determine whether the agency's financial statements are free of material misstatement. The audit, conducted by Acuity Consulting, Inc., under a contract with OIG, includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. It also includes assessing the accounting principles used and significant estimates made by agency management as well as evaluating the overall financial statement presentation. In addition, the audit evaluated the effectiveness of internal controls over financial reporting and the agency's compliance with laws and regulations.

The audit objectives were to

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

Audit Results:

Opinion: The auditors expressed an unmodified opinion on the agency's FY 2017 financial statements.

Internal Controls: The auditors expressed an unmodified opinion on the agency's internal controls.

Compliance with Laws and Regulations: The auditors found no reportable instances of noncompliance with laws and regulations.

(Addresses Management and Performance Challenge # 5)

Audit of NRC's Compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act)

OIG Strategic Goal: Corporate Management

Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Government wide data definition standards issued by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury). Spending data are displayed on the USAspending.gov Web site.

A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAOs) are required to provide assurance over the quality of the data submitted and begin reporting fiscal year (FY) 2017 second quarter data for public display by May 2017. The DATA Act also requires OIGs to submit this audit report to Congress and the public.

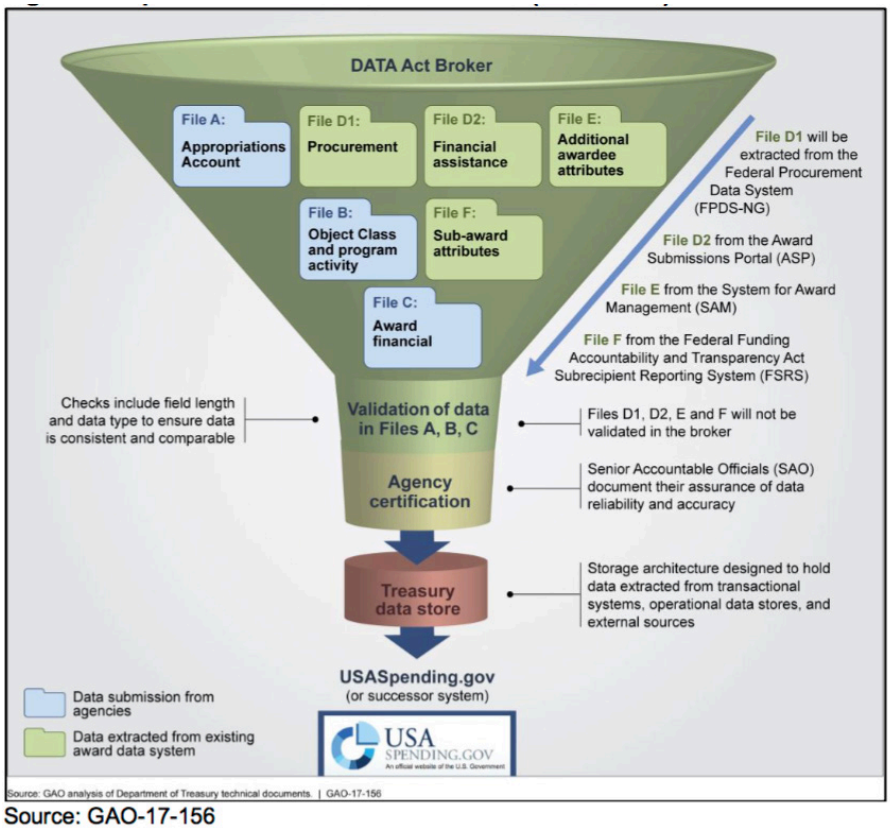
The audit objectives were to assess the (1) completeness, timeliness, quality, and accuracy of FY 2017, second quarter financial and award data submitted for publication on USAspending.gov, and (2) NRC's implementation and use of the Governmentwide financial data standards established by OMB and Treasury.

Audit Results:

NRC submitted the required FY 2017, second quarter financial and award data for publication on USAspending.gov on time and within acceptable error rate parameters. However, the completeness, quality, and accuracy of the data submitted did not always comply with applicable laws, regulations, and policies. Specifically, OIG tested the data submitted by NRC for completeness and accuracy. OIG found a 2-percent overall error rate percentage for both. NRC's result for data timeliness was zero errors. NRC's submitted information generally conformed to OMB and Treasury standards. However, improved controls are needed over the resolution and acceptance of Broker warning messages, and over the agency's file linkage testing processes for DATA Act submissions.

Additionally, the agency's SAO assurance statement lacked explanations for data misalignments and Broker[2] warnings and did not clearly indicate the extent of testing over file linkages.

[2]A key component of the reporting framework laid out in the DATA Act Schema is the DATA Act Broker, a system of software applications designed to standardize data formatting and assist reporting agencies in validating data prior to submitting it to Treasury. Treasury developed the broker using a process that emphasizes frequent user feedback so that changes can be incorporated into the prototype early and often.



Source: GAO-17-156

(Addresses Management and Performance Challenge # 5)

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017

OIG Strategic Goal: Security

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 OIG or by an independent external auditor. Office of Management and Budget (OMB) memorandum M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements, dated October 16, 2017, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The evaluation objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017.

Evaluation Results:

NRC has made significant improvements in the effectiveness of its information technology security program, and continues to make improvements in performing continuous monitoring activities. However, the independent evaluation identified weaknesses in the areas of outdated security program documentation; latent performance of continuous monitoring activities; and irregularly reviewed and updated security categorizations, contingency plans, and business impact assessments. These weaknesses were caused by

- Office reorganizations that left some responsibilities unaccounted for.
- Outdated guidance.
- Inattention to maintaining IT security program documentation.
- Insufficiently detailed Cybersecurity Risk Dashboard metrics.
- Lack of detailed procedures.

It is important for NRC staff to effectively implement the NRC IT security program to confirm it aligns with agency and Federal policies, and applicable regulations and laws. Furthermore, a continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

(Addresses Management and Performance Challenge # 4)

Summary Report of FISMA Evaluations Conducted in Fiscal Year 2017

OIG Strategic Goal: Security

During FY 2017, OIG conducted six *Federal Information Security Modernization Act of 2014* (FISMA 2014) evaluations of NRC headquarters, the four NRC regional offices, and NRC's Technical Training Center (TTC). FISMA 2014 outlines the information security management requirements for Federal agencies, which includes an independent evaluation of the agency's information security program and practices to determine their effectiveness.

Each regional office and the TTC is responsible for implementing NRC's information security program at their location. In order to evaluate the effectiveness of NRC's information security program and practices across the entire agency, NRC OIG conducts periodic independent evaluations at the regional offices and TTC.

The objective of this report was to summarize the findings and recommendations of the six FISMA evaluations conducted in FY 2017.

Number of Findings	Topic	Recommendations
3	IT documentation was not up-to-date.	3 (HQ) 2 (Region IV)
2	Vulnerability scans identified high risk and moderate risk findings.	1 (Region I) 1 (Region IV)
1	Continuous monitoring activities were not performed as required.	4 (HQ)
1	Backups were not being performed on the local backup server.	0 (Region II)
1	Inventory was not updated to reflect new components.	1 (TTC)
1	One laptop with a lapsed ATO and approximately 80 other laptops and standalone desktops were never issued an ATO.	2 (TTC)

Source: OIG Analysis of FISMA Reports Conducted in FY 2017.

Management Issue	Topic	Recommendations
1	Links on the internal Web site do not lead to the most current division instructions that have final approval in ADAMS.	0 (Region III)

Source: OIG Analysis of FISMA Reports Conducted in FY 2017.

Evaluation Results:

Overall, the 6 FY 2017 FISMA evaluations at headquarters, the regions, and TTC resulted in 9 findings and 14 recommendations to address those findings. There also was one management issue identified. Because this is a summary report of all FISMA evaluations conducted at NRC headquarters and regional offices for FY 2017, there are no new recommendations in this report. The chart below identifies the number of findings, general nature of the findings, and the number of recommendations issued for headquarters, each region and TTC.

(Addresses Management and Performance Challenge # 3)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC in Fiscal Year 2018

OIG Strategic Goal: Corporate Management

In accordance with the Reports Consolidation Act of 2000, the IG identified what he considered the most serious management and performance challenges facing NRC as of October 1, 2017. These management and performance challenges are directly related to NRC's mission areas (i.e., commercial nuclear reactors and nuclear materials), security, information technology and information management, financial programs, and administrative functions. OIG's work in these areas indicates that while program improvements are needed, NRC is continually making progress to address OIG recommendations and improve the efficiency and effectiveness of its programs.

The following six challenges represent what OIG considers to be inherent and continuing program challenges relative to maintaining effective and efficient oversight and internal controls:

1. Regulation of nuclear reactor safety programs.
2. Regulation of nuclear materials and radioactive waste programs.
3. Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.
4. Management of information technology and information management.
5. Management of financial programs.
6. Management of administrative functions.

(Addresses All Management and Performance Challenges)

Audits in Progress

Audit of NRC's Force-on-Force Security Inspections of Fuel Cycle Facilities

OIG Strategic Goal: Security

NRC requires robust security at the Nation's nuclear facilities. To achieve this, the Office of Nuclear Security and Incident Response has the responsibility for assessing the development and implementation of security programs at various nuclear facilities throughout the United States including fuel cycle facilities. Each licensee is required to provide "defense in depth" at these facilities. An essential part of the

NRC oversight for security at fuel cycle facilities is the Force-on-Force security inspection. This inspection is conducted at least once every 3 years for several weeks.

Force-on-Force exercises are designed to test various elements of the facility's security program in order to determine if the licensee has the ability to defend the facility against the design basis threat for theft or diversion and if the exercise has been designed in accordance with the agency's regulations.

The audit objective is to determine the effectiveness of the Force-on-Force program for fuel cycle facilities.

(Addresses Management and Performance Challenge #3)

Audit of NRC Code Sharing

OIG Strategic Goal: Security

NRC uses computer codes to model and evaluate fuel behavior, reactor kinetics, thermal-hydraulic conditions, severe accident progression, time-dependent dose for design-basis accidents, emergency preparedness and response, health effects, and radionuclide transport, during various operating and postulated accident conditions. Results from applying the codes support decisionmaking for risk-informed activities, review of licensees' codes and performance of audit calculations, and resolution of other technical issues. NRC's Office of International Programs is responsible for NRC code sharing and distribution. This program involves the signing of international agreements that contemplate code sharing activities. These activities provide NRC codes to foreign counterparts in exchange for data related to NRC code application, verification, and validation.

The majority of the codes have no relevance to U.S. foreign policy; however, some codes are relevant to dealing with the production of special nuclear material (SNM) that are transferred to certain countries. In 2011, DOE revised Title 10 CFR Part 810 to formalize an agreed upon transparent coordination process related to NRC code sharing activities with foreign counterparts. This enhanced coordination includes exchange with certain foreign regulators, designated foreign entities and multinational entities (foreign counterparts).

DOE involvement with regard to code sharing is based on an NRC cross-check review of the sensitivity of the code and the country. "Sensitive codes" refer to codes that have the potential to be useful for formulating calculations that support the production of SNM and could be of interest to an adversary of the United States. Based on the NRC's cross-check review, NRC will (1) distribute the code pursuant to an existing Umbrella Arrangement or stand-alone agreement; or (2) will notify, consult with, or request review by a DOE contact. The audit objective is to determine if NRC and DOE interagency coordination and transparency will enhance the overall coordination of the code sharing activities.

(Addresses Management and Performance Challenge #3)

Evaluation of Headquarters Operations Center Staffing

OIG Strategic Goal: Security

The NRC Headquarters Operations Center is the primary center of communication and coordination among the NRC, its licensees, State and Tribal agencies, and other Federal agencies, regarding operating events involving nuclear reactors or materials. Located in Rockville, MD, the Operations Center is staffed 24 hours a day by employees trained to receive and evaluate event reports and coordinate incident response activities.

The evaluation objective is to determine whether NRC staffing of the Headquarters Operations Center adequately supports necessary response and coordination activities.

(Addresses Management and Performance Challenge #3)

Evaluation of NRC's Efforts to Secure Its Network Perimeter

OIG Strategic Goal: Security

NRC OIG contracted Carson, Inc. to determine the effectiveness of NRC's efforts to secure its network perimeter, including conducting an external vulnerability assessment and penetration test, hereafter referred to as security testing.

Carson, Inc. used open source, proprietary tools, and methodologies used by "hackers" and security auditors to conduct the security testing, with the exception of those tools and techniques known by Carson, Inc. to cause denial of service. Carson, Inc. emulated the tactics used by an outside attacker, with knowledge of the NRC's infrastructure, whose goal is to attempt to breach the security of network and computer systems. External testing took place across the Internet from the Carson, Inc. security testing lab physically located in Bethesda, Maryland.

The security testing occurred in three phases

- Initial setup.
- Information assurance activity.
- Review, analysis, and reporting.

The objective of the security testing was to identify potential vulnerabilities in NRC's network perimeter that may be vulnerable to exploitation by threats through the Internet.

(Addresses Management and Performance Challenge #3)

Audit of NRC's Process for Developing and Coordinating Research Plans

OIG Strategic Goal: Safety

NRC's regulatory research program addresses issues in nuclear reactors, nuclear materials, and radioactive waste. The Office of Nuclear Regulatory Research is a technical support office that supplies technical tools, analytical models, analyses, experimental data, and technical guidance to support NRC's regulatory programs and decisions.

Agency research projects are conducted in accordance with user needs, research assistance requests, and research plans. User needs and research assistance requests focus on fulfilling specific needs for research in support of licensing and other regulatory functions. In contrast, a research plan typically integrates and coordinates work from a variety of sources including user requests, long-term research, and support for codes and standards development. Research plans require significant resources and document multiple facets of a regulatory issue with the main purpose of gaining a sound understanding of the underlying technical bases to aid regulatory decisionmaking and promulgating regulations and guidance.

Based on recommendations from Project Aim, the agency is working to enhance its effectiveness, efficiency, and agility. The process for developing and coordinating research plans should be consistent with these objectives to further NRC's mission on broad, complex, and crosscutting technical issues and challenges that have regulatory implications.

The audit objective is to assess the effectiveness and efficiency of the development, use, and coordination of research plans.

(Addresses Management and Performance Challenge #2)

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)

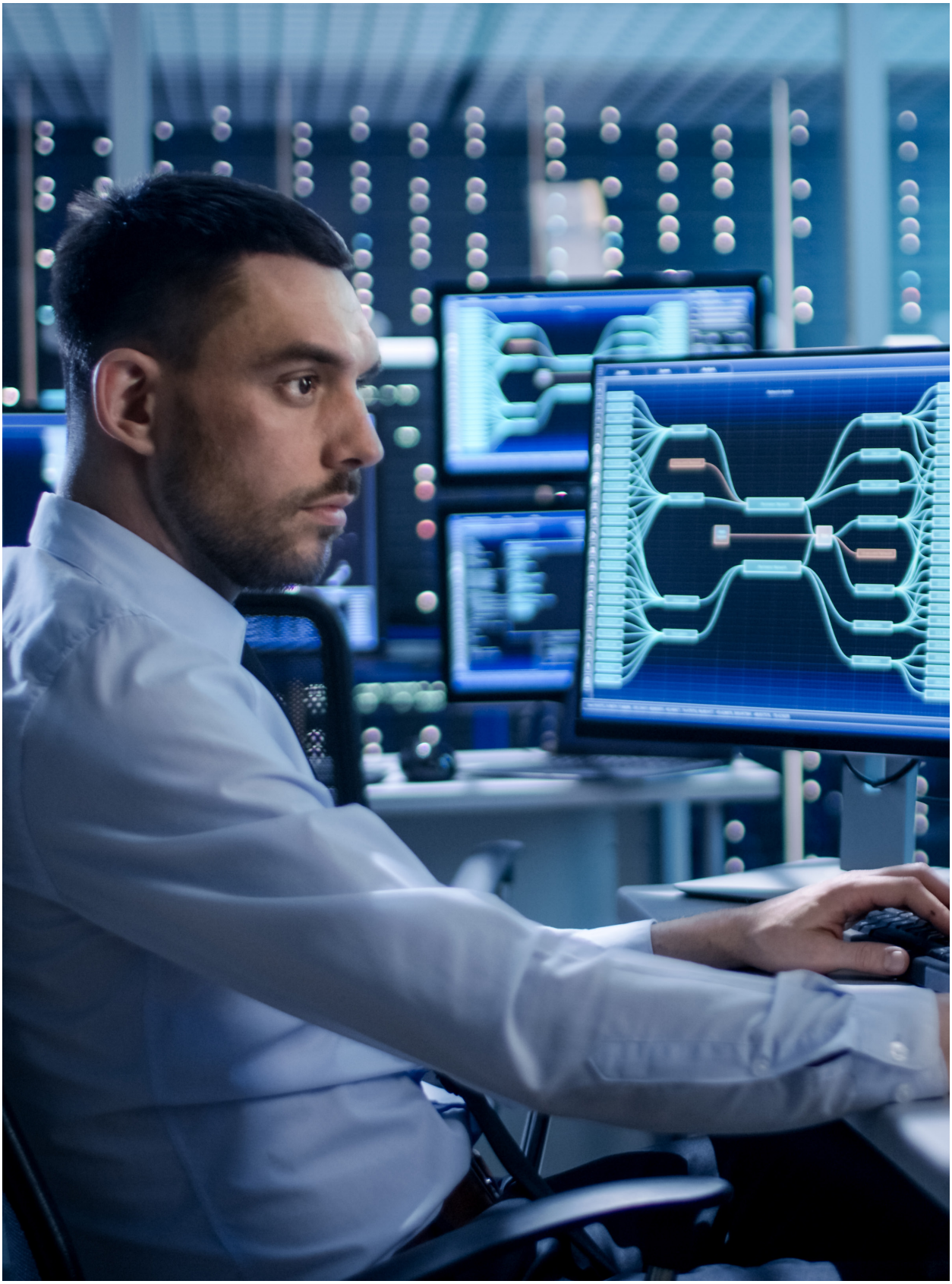
Audit of NRC's Special and Infrequently Performed Inspections

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, 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)



Cyber security agent.

NRC INVESTIGATIONS

During this reporting period, OIG received 125 allegations, initiated 18 investigations, and closed 13 cases. Of the 13 closed cases, 2 resulted in issued reports.

Investigative Case Summaries

Alleged Conflict of Interest and Ethics Violations

OIG Strategic Goal: Corporate Management

OIG conducted an investigation into an allegation that a former NRC Branch Chief, now employed at a nuclear power plant (NPP), was working on the same license amendment issues at the NPP that he was assigned while working at the NRC, potentially a violation of ethics rules. Specifically, an NRC employee participating in a teleconference with NPP personnel concerning a license amendment shortly after the former Branch Chief's departure recalled hearing a voice of an individual who sounded like the former Branch Chief. The NRC employee was concerned that the former Branch Chief was representing the NPP and discussing with NRC a topic that he was previously involved with as an employee of NRC. It was also alleged that the former Branch Chief had influenced an NRC Division Director to relax testing related to the NPP's license amendment request and that this Division Director was having private discussions with licensee executives regarding NRC issues that should have been coordinated with NRC licensing staff. It was also alleged that the Division Director was "advocating industry positions and lacks respect for NRC licensing procedures."

Investigative Results:

OIG did not substantiate any potential misconduct by the Division Director or the former Branch Chief.

Even though, as a NPP manager, the Branch Chief may have participated in discussions with NRC dealing with some topics (such as Probabilistic Risk Assessment (PRA), where the former Branch Chief was a subject matter expert, there is no indication that the former Branch Chief was representing the NPP. Further, there is no evidence that the former Branch Chief attempted to contact any NRC personnel with the intent to influence the regulatory decision making process.

OIG interviewed several NRC employees who worked for the former Branch Chief when he was the chief of the PRA, and other NRC senior managers who closely worked on issues relating to the NPP to ascertain whether the former Branch Chief had contacted any of his previous colleagues with the intent to influence the NRC's regulatory decisionmaking process pertaining to any other regulatory action under review. None of the former Branch Chief's former colleagues interviewed by OIG indicated that the former branch chief had attempted to improperly influence them into taking a regulatory position in favor of the NPP after he left NRC.

OIG interviewed the Division Director who advised his dealings with the NPP were no different from any other power plants. The Division Director denied any

wrongdoing and denied giving the NPP any preferential treatment. Regarding whether the Division Director had "private discussions with licensee executives" pertaining to any of NRC's regulatory affairs, the Division Director stated that "just as a manager at division director level" would, there were occasions to attend meetings with licensee senior executives and have small discussions about the NRC's review process; however, these discussions were "just a normal sidebar discussion(s)," and he did not believe that these discussions would possibly benefit the licensees in any way. Further, the Division Director denied receiving any "kickbacks or gifts" from any of the licensees.

The Division Director recalled hearing the former Branch Chief on a conference call during which the former Branch Chief may have "touch[ed] on some of the PRA issues," however, he did not believe the former Branch Chief was intentionally making attempts to represent the licensee to NRC with his previous Government-work expertise to possibly influence the NRC's direction. Further, the Division Director denied being in contact with the former Branch Chief for any reasons to possibly influence the NRC's decisionmaking process.

OIG discussed this investigation with NRC's Office of the General Counsel ethics counselors, and informed them that the former Branch Chief may have participated in teleconference calls with the NRC personnel to discuss topics that the former branch chief was previously involved in as an NRC employee. Further, the former Branch Chief was identified as the point-of-contact on some of the documents that the NPP had submitted to NRC. The ethics counselors conveyed that because the former Branch Chief now works for a licensee, he is likely to make contact with the NRC; further, it is not a violation for former employees to make contact with former colleagues as long as he has no intention to influence the regulatory process. They also indicated the former Branch Chief is authorized to work on PRA for the NPP, as long as his work is "behind the scene" and he has no intentions of influencing the outcome of NRC's decisions. One of the ethics counselors further clarified that "making an appearance or communication" would require for the individual to be officially representing the licensee with the specific topic. Because the former branch chief had participated in a teleconference or been identified as the POC for the NPP's submittal would not constitute that he is the licensee's representative on the topic discussed.

(Addresses Management and Performance Challenge # 1)

Misuse of Government Computers by NRC Employees

Strategic Goal: Corporate Management

OIG conducted two separate investigations into misuse of NRC-issued computers by NRC employees. The first investigation was based on an allegation of unusual after-hours activity in NRC headquarters by an NRC employee. The alleger indicated that the employee routinely works well into the evening even though the employee's

supervisor said the employee had no assigned work that would warrant working late hours each night. In the second investigation, during a proactive review of network activity for violations, OIG identified a computer assigned to an NRC employee that was being used to search Internet Web sites for sexually explicit material.

Investigative Results:

OIG conducted searches of the Government computer assigned to the employee alleged to have unusual after-hours activity. The OIG investigation determined that the employee used an NRC computer assigned to him to view sexually explicit images and videos during his work hours. OIG found that he sometimes viewed sexually explicit images while earning overtime hours. The agency suspended the employee for his actions.

During the other investigation, OIG learned the employee borrowed an NRC laptop computer while on personal vacation overseas. OIG reviewed the loaner laptop computer and found sexually explicit material on it as well. The OIG investigation determined that the NRC employee misused his NRC issued computer while at work to view sexually explicit material. He also misused an NRC loaner laptop computer to view sexually explicit images and videos during the period he was on vacation. After OIG issued a report of investigation to the agency for action, the employee retired from Federal service.

(Addresses Management and Performance Challenge # 4)

Impersonation of NRC Employee

OIG Strategic Goal: Safety

OIG conducted an investigation into an allegation from the Better Business Bureau in Shreveport, LA, that it had received complaints that someone was impersonating an NRC official to obtain citizens' personal information and money in exchange for alleged grants from the NRC. The unknown individual(s) communicated with the citizens via text through Facebook Messenger. In reviewing the information, OIG identified that an individual had created a Facebook page claiming to be "Larry Mankel," which contained photographs that appear to be that of a U.S. Congressman. OIG also received a similar allegation of an unknown individual(s) claiming to be "Larry Markel."

Investigative Results:

OIG was not able to identify the individual(s) claiming to represent NRC who sent text messages to public citizens to obtain personal information or money because such individuals frequently mask their identity and create fake social media accounts. OIG verified that one of the telephone numbers originated from Nigeria.

OIG contacted the Better Business Bureau in Shreveport, LA, to obtain additional information; however, the agency was unable to provide identifying information regarding any public citizen who had reported being contacted by someone claiming to be an NRC official to obtain personal information or money.

OIG reviewed the Facebook page purportedly belonging to "Larry Mankel" and found that while the Facebook page was registered to a "Larry Mankel," the profile picture was that of a U.S. Congressman. The only identifying information that related to the NRC was what appeared to be an altered photograph. The photograph depicted the Congressman and two other people holding an image of an oversized large fake check. The photograph reflected that NRC had issued a check to a grant winner in the amount of $250,000. OIG contacted Facebook and requested that the Mankel page be removed from its site.

(Addresses Management and Performance Challenge # 4)

Misconduct by NRC Manager Relating Alleged Falsification of Time & Attendance Records

OIG Strategic Goal: Corporate Management

OIG conducted an investigation into an allegation that an NRC senior official committed time card fraud when he instructed an employee to work from home for approximately 4 months, instead of using sick leave due to a family medical issue. According to the alleger, the senior official misled the NRC staff by telling them the employee was working from home on a special project when there was no special project.

Investigative Results:

OIG did not substantiate any misconduct by the NRC senior official or employee. OIG found from a review of time and attendance records that the employee used leave the majority of the timeframe in question. OIG learned the employee used a combination of personal leave and donated leave because a family member had a medical issue. OIG learned that the NRC Office of the Chief Human Capital Officer approved the employee to use donated leave. Also, OIG learned that the NRC senior official did provide work to the employee on several occasions when the employee teleworked. The OIG senior official told staff the employee was working on a "special project" in an attempt to respect the privacy of the employee experiencing the family medical issue.

(Addresses Management and Performance Challenge # 6)

Alleged Harassment of NRC Employee

OIG Strategic Goal: Corporate Management

OIG conducted an investigation into an allegation that an NRC staff member had been sexually harassed by a senior manager.

Investigative Results:

OIG could not substantiate whether or not the manager sexually harassed the employee. OIG made several attempts to interview the employee who declined to be interviewed and subsequently resigned from the agency. The manager, when interviewed by OIG, denied sexually harassing the employee. No witnesses were identified who could corroborate either account.

(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.

DNFSB MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board* as of October 1, 2017
(as identified by the Inspector General)

Challenge 1: *Management of a healthy and sustainable organizational culture and climate.*

Challenge 2: *Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.*

Challenge 3: *Management of administrative functions.*

Challenge 4: *Management of technical programs.*

* *For more information on the challenges, see DNFSB-18-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board.* https://www.nrc.gov/docs/ML1729/ML17291A571.pdf

DNFSB AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed four audits and evaluations. These audits and evaluations are summarized below.

Audit Summaries

Audit of DNFSB's Financial Statements for Fiscal Years 2017 and 2016

The *Accountability for Tax Dollars Act of 2002* requires the Inspector General(IG) or an independent external auditor, as determined by the IG, to annually audit DNFSB's financial statements in accordance with applicable standards. In compliance with this requirement, OIG retained Acuity Consulting, Inc. (Acuity), to conduct this annual audit. The audit included, among other things, obtaining an understanding of DNFSB and its operations, including internal control over financial reporting; evaluating the design and operating effectiveness of internal control and assessing risk; and testing relevant internal controls over financial reporting.

The objective of a financial statement audit is to determine whether the audited entity's financial statements are free of material misstatement.

Audit Results:

Financial Statements: The auditors expressed an unmodified opinion on the agency's FY 2015 and FY 2016 financial statements.

Internal Controls: The auditors expressed an unmodified opinion on the agency's internal controls over financial reporting.

Compliance with Laws and Regulations: The auditors found no reportable instances of noncompliance.

(Addresses Management and Performance Challenge #3)

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

Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The DATA Act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Government wide data definition standards issued by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury). Spending data are displayed on the USAspending.gov Web site. A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAOs) are required to provide assurance over the quality of the data submitted and were to begin reporting

FY 2017 second quarter data for public display by May 2017. The DATA Act also requires OIGs to submit this audit report to Congress and the public.

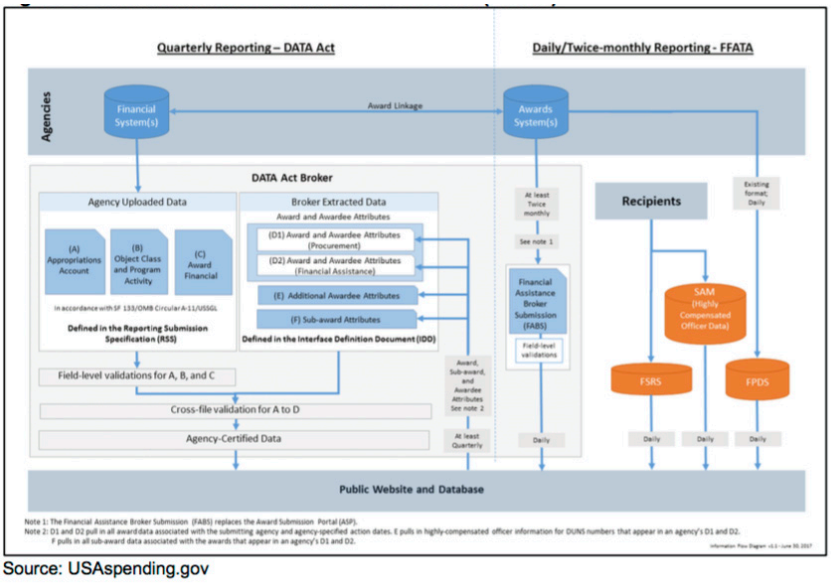
The audit objectives were to assess the (1) completeness, timeliness, quality, and accuracy of FY 2017 second quarter financial and award data submitted for publication on USAspending.gov, and (2) DNFSB's implementation and use of the Governmentwide financial data standards established by OMB and Treasury.

Audit Results:

Auditors assessed the DNFSB second quarter financial and award data submitted for publication on USAspending.gov and found while it contained most of the required information and conformed to the OMB and Treasury standards, there were deficiencies in completeness, timeliness, quality, and accuracy of the sampled submitted information. All of the 13 sampled transactions were found to be incomplete, not timely, inaccurate, and did not meet quality standards. Further, DNFSB's implementation of the Governmentwide financial data standards established by OMB and Treasury should be improved in the following areas:

- SAO's statement of assurance attesting to the internal controls over the validity and reliability of the DATA Act submission.
- Implementation of guidance and internal procedures governing submissions under the DATA Act.

These weaknesses occurred because of a lack of internal procedures that clearly delineate the requirements for publishing DATA Act information and developing an SAO Statement, and due to weaknesses in DNFSB's documentation of the processes for linking internal systems data, transforming data into the required DATA Act schema format, and mapping the data from the DNFSB schema to the DATA Act schema. With these weaknesses, DNFSB risks continuing to post untimely, unreliable, inconsistent, and inaccurate data, thereby not meeting DATA Act submission requirements.



Source: USAspending.gov

(Addresses Management and Performance Challenge #3)

Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014) for Fiscal Year 2017

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 DNFSB's implementation of FISMA 2014 for FY 2017 at DNFSB.

The objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2017.

Evaluation Results:

DNFSB has continued to make improvements in its information security program, and has completed implementing the recommendations from previous FISMA evaluations. However, the independent evaluation identified the following security program weaknesses:

- Information security program documentation is not up-to-date, and
- Information system contingency planning needs improvement.

Up-to-date documentation is important for DNFSB staff in order to effectively implement the information security program. It is also important for ensuring the DNFSB information security program aligns with agency and Federal laws, regulations and policies. Up-to-date documentation also helps ensure consistent information technology (IT) security practices despite staff turnover or changes in IT security positions.

While DNFSB has developed both a disaster recovery plan and continuity of operations plan for restoration of operational capability at an alternate site, it has not developed an Information System Contingency Plan (ISCP) for its General Support System. Lack of an ISCP may prevent timely restoration of services in the event of short-term system disruptions that do not require restoration of operational capability at an alternate site.

(Addresses Management and Performance Challenge #2)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing DNFSB in Fiscal Year 2018

In accordance with the Reports Consolidation Act of 2000, the Inspector General identified what he considered the most serious management and performance challenges facing DNFSB as of October 1, 2017. These management and performance challenges are directly related to DNFSB's organizational culture and climate, security, human capital, and internal controls. OIG's work in these areas indicates that the program improvements are needed. DNFSB is responding positively to recommendations to improve the efficiency and effectiveness of its programs.

The following four challenges represent what OIG considers to be inherent and continuing program challenges relative to maintaining effective and efficient oversight and internal controls at DNFSB:

1. Management of a healthy and sustainable organizational culture and climate.
2. Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.
3. Management of administrative functions.
4. Management of technical programs.

(Addresses all Management and Performance Challenges)

DNFSB AUDITS

Audits in Progress

Audit of DNFSB's Issue and Commitment Tracking System

DNFSB's Issue and Commitment Tracking System (IACTS) is an electronic system that DNFSB's technical staff uses to support management of Board and staff safety issues, potential safety issues, and related DOE and internal staff commitments. The purpose of IACTS is to ensure DNFSB does not lose any safety issues and to track whether the issues are open or closed.

Safety issues are safety concerns identified at defense nuclear facilities, and the followup actions to be completed on the given safety issues are called commitments. Technical staff are responsible for proposing new safety issues and commitments and maintaining IACTS records to ensure IACTS is up-to-date. After recording safety issues in IACTS, technical staff perform follow-up oversight activities to facilitate resolution of the safety issues. It is then management's responsibility to decide when an issue is ready for closure in IACTS.

During the 2016 Audit of DNFSB's Oversight of Construction Projects at Defense Nuclear Facilities, OIG determined IACTS guidance did not adequately detail what information should be included in the system. As a result, DNFSB's technical staff inconsistently filled in information in IACTS and infrequently updated the IACTS entries.

The audit objective is to determine if safety issues and follow up actions are negatively impacted by DNFSB's inconsistent use of IACTS.

(Addresses Management and Performance Challenge #4)

Audit of the 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 was 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)

DNFSB INVESTIGATIONS

Investigative Case Summaries

DNFSB Office of General Counsel Not Fully Supporting the Board's Direction to Staff

OIG conducted an investigation into an allegation that the former Acting General Counsel had acted in an unethical manner by providing misleading information to the Board, which in turn was to be provided to the Government Accountability Office (GAO), in response to a GAO audit recommendation.

Investigative Results:

OIG did not substantiate that the General Counsel attempted to mislead the Board in order to mislead GAO. According to two then current Board Members and an OGC attorney, there was no requirement for DNFSB to report to GAO the intricate details of how its recommendations were being addressed or satisfied by DNFSB. Furthermore, while the General Counsel's purposed responses to GAO lacked the details that the board member wanted to be included, the responses were appropriate and not misleading.

As background, in response to a congressional request, in the fall of 2013, GAO reviewed the operations and oversight of DNFSB and recommended, among other things, that the DNFSB implement a policy to publicly disclose the results of Board Members' votes. In June 2014, the Board approved a Request for Board Action (RFBA) to develop an operating procedure that would require each notational vote and all completed forms in the appendices to the Board Procedures to be posted on the Board's public Web site. In October 2014, the staff submitted a draft policy describing operating procedures for Board approval. The draft operating procedure did not contain language that fully addressed the Board's direction; however, the staff provided alternative options with justifications for Board consideration. In late November 2014, the staff produced a revised draft operating procedure that was approved by the Board on December 4, 2014.

The then DNFSB Chairman tasked the then Acting General Counsel (GC) with drafting the official response to GAO's audit recommendations. Board Procedures required the GC to submit the draft responses to the Board for approval prior to responding to GAO. Between December 5, 2014, and December 16, 2014, the GC submitted four different draft responses to the Board. One Board Member contested each of the GC's responses and asserted that the GC was attempting to mislead the GAO because the draft procedure would not have completely satisfied GAO recommendation or the board member's RFBA. On December 17, 2014, during a Board Gathering, the Board Member asked the GC if the draft operating procedure would have satisfied both. The GC responded that it did, but he later sent an email to all Board Members indicating that after reviewing the October 2014, draft proposed operating procedure, the GC acknowledged that it would have partially satisfied the GAO recommendation. The GC also submitted an updated proposed response to GAO indicating that although the staff had developed a draft operating procedure by October 2014, the Board had not approved the operating procedure.

OIG learned from the then Chairman that he tasked the GC with the responsibility to draft the DNFSB response to the GAO Audit. The then Chairman reviewed the GAO report, the GC's draft proposed responses, and was comfortable with how the Board was proceeding. He went on to say that based on all the information he considered, he never believed that the GC had attempted to influence the Board to mislead GAO.

OIG also learned from the then Vice Chairman that OGC and OGM drafted an operating procedure relating to the RFBA. Although the draft policy did not initially satisfy the GAO recommendation or the Board's direction, the Vice Chairman believed the GC's proposed comment to GAO was factually correct. Also, the Vice Chairman stated the GC wrote the response to reflect what the staff had done, not what the Board had done, to try to satisfy GAO's recommendation.

A DNFSB staff attorney with knowledge of the drafting of the operating procedure told OIG the GC's proposed responses to GAO were appropriate and not misleading. The attorney said that the Board was not required to respond to GAO's audit in detail and that she believed it was not appropriate to disclose details of the disagreements between Board Members and the Staff to GAO.

(Addresses Management and Performance Challenges # 1 and 3)

Potential Failure To Follow Procurement Requirements for Information Technology Software

OIG conducted this investigation based on an allegation that DNFSB "mismanaged an effort to procure a Correspondence Management System (CMS) software program that could have been developed with existing software tools at a lower cost to the Federal Government." It was reported that DNFSB had spent over $300,000, plus additional maintenance costs, for a system that could have been easily developed in-house and that DNFSB staff did not do a proper job analyzing the different options that were available.

Investigative Results:

OIG did not substantiate any misconduct in the DNFSB procurement of CMS. OIG found that the DNFSB Office of General Manager (OGM) Fiscal Year 2017 Work Plan included a plan to procure and develop a new CMS to accommodate the Board's folder, voting, and correspondence processes, which Board Members approved. OGM also provided information on how potential systems were evaluated and how they arrived at a sole source contract. The 2017 Work Plan, did not direct or suggest that the agency consider developing a CMS with existing software tools. A subsequent comparison of CMS and a system that was developed in-house, revealed that CMS is far more capable of achieving agency requirements than the in-house developed system.

(Addresses Management and Performance Challenge # 3)



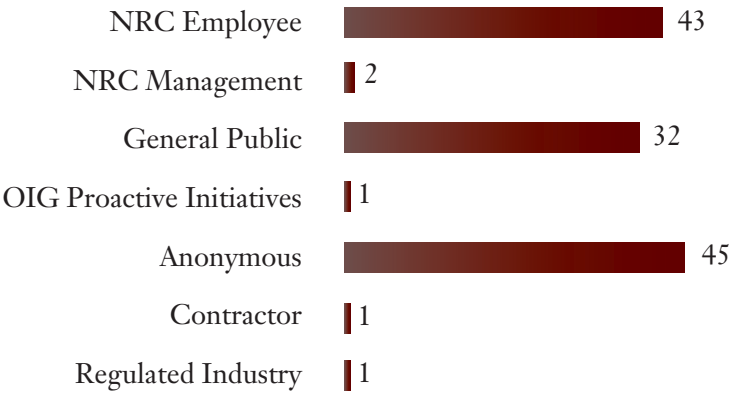
Nuclear power plant generator

SUMMARY OF OIG ACCOMPLISHMENTS AT NRC

September 30, 2017—March 31, 2018

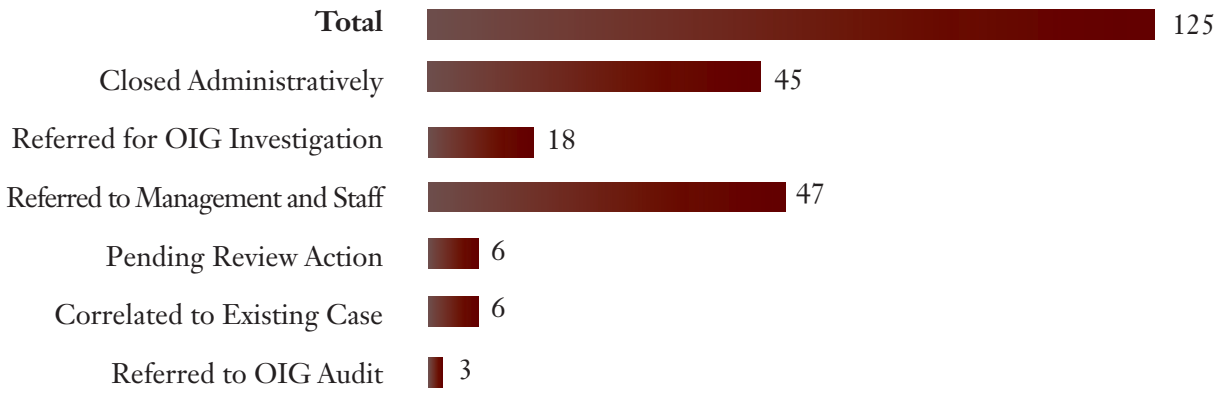
Investigative Statistics

Source of Allegations



Allegations resulting from the NRC OIG Hotline calls: 67 **Total: 125**

Disposition of Allegations



Status of Investigations

DOJ Referrals . . . 3
DOJ Declinations . . . 2
DOJ Pending . . . 3
Criminal Informations/Indictments . . . 1
Criminal Convictions . . . 0
Criminal Penalty Fines . . . 0
Civil Recovery . . . 0
State and Local Referrals . . . 2
Criminal Informations/Indictments . . . 1
Criminal Convictions . . . 0
Civil Penalty Fines . . . 0
Civil Recovery . . . 0
NRC Administrative Actions:
- Counseling and Letter of Reprimand . . . 0
- Terminations and Resignations . . . 1
- Suspensions and Demotions . . . 1
- 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	1	0	0	0	1
Employee Misconduct	14	9	2	1	21
External Fraud	11	1	2	0	10
Internal Fraud	1	1	1	0	1
Management Misconduct	13	4	6	0	11
Miscellaneous	4	0	0	0	4
Proactive Initiatives	3	0	0	0	3
Technical Allegations	7	1	1	0	7
Theft	0	2	1	1	1
Total	**54**	**18**	**13**	**2**	**59**

[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
02/08/2018	Audit of NRC's Decommissioning Financial Assurance Instrument Inventory	OIG-18-A-09
12/21/2017	Summary Report of FISMA Evaluations Conducted in Fiscal Year 2017	OIG-18-A-08
12/21/2017	Audit of NRC's Security Oversight of Research and Test Reactors	OIG-18-A-07
12/21/2017	Evaluation of NRC's Shared "S" Drive	OIG-18-A-06
11/16/2017	Audit of the Nuclear Regulatory Commission's Special Purpose Financial Statements FY 2017 Closing Package	OIG-18-A-05
11/09/2017	Results of the Audit of the United States Nuclear Regulatory Commission's Financial Statements for FY 2017	OIG-18-A-04
11/08/2017	Audit of NRC's Compliance with the Digital Accountability And Transparency Act of 2014	OIG-18-A-03
10/30/2017	Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017	OIG-18-A-02
10/18/2017	Inspector General's Assessment of the Most Serious Management And Performance Challenges Facing the Nuclear Regulatory Commission in Fiscal Year 2018	OIG-18-A-01

NRC Contract Audit Reports

OIG Issued Date	Contractor/Title/ Contract Number	Questioned Costs (Dollars)	Unsupported Costs (Dollars)
11/09/2017	**SOUTHWEST RESEARCH INSTITUTE** Independent Audit Report on Southwest Research Institute's Proposed Amounts on Select Unsettled Flexibly Priced Contracts for Fiscal Years 2012 - 2014 NRC-02-06-018 NRC-02-06-021 NRC-02-07-006 NRC-03-10-066 NRC-03-10-081 NRC-04-10-144 NRC-41-09-011 NRC-HQ-11-C-03-0047 NRC-HQ-11-C-03-0058 NRC-HQ-11-C-02-0084 NRC-HQ-12-C-07-0036 NRC-HQ-12-C-04-0069 NRC-HQ-12-C-42-0083 NRC-HQ-12-C-42-0057 NRC-HQ-12-C-03-0102 NRC-HQ-12-C-02-0089 NRC-HQ-12-C-03-0052 NRC-HQ-13-C-03-0044 NRC-HQ-13-C-03-0048 NRC-HQ-50-E-14-0001	$394,669	$0
11/09/2017	**ADVANCED SYSTEMS TECHNOLOGY MANAGEMENT, INC.** Independent Audit Report on Advanced Systems Technology Management, Inc.'s Proposed Amounts on Unsettled Flexibly Priced Contracts for Contractor Fiscal Years 2013 and 2014 NRC-08-09-306	$1,287,168	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	2	$1,950,343	0
B.	Which were issued during the reporting period	2	$1,681,837	0
	Subtotal (A + B)	4	$3,632,180	0
C.	For which a management decision was made during the reporting period:			
	(i) dollar value of disallowed costs	1	$721,188	0
	(ii) dollar value of costs not disallowed	0	$926,527	0
D.	For which no management decision had been made by the end of the reporting period	3	$1,984,465	0

[5] *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.*

TABLE II

OIG Reports Issued with Recommendations That Funds Be Put to Better Use[4]

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

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

TABLE III

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

Date	Report Title	Number
5/26/2003	**Audit of NRC's Regulatory Oversight of Special Nuclear Materials**	**OIG-03-A-15**
	Recommendation 1: Conduct periodic inspections to verify that material licensees comply with material control and accounting (MC&A) requirements, including, but not limited to, visual inspections of licensees' s pecial 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.	

SUMMARY OF OIG ACCOMPLISHMENTS AT THE DNFSB

October 1, 2017, through March 31, 2018

Investigative Statistics

Source of Allegations

DNFSB Employee	2
DNFSB Management	1
Allegations Received from NRC OIG Hotline: 1	**Total: 3**

Disposition of Allegations

Total	**3**
Referred for OIG Investigation	1
Pending Review Action	0
Closed Administratively	2
Referred to Other Agency	0

Status of Investigations

DOJ Referrals 0
DOJ Declinations 0
DOJ Pending 1
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 0
- Suspensions and Demotions 0
- Other (e.g., PFCRA) 1

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued[5]	Cases in Progress
Employee Misconduct	1	1	1	0	1
Management Misconduct	6	1	1	0	6
Proactive Initiatives	2	0	0	0	2
Total	**9**	**2**	**2**	**0**	**9**

[5] *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
11/15/2017	Audit of the Defense Nuclear Facilities Safety Board's Financial Statements for Fiscal Years 2017 and 2016	DNFSB-18-A-04
11/08/2017	Audit of DNFSB's Compliance with the Digital Accountability Act of 2014 (DATA Act)	DNFSB-18-A-03
10/30/2017	Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017	DNFSB-18-A-02
10/18/2017	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in Fiscal Year 2018	DNFSB-18-A-01

DNFSB AUDIT RESOLUTION ACTIVITIES

TABLE I

OIG Reports Containing Questioned Costs[6]

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

[6] *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[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.*

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. NRC requires that materials licensees report information to the Nuclear Materials Management and Safeguards System, a computer database managed by the U.S. Department of Energy 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 SNM. 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	1	$0	NRC oversees 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 the Code of Federal Regulations. NRC conducts reactive and routine inspections of vendors' implementation of these 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 10 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	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 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." NRC staff can process electronic documents containing SUNSI in a variety of ways including on shared network drives. Regardless of how NRC employees exchange SUNSI on agency networks, Federal law requires that NRC maintain adequate controls over the confidentiality, integrity, and availability of this information. 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.

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	2	$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	mmary
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. 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	1	$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 objective of this audit 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
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 Internal Controls Over Fee Revenue	OIG-15-A-12	3/19/15	2	$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 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.
2015	Audit of NRC's Regulatory Analysis Process	OIG-15-A-15	6/24/15	1	$0	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.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Reactor Business Lines' Compliance with Agency Non-Financial Internal Control Guidance	OIG-15-A-16	6/24/15	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.
2015	Audit of NRC's Web-Based Licensing (WBL) System	OIG-15-A-17	6/29/15	2	$0	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.

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	2	$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 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. OIG contracted with AEGIS.net, Inc., to evaluate 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. 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	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	Independent Evaluation of the Security of NRC's Publicly Accessible Web Applications	OIG-16-A-15	6/1/16	2	$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 IT 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 OIG has joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG will assess its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications. This evaluation was conducted by Richard S. Carson & Associates, Inc. (Carson Inc.) to assess NRC's publicly accessible Web applications as part of this crosscutting project. The objective of the evaluation 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 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 made 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 made 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. Management agreed 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	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 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 made three recommendations to improve the effectiveness of NRC's process to assess internal control over program operations. Agency management agreed with the report.
2016	Audit of NRC's Significance Determination Process for Reactor Safety	OIG-16-A-21	9/26/16	3	$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.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
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	2	$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. The evaluation objective was to perform an independent evaluation of NRC's 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.
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 objective of this audit was to assess whether the NRC foreign assignee program provides adequate information security. The audit report made 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.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Audit of NRC's Oversight of Source Material Exports to Foreign Countries	OIG-17-A-08	2/16/17	1	$0	One of NRC'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 made 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.
2017	Audit of NRC's Oversight of Security at Decommissioning Reactors	OIG-17-A-09	2/22/17	2	$0	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 made 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 agreed 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
2017	Audit of NRC's Purchase Card Program	OIG-17-A-14	05/30/17	6	$0	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. The resulting audit report had three findings and six recommendations that were all implemented by the agency before the start of this audit. Generally, NRC's purchase card program is adequately governed by internal controls. However, opportunities exist to improve the effectiveness of internal controls in the areas of documentation and program oversight. 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. OIG made seven recommendations to improve communication to cardholders and approving officials and strengthen internal controls. Agency management agreed with the findings and recommendations in this report.
2017	Audit of NRC's PMDA and DRMA Functions to Identify Program Efficiencies	OIG-17-A-18	07/03/17	1	$0	Many NRC offices maintain corporate support through Program Management, Policy Development and Analysis Staff (PMDA) and Division of Resource Management and Administration (DRMA) functions. The PMDA function at NRC headquarters and the DRMA function at NRC regional offices manage service delivery in support areas. 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. 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 made one recommendation to complete implementation of all Mission Support Task Force recommendations that may assist in optimizing the use of resources and result in improving standardization and centralization throughout the agency. Agency management agreed with the finding and recommendation in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Audit of NRC's Contract Administration Process	OIG-17-A-20	08/16/2017	3	$0	The Federal Acquisition Regulation and Nuclear Regulatory Commission's (NRC) Management Directive 11.1, NRC Acquisition of Supplies and Services, and NRC's Acquisition Regulation under 48 Code of Federal Regulations Chapter 20 provide specific requirements for NRC's contract administration process. 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. The audit objective was to assess the effectiveness of NRC's contract administration process and compliance with Federal and agency regulations. Generally, NRC's contract administration processes comply with applicable regulations, and the agency's internal controls governing contract administration are adequate. However, opportunities exist to improve the effectiveness of internal controls for NRC's management of contractor invoices and supporting documentation and for contract closeout procedures followed by CORs. OIG made three recommendations to improve the effectiveness of management of contractor invoices and supporting documentation and to strengthen adherence to contract closeout procedures by CORs. Two recommendations address the effectiveness of internal controls over recordkeeping for contractor invoices and supporting documentation. The third recommendation addresses enhancement of internal controls to ensure better adherence to contract closeout procedures. Agency management agreed 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
2017	Audit of NRC's Oversight for Issuing Certificates of Compliance for Radioactive Material Packages	OIG-17-A-21	8/16/17	4	$0	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. 10 CFR Part 71 establishes the requirements for transportation of radioactive material package designs. Additionally, 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 provide adequate protection for public health, safety, and the environment. 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. This report made four recommendations to improve NRC's oversight for issuing certificates of compliance for radioactive material packages. Agency management agreed 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
2017	Independent Evaluation of the Federal Information Security Modernization Act of 2014 for FY 17 – Technical Training Center, Chattanooga, Tennessee	OIG-17-A-22	08/17/17	2	$0	On December 18, 2014, the President signed 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. The NRC Technical Training Center (TTC) provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities and is located in Chattanooga, TN. The TTC is part of the Office of the Chief Human Capital Officer and operates under the direction of the Associate Director for Human Resources Training and Development. The objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2017 at the TTC and to evaluate the effectiveness of agency information security policies, procedures, and practices as implemented at this location. The evaluation found that 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. OIG makes recommendations to address these findings. Additionally, OIG identified an issue with unclear and out-of-state laptop security policies and procedures that will be further evaluated during the FY 2017 FISMA evaluation. This evaluation made three recommendations to update the software and hardware inventories, managing the authorization of an SGI laptop, and updating the system boundary and performing all required system cybersecurity assessment processes and procedures. Agency management stated their general agreement with the evaluation results.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Audit of NRC's 10 CFR 2.206 Petition Review Process	OIG-17-A-23	08/22/17	2	$0	Since established in 1975, NRC has encouraged 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 has not issued orders in response to any of the thirty-eight (38) 10 CFR 2.206 petitions filed from fiscal year (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 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. 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. As a result, NRC missed opportunities to use data to enhance the 10 CFR 2.206 petition process. In addition, NRC staff have difficulty applying 10 CFR 2.206 petition review and rejection criteria because the criteria are not clear. As a result, some petitions might not be dispositioned consistently or properly. This report made two recommendations to (1) develop controls to ensure formal assessments are performed and are documented for future use, and (2) clarify the criteria for reviewing and rejecting petitions. Agency management agreed 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
2017	Evaluation of Proposed NRC Modifications to the Probabilistic Risk Assessment Process	OIG-17-A-26	9/21/17	1	$0	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 has a tool to estimate risk at nuclear power plants known as Standardized Plant Analysis Risk (SPAR) Model Development Programs. SPAR models are used by NRC staff in support of risk-informed activities. During the period January 2016 through July 2016, NRC staff assessed alternatives to using SPAR models, including use licensee PRA models, which includes purchasing licensee software. The evaluation objective was to assess NRC's process for piloting alternative risk modeling techniques including analyzing costs, benefits, and feasibility of these alternatives. The evaluation found that 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, 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 decision-making. Moreover, better process management can help NRC more efficiently revisit SPAR alternatives if new cost data and feasibility solutions become available. The evaluation report made a recommendation to improve the process for assessing alternatives to using SPAR models. Agency management agreed with the results and recommendation in this report and opted to provide formal comments for inclusion in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Evaluation of NRC's Management of Government Cell Phones	OIG-17-A-27	9/21/17	4	$0	In April 2016, 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. The contract was expected to run through November 30, 2017, and was valued at approximately $1.8 million. 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 evaluation objective was to evaluate whether NRC's Government furnished cell phones are sufficiently managed to provide information security. OIG did not identify weaknesses relative to cell phone information security; however, the evaluation identified three areas for improvement in the overall management of Government cell phones: (a) guidance and training on cell phone management for property custodians, (b) Government cell phone record management, and (c) the rules of behavior associated with cell phones. The report made four recommendations to improve NRC's management of Government phones. Agency management agreed with the finding and recommendations in this report.
2018	Independent Evaluation of NRC's Implementation of FISMA 2014 for FY 2017	OIG-18-A-02	10/30/17	7	$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. The evaluation objective was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA 2014 for FY 2017. The evaluation found that NRC has made significant improvements in the effectiveness of their information technology security program, and continues to make improvements in performing continuous monitoring activities. However, the independent evaluation identified information technology security program areas including Information technology security program documentation and continuous monitoring activities that need improvement. To improve NRC's implementation of FISMA 2014, the report made seven recommendations. Management agreed 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
2017	Audit of NRC's Compliance with the DATA Act	OIG-18-A-03	11/8/17	2	$0	Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Government wide data definition standards issued by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury). Treasury displayed spending data on the USAspending.gov Web site. A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAO) are required to provide assurance over the quality of the data submitted and begin reporting FY 2017 second quarter data for public display by May 2017. The DATA Act also requires Office of the Inspector General (OIG) to submit this audit report to Congress and the public. The audit objective was to assess the (1) completeness, timeliness, quality, and accuracy of fiscal year 2017, second quarter financial and award data submitted for publication on USAspending.gov, and (2) NRC's implementation and use of the Government-wide financial data standards established by OMB and Treasury. NRC's policies and procedures governing DATA Act submissions do not fully address the completeness, quality, and accuracy of the data submitted and do not always comply with applicable laws, regulations, and policies. This report made two recommendations to improve NRC's documentation of policies and procedures for the SAO assurance statement, and to improve the agencies policies and procedures governing Broker submission warning messages. NRC management stated their disagreement with the report and recommendations in this report, and opted to provide formal comments for inclusion in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2017	Evaluation of the Shared "S" Drive	OIG-18-A-06	12/21/17	4	$0	On July 6, 2017, OIG identified and accessed an employee's bank account information on a personal check that was scanned and saved to the agency's shared "S" drive. After finding that the sensitive information was not protected by access controls, OIG reviewed the shared "S" drive for PII and identified a folder dated 2011, which had 35 subfolders for several offices in the agency. Of the 35 subfolders, 17 contained PII without appropriate access controls. The objective was to assess how NRC effectively manages and protects Personally Identifiable Information (PII) stored on the shared "S" drive in accordance with Federal regulations. OIG found weaknesses in the areas of inappropriate storage and management of PII on the shared "S" drive. This report made four recommendations to improve NRC's procedures and process for managing and protecting PII stored on the shared "S" drive. Management agreed with the findings and recommendations in this report.
2018	Audit of NRC's Decommissioning Financial Assurance Instrument Inventory	OIG-18-A-09	02/08/18	1	$0	As part of its regulatory function, NRC issues licenses for nuclear materials and regulates the decommissioning of material sites. Material licensees must provide financial assurance for decommissioning costs before they receive nuclear material or begin site operations. They must also maintain that funding throughout the duration of site operations. In June 2016, OIG issued an audit report on NRC's Decommissioning Funds Program. During that audit, OIG auditors were not able to examine the original financial instruments maintained by the agency because the safe containing the instruments was inaccessible. As a result, the audit had a scope limitation which informed the decision to perform this audit. The audit objectives were to determine whether (1) the Office of Nuclear Material Safety and Safeguards Inventory 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. Auditors found that the original signed decommissioning financial instruments are properly safeguarded in a fire-proof safe, however, opportunities exist to improve management of the program. This report makes a recommendation to update guidance to reflect current practices. Agency management stated their general agreement with the finding and recommendation in this report.

Total unimplemented recommendations: 85

DNFSB Unimplemented Recommendations

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of DNFSB's Process for Developing, Implementing, and Updating Policy Guidance	DNFSB-16-A-05	06/29/16	1	$0	In January 2015, a Government Accountability Office (GAO) audit highlighted that 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 agreed with the finding and recommendations in this report.
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. 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. OIG found that DNFSB's cybersecurity program has established policies, procedures, and controls to access to its "covered systems." However, DNFSB does not comply with all requirements of the Privacy Act of 1974 and the E-Government Act of 2002. Specifically, DNFSB does not conduct required reviews of its systems of record, or review privacy impact assessments for external servicing organizations. 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 agreed 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
2017	Audit of DNFSB's Resident Inspector Program	DNFSB-17-A-05	6/5/17	1	$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. 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 audit 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. DNFSB management agreed with finding and recommendations in this report.
2017	Audit of DNFSB's Telework Program	DNFSB-17-A-06	7/10/17	3	$0	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. 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. This report made three recommendations to improve DNFSB's telework policies to ensure continued compliance with Federal requirements, and consistency in the application of the policies and recordkeeping practices. DNFSB management agreed with findings and recommendations in this report.

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2018	Independent Evaluation of DNFSB's Implementation of FISMA 2014 for FY 2017	DNFSB 18-A-02	10/30/17	2	$0	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. The evaluation objective was to perform an independent evaluation of DNFSB implementation of FISMA 2014 for FY 2017. DNFSB has continued to make improvements in its information security program, and has completed implementing the recommendations from previous FISMA evaluations. However, the independent evaluation identified security program weaknesses in the areas of information security program documentation and information security contingency planning. This report made two recommendations to improve DNFSB's implementation of FISMA. DNFSB management agreed with the findings and recommendations in this report.
2018	Audit of DNFSB's Compliance with the DATA Act	DNFSB-18-A-03	11/8/17	7	$0	Congress enacted the Digital Accountability and Transparency Act of 2014 (DATA Act) on May 9, 2014. The act allows taxpayers and policymakers direct access to Federal agency spending data, and reporting by Federal agencies of financial and award information in accordance with Government wide data definition standards issued by the Office of Management and Budget (OMB) and the Department of the Treasury (Treasury). Spending data are displayed on the USAspending.gov Web site. A core requirement of the DATA Act is ensuring that posted spending data are reliable and consistent. Agency Senior Accountable Officials (SAOs) are required to provide assurance over the quality of the data submitted and begin reporting fiscal year (FY) 2017 second quarter data for public display by May 2017. The DATA Act also requires OIG to submit this audit report to Congress and the public. The audit objective was to assess the (1) completeness, timeliness, quality, and accuracy of fiscal year 2017, second quarter financial and award data submitted for publication on USAspending.gov, and (2) DNFSB's implementation and use of the Government-wide financial data standards established by OMB and Treasury. OIG found there were no differences between the Defense Nuclear Facility Safety Board's (DNFSB) definitions of DATA Act standards and those of Treasury and OMB. However, DNFSB's implementation and use of those standards did not comply with applicable Treasury and OMB guidance. This report made a recommendation to improve DNFSB's documentation of policies and procedures for the SAO statement of assurance, and to improve DNFSB's internal policies and procedures governing submissions under the DATA Act. DNFSB management agreed with the finding and recommendation in this report.

Total Unimplemented Recommendations: 16

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
AEA	Atomic Energy Act
AIGA	Assistant Inspector General for Audits
APC	Agency Program Coordinator
ATO	Authority to Operate
AWOL	Absence without leave
CFR	Code of Federal Regulations
CO	Contracting Officer
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
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Integrity Act
FOF	Force On Force
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
IACTS	Issue And Commitment Tracking System
IG	Inspector General
IMC	Inspection Manual Chapter
IMPEP	Integrated Materials Performance Evaluation Program
IPERA	Improper Payments Elimination and Recovery Act
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
IPP	Invoice Processing Platform
ISCP	Information system Contingency Plan
IT	Information Technology
ITISS	Information Technology Infrastructure Support Services
LAN	Local Area Network
MD	Management Directive
NMMSS	Nuclear Materials Management and Safeguards System
NMP	Nuclear Materials Program
NMMSS	Nuclear Materials Management and Safeguards System
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Officer of Personnel Management
OWFN	One White Flint North
PII	Personally Identifiable Information
PMDA	Program Management, Policy Development and Analysis

PRA	Probabilistic Risk Assessment
PRB	Petition Review Board
RES	Office of Nuclear Regulatory Research
RIDM	Risk Informed Decision Making
RISC	Risk Informed Steering Committee
SAO	Senior Accountable Official
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
SRI	Senior Resident Inspector
SUNSI	Sensitive, Unclassified Non-Safeguards Information
Treasury	Department of the Treasury
TTC	Technical Training Center
TWFN	Two White Flint North
WBL	Web-based Licensing
3WFN	Three White Flint NorthSDP 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	7-9
Section 5(a)(1)	Significant problems, abuses, and deficiencies	11-19, 28-29, 34-37, 38-39
Section 5(a)(2)	Recommendations for corrective action	11-18, 38-39
Section 5(a)(3)	Prior significant recommendations not yet completed	49
Section 5(a)(4)	Matters referred to prosecutive authorities	44, 51
Section 5(a)(5)	Listing of audit reports	45-46, 52
Section 5(a)(6)	Listing of audit reports with questioned costs or funds put to better use	11-19, 27-31, 34-37, 40-41
Section 5(a)(7)	Summary of significant reports	11-19, 27-31, 34-37, 40-41
Section 5(a)(8)	Audit reports — questioned costs	47, 53
Section 5(a)(9)	Audit reports — Funds put to better use	48, 54
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, and (c) with outstanding, unimplemented recommendations, including aggregate potential costs savings	55-81
Section 5(a)(11)	Significant revised management decisions	none
Section 5(a)(12)	Significant management decisions with which OIG disagreed	none
Section 5(a)(19)	Significant revised management decisions	none
Section 5(a)(13)	FFMIA section 804(b) information	none
Section 5(a)(14)(15)(16)	Peer review information	87
Section 5(a)(17)	Investigations statistical tables	43-44, 50-51
Section 5(a)(18)	Description of metrics	44, 51
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)	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	27-28, 30, 31, 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, in accordance with CIGIE requirements. 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. 32, No. 1
April 2018

Blog @NRCgov