

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



# Semiannual Report to Congress

**October 1, 2016—March 31, 2017**



## **OIG VISION**

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

## **OIG MISSION**

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

## **COVER PHOTOS:**

From left to right:

Decommissioning of Elk River Power Station,  
Elk River, Minnesota.

Low-level waste disposal site.

Inspection of yellowcake uranium in  
containment barrel.

---

# 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, 2016, to March 31, 2017.

Our work reflects the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse through the conduct of audits and investigations relating to NRC 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 the 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's and DNFSB's financial statements, information technology security, and management and performance challenges during this reporting period, my office issued reports intended to strengthen NRC's foreign assignee program and its oversight of security at decommissioning reactors, source material exports to foreign countries, and low-level radioactive waste disposal and waste blending.

During this semiannual reporting period, we issued nine program audit reports. As a result of this work, OIG made a number of recommendations to improve the effective and efficient operation of NRC's safety, security, and corporate management programs. OIG also opened 19 investigations, and completed 15 cases. This Semiannual Report also reflects new Inspector General (IG) Empowerment Act reporting requirements, including summaries of all IG reports with outstanding, unimplemented recommendations.

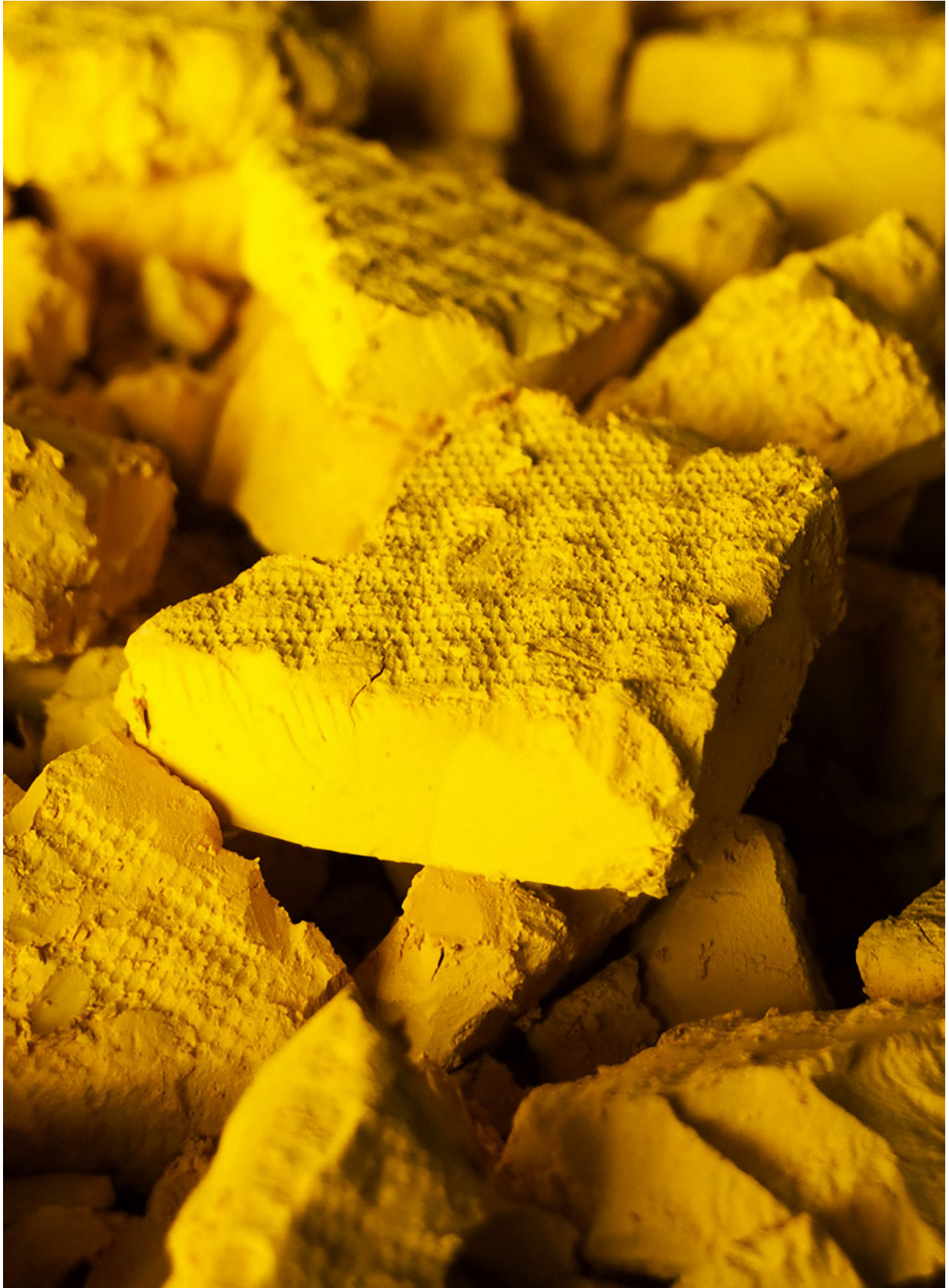
NRC OIG is committed to the integrity, efficiency, and effectiveness of NRC programs and operations, and our audits, investigations, and other activities highlighted in this report demonstrate our ongoing commitment. My staff strives to maintain the highest possible standards of professionalism and quality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

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

A handwritten signature in black ink that reads "Hubert T. Bell". The signature is written in a cursive, flowing style.

Hubert T. Bell  
Inspector General





*Yellowcake Uranium.*



---

# CONTENTS

<b>Highlights</b>	v
Audits	v
Investigations	x
<b>Overview of NRC and OIG</b>	1
NRC's Mission	1
OIG History, Mission, and Goals	2
OIG History	2
OIG Mission and Goals	3
<b>NRC OIG Programs and Activities</b>	5
Audit Program	5
Investigation Program	6
OIG General Counsel Regulatory Review	7
Regulatory Review	7
Other OIG Activities	9
<b>NRC Management and Performance Challenges</b>	10
<b>Audits</b>	11
Audit Summaries	11
Audits in Progress	21
<b>Investigations</b>	29
Investigative Case Summaries	29
<b>Defense Nuclear Facilities Safety Board</b>	35
<b>DNFSB Management and Performance Challenges</b>	35
Audit Summaries	36
Audits in Progress	39
<b>Summary of OIG Accomplishments at NRC</b>	41
NRC Investigative Statistics	41
NRC Audit Listings	43
NRC Audit Resolution Activities	44
<b>Summary of OIG Accomplishments at DNFSB</b>	47
DNFSB Investigative Statistics	47
DNFSB Audit Listings	49
DNFSB Audit Resolution Activities	50
<b>Unimplemented Audit Recommendations</b>	52
NRC	52
DNFSB	69
<b>Additional IG Empowerment Act Reporting</b>	71
<b>Abbreviations and Acronyms</b>	72
<b>Reporting Requirements</b>	73
<b>Appendix</b>	74



*Spent fuel storage cask in place on storage pad at the Haddam Neck Plant in Meriden, CT. Photo courtesy of Connecticut Yankee*



---

# HIGHLIGHTS

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

## *NRC Audits*

- 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. Source material (uranium) could potentially be enriched to produce highly enriched uranium—the primary ingredient of an atomic weapon. Therefore, tracking and accounting for the exports of source material are important to (1) ensure that it is used only for peaceful purposes, (2) comply with international treaty obligations, and (3) provide data to policymakers and other government officials. The audit objective was to determine the effectiveness of NRC's oversight of the export of source material. This audit report makes five recommendations to improve NRC's oversight of the export of source material through the creation of an export inspection program, clarification of specific NRC regulations related to exports, and creation of a qualification program for export licensing officers.
- NRC regulates the decommissioning of commercial nuclear power plants. Decommissioning is the process used to safely remove a nuclear power plant from service and reduce residual radioactivity to a level that permits release of the property and termination of its license. NRC has rules governing power plant decommissioning that protect workers and the public during the decommissioning process. For example, NRC regulations require power plant licensees to establish, maintain, and implement an insider mitigation program. In addition, NRC has regulations for the management of worker fatigue. These regulations are designed to ensure licensees effectively manage worker fatigue and provide reasonable assurance that workers are able to safely and competently perform their duties. The audit objective was to determine whether NRC's oversight of security at decommissioning reactors provides for adequate protection of radioactive structures, systems, and components. The audit report makes three recommendations to clarify which fitness-for-duty elements decommissioning licensees must implement to meet the requirements of the insider mitigation program and to establish requirements for a fatigue management program.
- Under the foreign assignee program, NRC invites peers from other nuclear safety regulators to obtain experience that would enhance safety programs and research programs worldwide, as well as promote exchange of technical information and expertise. Foreign assignees remain employees of the sponsoring regulatory or research organization in their home country. Approximately 80 foreign nationals have worked as assignees at NRC since 2005, representing 21 countries. The Office of International Programs has primary responsibility for the foreign assignee program and coordinates with

---

other offices through the process of onboarding a foreign assignee and during the assignment. Federal standards designate management as responsible for providing procedures that serve as a mechanism to support efficient operations, reliable reporting and communication, and reasonable assurance that requirements are met. Additionally, NRC policies for the foreign assignee program appear in management directives (MD) that assign responsibilities and establish requirements for processing, onboarding, and supervision of assignees, as well as development of security plans detailing access restriction to NRC information systems to prevent unauthorized access to sensitive information. The audit objective was to assess whether the NRC foreign assignee program provides adequate information security. The audit report makes three recommendations to develop a procedure for security planning during the process of onboarding and hosting a foreign assignee, and a secure, cost-efficient method to provide foreign assignees an email account.

- The *Digital Accountability and Transparency Act of 2014* (DATA Act) was enacted May 9, 2014, and requires that Federal agencies report financial and payment data in accordance with data standards established by the Department of the Treasury and the Office of Management and Budget. The data reported will be displayed on a Web site available to taxpayers and policymakers. In addition, the DATA Act requires that agency Inspectors General review statistical samples of the data submitted by the agency under the DATA Act and report on the completeness, timeliness, quality, and accuracy of the data sampled and the use of the data standards by the agency. The objective of the readiness assessment was to determine if NRC is on track to implement DATA Act requirements by the May 2017 deadline. The assessment concluded NRC has demonstrated readiness to meet the requirements set forth in the DATA Act. Therefore, no recommendations were made.
- The *Chief Financial Officers Act of 1990*, as amended, requires the Inspector General or an independent external auditor, as determined by the Inspector General, to annually audit NRC's financial statements to determine whether the agency's financial statements are free of material misstatement. The audit 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 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 regulation, (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*, and (5) assess agency compliance with *Improper Payments Elimination and Recovery Act*. The auditors expressed unmodified opinions on the agency's



---

Fiscal Year 2016 and Fiscal Year 2015 financial statements and internal controls, and found no reportable instances of noncompliance with laws and regulations. Therefore, no recommendations were made.

- The *Federal Information Security Modernization Act of 2014* (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General or by an independent external auditor. The Office of Management and Budget (OMB) requires OIGs to report their responses via an automated collection tool. The evaluation objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for F Y 2016. The evaluation determined that NRC has continued to make improvements in its information technology security program and progress in implementing the recommendations resulting from previous FISMA evaluations. However, the evaluation identified five recommendations aimed at strengthening the agency's approach to control testing, managing system inventory, and performing risk management activities.
- Low Level Radioactive Waste (LLRW) includes items that have become contaminated with radioactive materials or have become radioactive through exposure to neutron radiation. NRC classifies LLRW at the time of disposal based on its radioactivity. NRC has specified disposal and waste requirements for three classes of waste—Classes A, B, and C—with progressively higher concentrations of radioactive material. As waste class increases, additional measures to control the hazard to the public are required. The Office of Nuclear Material Safety and Safeguards is responsible for regulating activities which provide for the safe and secure production of nuclear fuel used in commercial nuclear reactors, including the disposal of radioactive waste and spent nuclear fuel. In addition, the Office of Nuclear Reactor Regulation develops and implements rulemaking, licensing, oversight, and incident response programs for nuclear reactors. This office also provides support to regional staff that conduct inspections of LLRW at nuclear reactor sites. Additionally, each of NRC's four regional offices plays a role in the oversight of LLRW as they execute established NRC policies and programs related to inspection, licensing, and enforcement for both reactor and non-reactor licensees. The audit objective was to determine if the disposal and waste blending processes at disposal facilities are done safely and effectively. The audit found that NRC provided adequate oversight through inspection activities. Therefore, the audit report did not identify any findings or make any recommendations; however, an opportunity for improvement was identified that pertains to centralizing LLRW guidance.

- 
- 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, 2016. These management and performance challenges are directly related to NRC's mission areas: 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.

### *Defense Nuclear Facilities Safety Board Audits*

- *The Accountability for Tax Dollars Act of 2002* requires the Inspector General or an independent external auditor, as determined by the Inspector General, to annually audit DNFSB's financial statements to determine whether the agency's financial statements are free of material misstatement. 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 was 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 2016 and FY 2015 financial statements and an unqualified 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.
- The DATA Act requires that Federal agencies report financial and payment data in accordance with data standards established by Treasury and OMB. The data reported will be displayed on a Web site available to taxpayers and policymakers. In addition, the DATA Act requires that agency Inspectors General review statistical samples of the data submitted by the agency under the DATA Act and report on the completeness, timeliness, quality, and accuracy of the data sampled and the use of the data standards by the agency. The objective of the readiness assessment was to determine if DNFSB is on track to implement the DATA Act requirements by the May 2017 deadline. The assessment determined that DNFSB, through its financial services provider, the United States Department of Agriculture, is on track to implement DATA Act requirements by the May 2017 deadline. Therefore, no recommendations were made.



- 
- FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General or by an independent external auditor. OMB requires OIGs to report their responses via an automated collection tool. The evaluation objective was to perform an independent evaluation of DNFSB implementation of FISMA 2014 for FY 2016. In FY 2016, DNFSB completed implementation of all recommendations from the FY 2014 evaluation. As implementation of these recommendations occurred less than 6 months prior to the completion of the evaluation, there was not sufficient information to measure their effectiveness. Therefore, no new recommendations were made for FY 2016.
  - 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, 2016. These management and performance challenges are directly related to DNFSB's organizational culture and climate, security, administrative functions, and technical programs. OIG's work in these areas indicates program improvements are needed and DNFSB is responding positively to IG recommendations to improve the efficiency and effectiveness of its programs.

---

## *NRC Investigations*

- OIG conducted an investigation into an allegation that an NRC senior official directed regional managers to terminate a 6-month senior resident inspector (SRI) rotational assignment being temporarily filled by a GG-13 inspector. Subsequently, another regional manager instructed staff to write a position description that ensured the acting SRI got a permanent GG-14 SRI position, thereby preselecting this individual for the permanent SRI position.
- OIG conducted an investigation into an allegation that a former senior official created a strong perception of a conflict of interest by highlighting his efforts to reduce the costs of regulatory compliance in his publicly available online resume.
- OIG conducted an investigation into an allegation that an NRC regional employee had, without authorization, taken a Government-issued laptop computer to an unauthorized computer vendor for repair. When the vendor found that it was not feasible to repair the computer, the vendor destroyed the computer. This resulted in the computer not being accounted for during an NRC periodic property inventory.
- OIG conducted an investigation into anonymous allegations pertaining to hiring practices and vacancy promotion selections by NRC regional management. Specifically, the allegations questioned the selections of two branch chiefs, reassignments of two branch chief positions, and promotion of an individual into a Senior Executive Service deputy director position. The investigation also addressed whether a regional manager had hired a family member into the manager's division.
- OIG conducted an investigation into an allegation that an NRC employee engaged in harassing behavior towards another NRC employee and provided derogatory information to an Office of Personnel Management investigator.

---

# 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*, 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 containment building.*



---

# 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 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.

---

## *Investigation Program*

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

Because NRC's mission is to protect the health and safety of the public, OIG's Investigative Program directs much of its resources and attention to investigating allegations of NRC staff conduct that could adversely impact matters related to health and safety. These investigations may address 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, 2016, to March 31, 2017, OIG reviewed a variety of agency documents including Commission papers (SECYs), Staff Requirements Memoranda, Federal Register Notices, MDs, regulatory actions, and statutes.

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

### NRC

Draft MD 4.3, *Financial Management Systems*—OIG suggested that the role of the Chief Human Capital Officer and the Federal Personnel/Payroll System be further described in the MD.

Draft update of the *NRC Domestic Violence Policy*—OIG stated the definition of “Employee” appeared to be overly broad. Under “Sexual Assault,” the language referencing “disciplinary action” as a basis for lack of consent also appeared to be overly broad. For Workplace Flexibilities, inclusion of the “employee’s family members” may be out of the scope of authority for this policy. Under “Disciplinary Actions,” the use of the term “retaliatory” may not be appropriate. OIG further suggested the inclusion of guidance on structuring reports to facilitate protection of individual identity (e.g., use position titles instead of names).



---

Draft MD and Handbook (DH) 11.7, *NRC Procedures for Placement and Monitoring of Work with Federal Agencies and the U.S. Department of Energy Laboratories*—OIG suggested guidance on specific citations and substantive advice on the Statement of Work (SOW) provision, noting that, this section stresses that the “SOW is the most important element of the entire agreement,” but failed to include some important aspects of the SOW. OIG suggested supplementing this section with the fact that the SOW defines the project, and includes specific activities such as deliverables and timelines for the vendor.

Draft MD and DH 5.10, *Formal Qualifications for Integrated Materials Performance Evaluation Program (IMPEP) Team Members and Team Leaders and Safety and Safeguards Self-Assessments—111, Formal Qualifications for Integrated Materials Performance Evaluation Program Team Members and Team Leaders*—OIG suggested technical corrections to class/course titles and also suggested that the MD include Agreement State personnel acting as IMPEP team members and team leaders in the applicability provision.

Draft MD and DH 5.12, *International Nuclear and Radiological Event Scale Participation*—OIG noted that the language describing two different positions in the draft appeared to be identical, without distinguishing responsibilities for each of these positions.

## **DNFSB**

Draft DNFSB Directive D-6XX, *Hatch Act Program*—OIG suggested correction of the draft to provide that alleged violations of political activity laws and regulations are reported to and investigated by the Office of Special Counsel.

Draft DNFSB Directive, *Employee Awards and Recognition Program*—OIG suggested that “Federal contractor personnel” should be deleted from the program, noting that Government employee awards to contractor personnel violate requirements related to non-personal services contracting and limitations on contractor performance of inherently governmental functions.

Draft DNFSB Directive D-622 *Alternate Dispute Resolution (ADR)*—OIG suggested changes to the draft to provide, that ADR should not be used in cases involving criminal, insider threat, or security allegations or issues. Further, that these matters should be reported to the Inspector General.

Draft DNFSB Directive D-XXX *Phased Retirement Program*—OIG suggested including requirements and details expected in identified reports and noted the need for additional specificity in definitions provided in the draft.

---

## *Other OIG Activities*

### **New Assistant Inspector General for Audits**

On October 31, 2016, Dr. Brett M. Baker became the new Assistant Inspector General for Audits (AIGA) in the NRC/OIG. Previously Dr. Baker served as the Deputy Inspector General for Audit for the Department of Defense OIG. He also worked as the AIGA at the National Science Foundation OIG, AIGA at the U.S Department of Commerce OIG, and the Director for Internal Review at the Defense Finance and Accounting Service.

Dr. Baker earned a doctorate in Information Technology and Systems Management from the University of Maryland. He holds a Master's Degree in Information Systems Management from Central Michigan University, a bachelors' degree in Accounting from the University of Northern Iowa, and a bachelors' degree in Sociology from Iowa State University. He is a Certified Public Accountant and a Certified Information Systems Auditor. Dr. Baker is also an Army veteran, having served in the U.S. Army Signal Corps.



Dr. Baker serves as the Chair of the Federal Audit Executive Council, and is a member of the Accounting and Auditing Policy Committee of the Federal Accounting Standards Advisory Board. In addition, he serves on the Government Accountability Office Yellow Book Advisory Council and the Green Book Advisory Council. He has published articles on auditing and data analytics, and is a frequent speaker at national conferences. Dr. Baker is a recipient of the 2015 Donald L. Scantlebury Memorial Award for Distinguished Leadership in Financial Management Improvement. He has also received four Awards for Excellence from the Council of the Inspectors General on Integrity and Efficiency.

### **OIG General Counsel Addresses Honor Law Graduate Attorneys**

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

---

# NRC MANAGEMENT AND PERFORMANCE CHALLENGES

## Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission\* as of October 1, 2016 *(as identified by the Inspector General)*

Challenge 1 *Regulation of nuclear reactor safety programs.*

Challenge 2 *Regulation of nuclear materials and radioactive waste programs.*

Challenge 3 *Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.*

Challenge 4 *Management of information technology and information management.*

Challenge 5 *Management of financial programs.*

Challenge 6 *Management of administrative functions.*

*\*For more information on the challenges, see OIG-17-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC, <http://pbadupws.nrc.gov/docs/ML15274A142.pdf>*



# NRC AUDITS

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

## Audit Summaries

### Audit of NRC’s Oversight of Source Material Exports to Foreign Countries

#### OIG Strategic Goal: Safety

NRC’s mission is to regulate the Nation’s civilian use of nuclear materials to ensure protection of public health and safety, promote the common defense and security, and protect the environment. One of the agency’s statutorily mandated responsibilities under the Atomic Energy Act of 1954, as amended, is to license the import and export of nuclear materials.

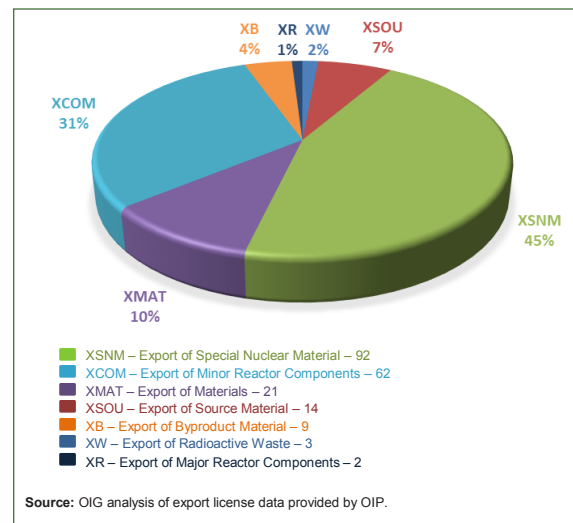
As a regulator, NRC fulfills one of its principal regulatory functions through oversight. Oversight consists of performance assessment, such as inspections and site visits, to verify licensee activities are properly conducted, and to ensure safe and secure operations in accordance with NRC’s regulations.

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.

Two NRC program offices are involved in the oversight of the export of source material. The Office of International Programs (OIP) licenses exports and imports, performs rulemaking activities associated with export and import of nuclear equipment and material, reviews nuclear nonproliferation initiatives, and develops international safeguards policy. The Office of Nuclear Material Safety and Safeguards (NMSS) provides technical reviews of export and import license applications to identify any potential proliferation concerns, and evaluates the adequacy of OIP’s export/import licensing reviews. Additionally, regional offices can potentially be involved should regional inspectors be called upon to perform material inspections, including those related to source material.

The audit objective was to determine the effectiveness of NRC’s oversight of the export of source material.

Export Licenses Issued from 2011–2015



---

### *Audit Results:*

NRC provides effective oversight of source material exports in coordination with other Federal agencies; however, opportunities for improvement exist within NRC's internal processes.

Specifically, OIG identified the need for NRC to

- Create an export inspection program.
- Clarify specific NRC regulations related to exports.
- Create a qualification program for export licensing officers.

### **No Prelicensing Site Visits or Source Material Export Inspections**

Federal regulations state each export licensee (1) must have an office in the United States, (2) shall maintain their export records for 5 years, and (3) shall maintain adequate safeguards against tampering with and loss of these records. The regulations also state that export licensees shall permit NRC to inspect their records, premises, and activities when necessary to fulfill the requirements of the *Atomic Energy Act*.

NRC has not performed prelicensing site visits to ensure that entities applying for an export license have a physical office in the United States where records would be kept and safeguarded, nor has NRC conducted source material export licensee inspections to verify that export activities are conducted in accordance with NRC's regulations. The lack of any prelicensing site visits is especially significant for applicants such as export brokers or carriers who, unlike shippers, are not inspected under any other NRC oversight program.

Prelicensing site visits and source material export inspections are not conducted because NRC does not require them and does not have sufficient controls in place to perform such verification and oversight activities. Specifically, NRC does not have export inspection procedures or inspection manual chapters requiring the need for site visits or export inspections to verify licensee compliance with Federal requirements.

Without prelicensing site visits and export inspections, NRC is not adequately fulfilling one of its regulatory functions—oversight. Additionally, NRC cannot confirm if export license applicants are legitimate and will use an export license for its intended purpose and in accordance with their licenses and regulations.

### **Incomplete Verification of Licensing Requirements**

Federal regulations state export applications must contain the name and address of the main applicant, and the name and address of any other party if different from the applicant. Additionally, carriers must have a specific license to possess source material if exporting over 500 kilograms of natural uranium per shipment.

OIG concluded that NRC does not enforce the requirement that all parties, including carriers, be listed on the export application, nor does it confirm if carriers have a license to possess source material if transporting over 500 kilograms per shipment of natural uranium for export purposes. This was verified during the audit when OIG identified 32 of 36 (nearly 89 percent) source material export applications that did not list any carriers. Collectively, these applications authorized the export of nearly 50 million kilograms of source material. Involved headquarters and regional staff as well as individuals from Agreement States further corroborated OIG's conclusion during the audit, noting they do not verify if carriers have the required license.

NRC staff do not enforce the requirement to list carriers on the export application because of confusion regarding the applicability of Federal regulation requirements as well as conflicting views regarding who is responsible for enforcing the requirement. Furthermore, NRC has not developed a qualification program or formalized training to promote better understanding and more consistent application of Federal requirements pertaining to oversight of source material exports among NRC licensing officers.

Not enforcing Federal regulations and neglecting to develop a qualification program or formalize training for NRC licensing officers will result in continued non-compliance among licensees while the potential for safety and security vulnerabilities increases. Consequently, NRC's ability to uphold its mission to regulate the Nation's civilian use of radioactive materials to protect public health and safety, promote the common defense and security, and protect the environment is compromised.

*(Addresses Management and Performance Challenge #2)*

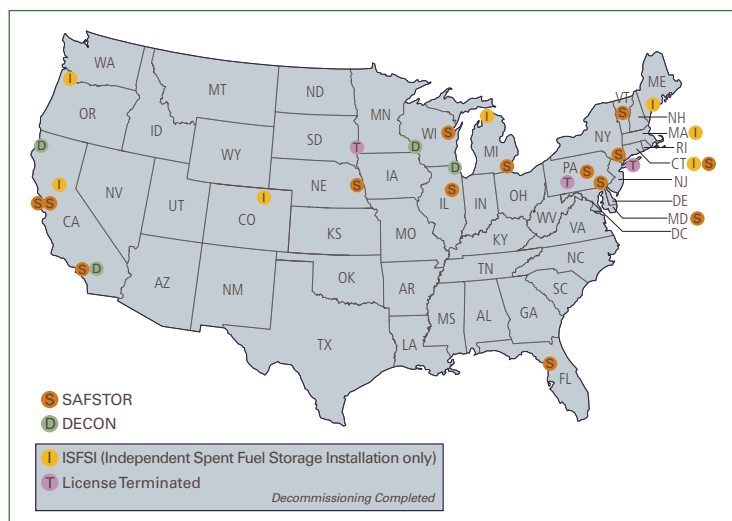
## Audit of NRC's Oversight of Security at Decommissioning Reactors

### OIG Strategic Goal: Security

NRC regulates the decommissioning of commercial nuclear power plants. Decommissioning is the process used to safely remove a nuclear power plant from service and reduce residual radioactivity to a level that permits release of the property and termination of its license (see 10 CFR 50.2).

NRC has rules governing power plant decommissioning that protects workers and the public during the decommissioning process. In addition, NRC has regulations for

Power Reactors Decommissioning Status



---

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.

***Audit Results:***

NRC's oversight of security at decommissioning reactors provides for adequate protection of radioactive structures, systems, and components. However, NRC can improve its oversight by clarifying regulatory requirements related to the insider mitigation program and fatigue management. NRC is currently taking steps to address both issues. Presently, there are ongoing rulemaking efforts in the area of decommissioning. Additionally, NRC recently finalized a report to document lessons learned associated with permanent power reactor shutdowns that occurred from 2013–2016.

NRC promotes five *Principles of Good Regulation* in carrying out the agency's mission. The principles address independence, openness, efficiency, clarity, and reliability. The principles focus on ensuring safety and security while appropriately balancing the interests of NRC's stakeholders, including the public and licensees. The principle of clarity states that regulations should be coherent, logical, and practical. For reliability, regulations should be based on the best available knowledge from research and operational experiences. Furthermore, regulatory actions should always be fully consistent with written regulations and should be promptly, fairly, and decisively administered so as to lend stability to nuclear operational and planning processes.

NRC regulations lack clarity in identifying which fitness-for-duty program elements must be implemented in order to satisfy the requirements of the insider mitigation program. 10 CFR Part 73.55(b)(9) requires licensees to establish, maintain, and implement an insider mitigation program and describe the program in their physical security plan. The program must be maintained as long as spent fuel remains in the reactor core or in the spent fuel pool and until the licensee comes under security requirements established for interim spent fuel storage. Additionally, the insider mitigation program must contain elements from the fitness-for-duty program in 10 CFR Part 26. However, 10 CFR Part 73 does not describe which fitness-for-duty elements are to be implemented for the insider mitigation program for 10 CFR Part 50 licensees, including decommissioning licensees.

Current regulatory guidance does not describe appropriate program elements during decommissioning to provide assurance that an effective program will be maintained. NRC staff and licensees agree there are elements from 10 CFR Part 26 that should be implemented as part of the insider mitigation program. Specifically, the drug and alcohol testing, employee assistance program, and behavioral observation are all cited by interviewees as especially important for licensees to implement.

NRC regulations and guidance are unclear on which elements of the fitness-for-duty program must be implemented for decommissioning 10 CFR Part 50 licensees because



---

10 CFR Part 26 does not apply following a licensee's 10 CFR 50.82 certifications. In addition, the agency's guidance, Regulatory Guide 5.77, does not incorporate current insights gained from industry and NRC staff lessons learned, inspections, and operating experience.

The insider mitigation program is designed to help identify an individual who may represent an insider threat by addressing a broad context of trustworthiness and reliability issues. For example, an individual with protected or vital area access, or access to digital computer and communications systems and networks from outside the protected area, can pose a significant threat to the security of a nuclear power plant. Without regulatory clarity and established guidance, future decommissioning licensees, including those that may unexpectedly cease operations, may choose not to implement all parts of the fitness-for-duty program. And, given that Oyster Creek, Pilgrim, and Palisades have indicated their intent to cease operations by the end of 2019, it is crucial for NRC to clarify regulatory requirements.

*(Addresses Management and Performance Challenge #3)*

## **Audit of NRC's Foreign Assignee Program**

### *OIG Strategic Goal: Security*

Under the foreign assignee program, NRC invites peers from other nuclear safety regulators to obtain experience that would enhance safety programs and research programs worldwide, as well as promote exchange of technical information and expertise. Foreign assignees remain employees of the sponsoring regulatory or research organization in their home country. Approximately 80 foreign nationals have worked as assignees at NRC since 2005, representing 21 countries.

The Office of International Programs has primary responsibility for the foreign assignee program and coordinates with other offices through the process of onboarding a foreign assignee and during the assignment. In recent years, assignees have worked in various offices at NRC headquarters and in NRC regional offices.

OIG conducted this audit to assess whether the NRC foreign assignee program provides adequate information security.

Federal standards designate management as responsible for providing procedures that serve as a mechanism to support efficient operations, reliable reporting and communication, and reasonable assurance that requirements are met. The U.S. Government Accountability Office *Standards for Internal Control in the Federal Government* (2014) states that effective procedures document control activities designed to achieve objectives and respond to risk, especially for complex processes. Management must communicate internally the information needed to achieve objectives. Additionally, NRC policies for the foreign assignee program appear in MDs. MD 5.13, *NRC International Activities Practices and Procedures*, has a brief synopsis of the purpose of the program, processing of assignees, onboarding assignees, and supervision.

---

The requirements for information security are published in the security MDs 12.1, *NRC Facility Security Program*; 12.3, *NRC Personnel Security Program*; and 12.5, *NRC Cybersecurity Program*. The directives assign responsibilities and establish requirements for the contents of security plans, supervision and monitoring of assignees, and access restriction to prevent unauthorized access to sensitive information.

***Audit Results:***

The existing foreign assignee program policies establish controls for protection of and access to information within the foreign assignee program. However, improvements are needed to better implement policies and strengthen information security. For example, information security requirements for the foreign assignee program are not implemented consistently because there is no specific procedure to guide implementation of those requirements. Additionally, program offices may not be able to maintain adequate information protection.

Foreign assignees access a non-NRC, external email account using their NRC desktop computer and Internet access. However, NRC does not know how the assignee uses the account, nor do NRC's security plans for foreign assignees mention or guide the use of email by foreign assignees. Foreign assignees use external email accounts because NRC email is available only with access to the local-area network, which assignees are not granted because they do not meet the agency's access standards for information security. However, NRC is not able to mitigate weaknesses or detect improper use of the external email, which poses the risk of unintentional spillage of sensitive information.

*(Addresses Management and Performance Challenge #3)*

## **Digital Accountability and Transparency Act of 2014 Readiness Assessment for the Nuclear Regulatory Commission**

### ***OIG Strategic Goal: Corporate Management***

The *Digital Accountability and Transparency Act of 2014* (DATA Act) was enacted May 9, 2014, and among other things, requires that Federal agencies report financial and payment data in accordance with data standards established by the Department of the Treasury and the Office of Management and Budget (OMB). In addition, the DATA Act requires that agency Inspectors General review statistical samples of the data submitted by the agency under the DATA Act and report on the completeness, timeliness, quality, and accuracy of the data sampled and the use of the data standards by the agency. The DATA Act provides for this oversight by requiring a series of oversight reports from agency Inspectors General and the Comptroller General of the United States providing their assessment of the completeness, timeliness, quality, and accuracy of data submitted.

The readiness assessment, conducted by Miracle Systems, LLC, under a contract with OIG, concentrated on steps 1 through 4 of the Agency 8-Step Plan as described in the Department of the *Treasury's Data Act Implementation Playbook, Version 2.0*.

---

The readiness assessment objective was to determine if NRC is on track to implement DATA Act requirements by the May 2017 deadline.

***Assessment Results:***

The assessment determined that NRC is on track to implement DATA Act requirements by the May 2017 deadline.

*(Addresses Management and Performance Challenge #4)*

## **Results of the Audit of the NRC's Financial Statements for Fiscal Years 2015 and 2016**

### ***OIG Strategic Goal: Corporate Management***

The *Chief Financial Officers Act of 1990*, as amended, requires the Inspector General or an independent external auditor, as determined by the Inspector General, to annually audit NRC's financial statements to determine whether the agency's financial statements are free of material misstatement. The audit, conducted by Clifton Larson Allen, LLP, 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 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 Elimination and Recovery Act* (IPERA).

### ***Audit Results:***

**Opinion:** 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.

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

*(Addresses Management and Performance Challenge # 5)*

---

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

### *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. OMB requires OIGs to report their responses to OMB's annual FISMA reporting questions via an automated collection tool.

The evaluation objective was to perform an independent evaluation of NRC implementation of FISMA 2014 for FY 2016. This evaluation was performed by Richard S. Carson & Associates, Inc., under a contract with OIG.

### *Evaluation Results:*

NRC has continued to make improvements in its information technology security program and progress in implementing the recommendations resulting from previous FISMA evaluations. However, the audit identified three repeat findings from prior FISMA evaluations:

- Continuous monitoring activities were not performed for all NRC systems.
- NRC did not provide the OIG with a complete inventory for review.
- NRC did not provide a current system inventory of all contractor systems and did not provide requested documentation to demonstrate oversight of contractor systems is performed.

There were no new findings for FY 2016. Recommendations for the repeat findings were made in prior reports, and implementation of those recommendations is being tracked through the OIG followup process.

*(Addresses Management and Performance Challenge #3)*



## Audit of NRC’s Oversight of Low-Level Radioactive Waste (LLRW) Disposal and Waste Blending

### OIG Strategic Goal: Safety

LLRW includes items that have become contaminated with radioactive materials or have become radioactive through exposure to neutron radiation. NRC classifies LLRW at the time of disposal based on its radioactivity. NRC has specified disposal and waste requirements for three classes of waste—Classes A, B, and C—with progressively higher concentrations of radioactive material. As waste class increases, additional measures to control the hazard to the public are required.

Commercial LLRW can be disposed of in facilities licensed by either NRC or Agreement States. The *Low-Level Radioactive Waste Policy Amendments Act of 1985* gave the States responsibility for LLRW disposal. There are four disposal facilities—all are located in Agreement States. Current LLRW disposal practices use shallow land disposal sites either with or without concrete vaults. NRC oversees the safety of these Agreement State sites through a review process called the Integrated Materials Performance Evaluation Program.

Blending of LLRW means mixing wastes of different concentrations to create a product with more uniform radionuclide concentrations. The purpose of blending higher and lower activity waste is to lower the overall concentration of radioactivity. The mixture would then be suitable for disposal at more locations and at a lower cost.

The Office of Nuclear Material Safety and Safeguards is responsible for regulating activities which provide for the safe and secure production of nuclear fuel used in commercial nuclear reactors, including the disposal of radioactive waste and spent nuclear fuel. In addition, the Office of Nuclear Reactor Regulation develops and implements rulemaking, licensing, oversight, and incident response programs for nuclear reactors. This office also provides support to regional staff that conduct inspections of LLRW at nuclear reactor sites.

Each of NRC’s four regional offices plays a role in the oversight of LLRW as well. These regional offices execute established NRC policies and programs related to inspection, licensing, and enforcement for both reactor and non-reactor licensees.

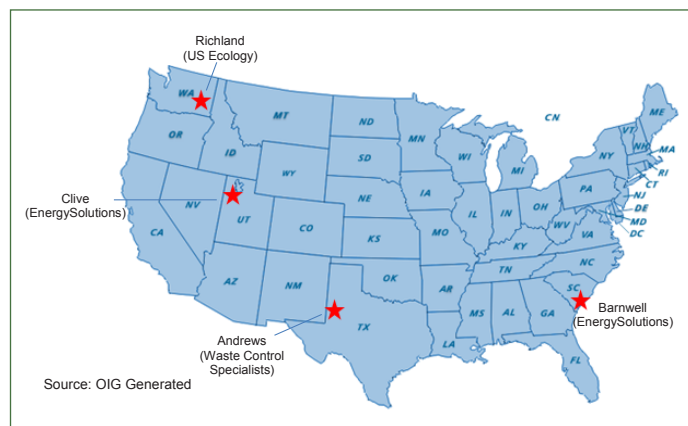
The audit objective was to determine if the disposal and waste blending processes at disposal facilities are done safely and effectively.

Table 1: Classes of LLRW

Low-Level Radioactive Waste	
Class of Waste	Definition
A	Represents the greatest volume and the lowest risk.
B	Represents much less volume but greater risk.
C	Represents the smallest volume and the greatest risk.

Source: NRC

Figure 1: LLRW Disposal Facilities



---

***Audit Results:***

OIG found that NRC provides adequate oversight of LLRW disposal and blending processes through inspection activities. The audit did not identify any findings. Therefore, this memorandum report does not make any recommendations. However, an opportunity exists to enhance the effectiveness and efficiency of the LLRW program through centralizing LLRW guidance, thereby enhancing stakeholder accessibility.

*(Addresses Management and Performance Challenge #2)*

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

### *OIG Strategic Goal: Corporate Management*

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, 2016. These management and performance challenges are directly related to NRC's mission areas: 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 Adoption of Cloud Computing**

#### *OIG Strategic Goal: Security*

Cloud computing refers to information technology services that allow delivery of on-demand computing solutions through the use of converged infrastructure and shared services. Cloud computing frees up organizations from having to invest in technology infrastructure, and allows them to focus resources on their actual business, get applications up and running faster, achieve greater agility in meeting fluctuating business requirements, and improve systems manageability and maintenance.

OMB established the *Federal Cloud Computing Strategy*. The strategy instituted a 'cloud-first' policy designed to accelerate the adoption and usage of cloud computing technologies by Federal agencies. The General Services Administration established the *Federal Risk Authorization Management Program* (FedRAMP), which provides a standard, centralized approach to assessing cyber controls and authorization of cloud computing based systems. All Federal agencies must use the FedRAMP process for doing security assessments, authorizations, and continuous monitoring of cloud services.

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

*(Addresses Management and Performance Challenge #3)*

### **Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2017**

#### *OIG Strategic Goal: Security*

FISMA 2014 requires an independent evaluation of NRC's information security program and practices. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security. In FY 2017, OIG will also evaluate each regional office's implementation of FISMA 2014.

FISMA 2014 provides the framework for securing the Federal Government's information technology including both unclassified and national security systems. All agencies must implement the requirements of FISMA 2014 and report annually to OMB and Congress on the effectiveness of their security programs.

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

*(Addresses Management and Performance Challenge #3)*

---

## Evaluation of NRC's Network Storage Service Interruption

### *OIG Strategic Goal: Security*

The evaluation will review the current information technology service contract as well as the future contract to identify any areas of improvement and possible solutions to prevent a future recurrence of NRC network storage service interruption. This evaluation was not included in the FY 2017 Annual Plan.

The evaluation objective is to evaluate the NRC network storage service interruption that occurred on November 16, 2016.

*(Addresses Management and Performance Challenge #4)*

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

### *OIG Strategic Goal: Safety*

NRC must approve any package used for shipping nuclear material before shipment. If the package meets NRC requirements, NRC issues a Radioactive Material Package Certificate of Compliance (CoC) to the organization requesting approval of a package. For a transportation package to be certified by the NRC, it must be shown by actual test or computer analysis to withstand a series of accident conditions.

To apply for a CoC to ship nuclear material, an organization must submit an application to NRC for review and approval. The application must address the safety and operational characteristics of the package analyses for structural and thermal design, radiation shielding, nuclear criticality, and material content confinement. After reviewing this information, NRC determines whether to grant a CoC. Ensuring NRC's oversight for issuing a CoC for a radioactive material package is essential to public health, safety, and the environment.

The audit objective is to determine if NRC's processes for issuing CoCs and reviewing 10 CFR Part 72.48 changes for radioactive material packages provides adequate protection for public health, safety, and the environment.

*(Addresses Management and Performance Challenge #2)*



---

## **Audit of NRC's PMDA and DRMA Functions To Identify Program Efficiencies**

### *OIG Strategic Goal: Corporate Management*

The Program Management, Policy Development and Analysis (PMDA) function at NRC headquarters offices and the Division of Resource Management and Administration (DRMA) function at NRC regional offices manage service delivery in support areas such as administration, human capital, budget, contract management, and information management/technology. These organizations address individual office support needs depending on the specific mission of each office. They perform functions that are specific to their organization, functions that are common across all the PMDA/DRMA organizations, and functions that were transferred from other offices. The FY 2016 budget included more than 200 staff positions for PMDA/DRMA functions.

The audit objective is to determine if the activities performed by NRC's PMDA/DRMA programs produce the intended results from operational processes in a manner that efficiently and effectively uses resources.

*(Addresses Management and Performance Challenge #6)*

## **Audit of NRC's Contract Administration Process**

### *OIG Strategic Goal: Corporate Management*

The Federal Acquisition Regulation (FAR), NRC Acquisition Regulations, and Management Directive 11.1, *NRC Acquisition of Supplies and Services*, discuss the importance of contract administration criteria that NRC uses for contract administration. According to the FAR, only Contracting Officers (CO), acting within the scope of their authority, are able to enter into and administer contracts. However, COs may, when appropriate, delegate responsibility for specific contract administration or technical supervision tasks to a Contracting Officer's Representative (COR). CORs may not redelegate any authority delegated to them by the CO.

CORs and COs are required to take biennial training to maintain certification as contracting professionals. CORs are responsible for the daily administration and technical direction of a contract during the period of performance. These responsibilities can include: verifying deliverables against contract terms, reviewing and reconciling invoices, monitoring contract funding, overseeing contractor performance, addressing security requirements for onsite contractors, on/off boarding of contractor staff, and verifying support for Intra-Governmental Payment and Collection.

The audit objective is to assess the effectiveness of NRC's compliance with applicable contract administration requirements.

*(Addresses Management and Performance Challenge #6)*

---

## Audit of NRC's Purchase Card Program

### *OIG Strategic Goal: Corporate Management*

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

Under the Charge Card Act, Inspectors General are required to conduct periodic risk assessments of agency purchase card programs to analyze the risks of illegal, improper, or erroneous purchases. Status reports on Inspectors General purchase card audit recommendations, if any, were to be submitted to OMB by January 31, 2017, for compilation and transmission to Congress and the U.S. Comptroller General.

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

*(Addresses Management and Performance Challenge #6)*

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

### *OIG Strategic Goal: Corporate Management*

On July 22, 2010, the *Improper Payments Elimination and Recovery Act of 2010* (IPERA) was signed into law, which amended *Improper Payments Information Act of 2002* (IPIA). IPERA requires Federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. The *Improper Payments Elimination and Recovery Improvement Act of 2012* (IPERIA) was signed into law on January 10, 2013. This law established the *Do Not Pay Initiative*, which directs agencies to verify the accuracy of payments using databases before making payments.

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

*(Addresses Management and Performance Challenge #5)*

---

## **Audit of NRC's 10 CFR 2.206 Petition Review Process**

### *OIG Strategic Goal: Safety*

The NRC considers public involvement in its activities a cornerstone of appropriate regulation of the nuclear industry. One opportunity it provides for its stakeholders to express their opinions is the petition process outlined in 10 CFR 2.206. This process allows members of the public to petition the NRC to take enforcement action, such as modifying, suspending, or revoking an NRC-issued license, to resolve a problem. When NRC receives a 2.206 petition, staff review it against criteria to determine if it should be accepted for evaluation or rejected. A petition undergoing this review is referred to as a petition under consideration. Rejection of a petition is communicated in a closure letter. If a petition has been accepted for further evaluation, it is considered an open petition until the staff formally grants or denies the requested action in a Director's Decision.

As of September 2016, NRC had eight 2.206 petitions under consideration and one open 2.206 petition. According to agency timeliness goals, staff are expected to issue a preliminary Director's Decision within 120 days of receiving and formally acknowledging a petition. Petitioners may then comment on the preliminary Director's Decision. A final Director's Decision is expected within 45 days of comment period closure.

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

*(Addresses Management and Performance Challenge #1)*

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

### *OIG Strategic Goal: Safety*

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

Employees assigned to voluntary standards and professional organizations such as ASME must adhere to NRC and other Federal regulations to prevent conflicts of

---

interest, misuse of Government position and resources, and actions that could directly and predictably affect the financial interests of that organization or members of that organization. Federal regulations and standards also require NRC to establish procedures to ensure employees serving on voluntary standards organizations and professional organizations while on official duty adhere to ethical and other agency requirements.

The audit objective is to assess NRC's oversight and compliance with applicable law, regulation, and policy relating to NRC employee participation in ASME Code Committees.

*(Addresses Management and Performance Challenge #6)*

## **Audit of NRC's Fire Protection Oversight**

### *OIG Strategic Goal: Safety*

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

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

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

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

*(Addresses Management and Performance Challenge #1)*



---

## Evaluation of Proposed NRC Modifications to the Probabilistic Risk Assessment Process

### *OIG Strategic Goal: Safety*

NRC uses Probabilistic Risk Assessment (PRA) modeling to estimate risks of potential accidents at nuclear power plants. PRA provides insights into the strengths and weaknesses of the design and operation of a nuclear power plant. For operating plants in the United States, a PRA can estimate three levels of risk, including the following:

- Level 1 PRA estimates the frequency of accidents that cause damage to the nuclear reactor core. This is commonly called core damage frequency.
- Level 2 PRA estimates the frequency of accidents that release radioactivity from the nuclear power plant based on Level 1.
- Level 3 PRA starts with Level 2 radioactivity release accidents and estimates the injury consequences to the public and environmental damage.

NRC is currently exploring a potential shift to using PRA models developed and maintained by licensees to replace the agency's Standardized Plant Analysis Risk models. In undertaking such a major change to existing procedures, NRC should consider a variety of factors, including gain of efficiencies, transition costs, and potential new training and skills that may be required in the use of newer and different risk models. NRC will also have to evaluate the potential for NRC staff having access to additional licensee proprietary information as well as the impact the change will have overall on NRC's ability to be an independent regulator.

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

*(Addresses Management and Performance Challenge #1)*



*Power lines from Indian Point Nuclear Power Station.*

---

# NRC INVESTIGATIONS

*During this reporting period, OIG received 87 allegations, initiated 19 investigations, and closed 15 cases. Of the 15 closed cases, 6 resulted in issued reports.*

## *Investigative Case Summaries*

### **Alleged Pre-Selection by NRC Regional Management**

#### *Strategic Goal: Corporate Management*

OIG completed an investigation into an anonymous allegation that in January 2016, an NRC senior official directed regional managers to terminate a 6-month senior resident inspector (SRI) rotation assignment being filled by an inspector. This inspector had received a temporary promotion from a GG-13 position to a GG-14. Subsequently, during a meeting with regional branch chiefs, a division director allegedly instructed managers to write a position description for a GG-14 SRI that ensured the inspector who had received the temporary promotion while on rotational assignment would receive the permanent GG-14 SRI position, thereby preselecting this individual for the permanent SRI position.

According to a senior NRC human resource specialist, the region's actions in filling the temporary SRI position at a nuclear power plant in 2015 and 2016 were accomplished in accordance with guidance contained in MD 10.1, *Recruitments, Appointments and Merit Staffing*. Specifically, under the Management Directive, 180 day temporary, non-competitive promotions are allowed. The region initially requested to extend the resident inspector's non-competitive promotion; however, the request was not approved. The region was advised to competitively advertise the position through a job announcement after the first 180 day period ended because of a continuing need for the position. Subsequently, a GG-14 vacancy for the SRI position was competitively announced in January 2016. The temporary GG-14 promotion was not to exceed 1 year.

According to a regional branch chief, two individuals applied for the position and made the certification list, including the resident inspector who was acting in the temporary SRI position. The acting SRI was later selected to fill the temporary GG-14 position. According to the branch chief, this individual was fully qualified and met the certification criteria for the SRI position.

#### *Investigative Results:*

OIG did not substantiate that any misconduct by regional managers pertaining to either the non-competitive temporary promotion or the competitive temporary promotion for the SRI position. Both the non-competitive and competitive temporary promotions were allowed under guidelines established in MD 10.1.

*(Addresses Management and Performance Challenge #7)*



---

## **Alleged Conflict of Interest by a Former Senior Official of the Office of Nuclear Reactor Regulation**

### *Strategic Goal: Corporate Management*

OIG conducted this investigation based on an allegation that a former senior official in the Office of Nuclear Reactor Regulation (NRR) created a strong perception of a conflict of interest by highlighting the former official's efforts to reduce the costs of regulatory compliance in the official's publicly available resume. This former official subsequently accepted a position as a vice president at an NRC licensee nuclear facility. This investigation addressed whether the former senior official's actions, before and since departing NRC, constituted a conflict of interest or created the appearance of a conflict of interest under applicable law and regulation.

OIG reviewed the former official's publicly available resume, and found that it contained a consistent and recurring emphasis on cost savings to (the nuclear) industry, with a summary stating, "Pay me a nickel and I will return to you \$100." The resume indicated the former official's abilities in "influencing" and "connecting." It contained bullet points, including "Saved the commercial energy generation industry \$1.6 billion," and repeatedly referenced the nuclear industry as the former official's "customer" at the NRC. The resume provided a list of positions while employed at NRC and cited the former official's supervision of 128 staff members and oversight of \$12M in contracts.

During an OIG interview just prior to the former official's departure from NRC, the official acknowledged awareness of a general 1-year prohibition against representing a licensee before NRC, and a 2-year prohibition for anything that the official was involved in that was "substantial." The former official confirmed that upon deciding to pursue employment in the nuclear industry, the official notified the Office of the General Counsel (OGC) that he was doing so.

According to an OGC Ethics Attorney, the former official had advised OGC in writing, per the appropriate process, that the official was in consideration for a vice president position with a nuclear facility. OIG reviewed an email from the former official to OGC that reflected the official's awareness of the responsibility to recuse himself/herself from any dealings with the licensee.

Subsequently, following the former official's departure from NRC, the former official and licensee personnel attended a meeting with NRC regional management and resident staff. The former official did not make any remarks during the meeting. The licensee management subsequently attempted to arrange the former official's attendance at another meeting with NRC staff at another nuclear power plant. NRC managers took the stance that if the former official had actually shown up at the meeting in question, they would have asked the former official to leave. According to the managers the former official did not attend the meeting and no interaction occurred on that day.

### *Investigative Results:*

OIG did not substantiate that the former official violated criminal conflict of interest statutes either prior to or after his departure from the NRC. However, OIG found that the former official's publicly available resume created an appearance of impropriety that



---

could have been administratively actionable had the official remained in Government service. OIG also found that the former official's actions after taking the position with the licensee were sufficiently close to the margin of potentially restricted activity as to require additional notification from the NRC OGC to the former official and to NRC staff who might come into contact with the former official of their obligations under Federal law and ethics guidelines. In addition, the licensee's proposals for the former officials participation in several meetings with NRC staff and management during the first year of the official's tenure were viewed by NRC management, with the concurrence of OGC, as potentially risking violations of Federal conflict of interest statutes. All such proposals were rejected by NRC: therefore, no violations occurred.

*(Addresses Management and Performance Challenge #7)*

## **Unauthorized Possession and Destruction of a Government Computer Assigned to a Regional Employee**

### *Strategic Goal: Security*

OIG conducted an investigation into an allegation that an NRC employee had, without authorization, taken a Government issued laptop computer to an unauthorized computer vendor for repair. This vendor was a private company and not affiliated with the NRC or the Federal Government. When the vendor found that it was not feasible to repair the computer, the company destroyed the computer. This resulted in the computer not being accounted for during a periodic regional property inventory conducted in March 2016.

OIG reviewed an NRC Form 395, "Report of Property for Survey," generated from NRC property records and partly filled out by the NRC employee after the destruction of the computer, which listed the computer's acquisition date as July 18, 2006, and its acquisition value as \$1,394.76.

OIG learned that the regional property custodian went to the employee's office to inventory the employee's NRC-issued property items, and at that time the employee informed the property custodian that the employee had taken the laptop computer to a computer repair store. According to the property custodian, the use of an outside repair vendor was unusual, and the more appropriate way to have a malfunctioning NRC computer repaired would be to request assistance from NRC regional information technology support staff.

The owner of the computer repair company advised OIG that at that time, the owner explained to the NRC employee that pursuant to the vendor's standard practice and policy, the computer had been destroyed because it had been deemed unrepairable and because the employee, despite multiple notifications by email, text, and voicemail in the 6-month period since the computer had been provided to the vendor, had not sought to retrieve the computer until March 12, 2016.

The NRC regional employee told OIG that the employee took the NRC computer to the vendor in October 2015. The vendor informed the employee they were unable to fix the computer. The NRC employee stated there had not been a chance to return

---

and retrieve the computer. According to the employee, there was no sensitive, classified or safeguards material on the computer.

***Investigative Results:***

OIG determined that the NRC employee disposed of a Government computer in a manner not authorized by NRC policy or consistent with normal NRC practice and, as a result, failed to safeguard and protect sensitive equipment as required by MD 13.1, *Property Management*, and failed to maintain the security controls necessary to provide protection for an IT asset as required by MD 12.5, *Information Security*. OIG also determined that the NRC employee took no action to retrieve the non-functional computer for approximately 6 months.

*(Addresses Management and Performance Challenge #5)*

## **Alleged Preselection by Region II Management**

***Strategic Goal: Corporate Management***

OIG conducted an investigation into anonymous allegations pertaining to hiring practices and vacancy promotion selections by NRC regional management. Specifically, the allegations questioned the (1) selections of two branch chiefs; (2) reassignments of two branch chief positions; and (3) promotion of an individual into a Senior Executive Service (SES) deputy director position. The investigation also addressed whether a regional manager had hired a family member into the manager's division.

***Investigative Results:***

OIG did not develop evidence of inappropriate hiring practices by NRC Region II management in the examples provided in the allegations. OIG found that the two branch chiefs were selected in accordance with applicable NRC Management Directive guidance. With regard to reassignment of two branch chiefs, regional management identified the need for the position reassignments and made the assignments in accordance with NRC Management Directive guidance. OIG found that the individual promoted into the deputy director SES position had completed an 18-month competitive SES candidate program. This individual was selected in accordance with guidance in NRC Senior Executive Service Employment and Staffing Programs. OIG did not find evidence of nepotism by the regional manager.

*(Addresses Management and Performance Challenge #7)*

## **False Information Provided by an NRC Employee Pertaining to a Security Related Background Investigation**

***OIG Strategic Goal: Corporate Management***

OIG conducted an investigation into an allegation that a Reactor Operations Engineer (ROE1) engaged in harassing behavior towards another Reactor Operations Engineer (ROE2). Specifically, ROE1 overwhelmed ROE2 with extensive emails, provided derogatory information to an Office of Personnel Management (OPM) background

---

investigator, and altered an NRC email, which was then provided to ROE 2 as part of the harassing behavior.

An NRC Facilities Security Specialist (FSS) told OIG that ROE2 reported that ROE1 had (1) overwhelmed ROE2 with extensive emails, (2) altered an official NRC email in furtherance of the harassing behavior, (3) inquired with NRC security and intelligence staff about potential issues involving ROE2's companion (a law enforcement officer), and (4) falsely alerted an OPM background investigator about concerns regarding ROE2's involvement with ROE2's companion. ROE2 provided FSS emails that ROE1 had sent to ROE2. According to the FSS, ROE1 was listed as a reference in ROE2's most recent OPM background investigation.

FSS advised OIG that when interviewed, ROE1 admitted to altering an NRC email that ROE1 gave to ROE2. ROE1 said the email was altered because of concerns ROE1 had about ROE2's involvement with current and former companions. ROE1 provided a written statement to FSS acknowledging that ROE1 had altered an email ROE1 received from a former NRC program manager involved in intelligence and threat assessment. After altering the February 11, 2016, email, ROE1 provided the email to ROE2.

The February 11, 2016, email from the former program manager stated, in part, "We agree that there is no concern with your co-worker with regards to security issues." ROE1 altered the February 11 email by adding two sentences, which reflected, in part, that ROE2's computer activities would be monitored.

OIG found that ROE2 contacted NRC FSS after receiving a letter from ROE1 indicating that ROE2 was about to be arrested by the Federal Bureau of Investigation. Prior to receiving that letter from ROE1, ROE2 had received other letters and documents from ROE1 stating that ROE2 was being monitored by an investigator for ROE2's security clearance, and that someone in ROE2's life was a security risk.

When interviewed, ROE1 admitted altering the February 11, 2016, email and providing it to ROE2 to read. ROE1 altered the email because ROE1 believed the former program manager never reviewed the concern that ROE2 was in a "really bad relationship and was being harassed by the companion." Also, according to ROE1, ROE2 was afraid of ROE2's companion because the companion carried a gun as part of the individual's official duties as a police officer.

### *Investigative Results:*

OIG determined that ROE1 altered the February 11, 2016, email and gave the altered email to ROE2, which contained potential security issues involving ROE2. OIG did not identify any derogatory information documented in OPM's records of its interview of ROE1 concerning ROE2. NRC issued ROE1 a Cease and Desist Letter on March 1, 2016, wherein ROE1 was ordered to refrain from any contact with ROE2. During the OIG investigation, ROE1 terminated employment with NRC.

*(Addresses Management and Performance Challenge #7)*





*NRC Resident Inspector.*



---

# 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, 2016 *(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-17-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board. <http://www.nrc.gov/docs/ML1627/ML16277A414.pdf>*

---

# DNFSB AUDITS

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

## *Audit Summaries*

### **Results of the Audit of the DNFSB's Financial Statements for Fiscal Years 2015 and 2016**

The *Accountability for Tax Dollars Act of 2002* requires the Inspector General or an independent external auditor, as determined by the IG, to annually audit the DNFSB financial statements 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 financial statement audit objective was to determine whether DNFSB's financial statements were 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 unqualified 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)*

### **Digital Accountability and Transparency Act of 2014 Readiness Assessment for the Defense Nuclear Facilities Safety Board**

The *Digital Accountability and Transparency Act of 2014* (DATA Act) was enacted May 9, 2014, and requires that Federal agencies report financial and payment data in accordance with data standards established by the Department of the Treasury and OMB. In addition, the DATA Act requires that agency Inspectors General review statistical samples of the data submitted by the agency under the DATA Act and report on the completeness, timeliness, quality, and accuracy of the data sampled and the use

---

of the data standards by the agency. The DATA Act provides for this oversight by requiring a series of oversight reports from agency IGs and the Comptroller General of the United States providing their assessment of the completeness, timeliness, quality, and accuracy of data submitted.

This assessment was conducted by Miracle Systems, LLC, under a contract with OIG, and concentrated on steps 1 through 4 of the Agency 8-step plan as described in the Department of the Treasury's *Data Act Implementation Playbook, Version 2.0*.

### ***Assessment Results:***

The assessment determined that DNFSB, through its financial services provider, the United States Department of Agriculture, is on track to implement DATA Act requirements by the May 2017 deadline. Therefore, OIG made no recommendations.

*(Addresses Management and Performance Challenge #3)*

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

The *Federal Information Security Modernization Act of 2014* (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General or by an independent external auditor. OMB requires OIGs to report their responses to FISMA reporting questions for OIGs via an automated collection tool.

The objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for Fiscal Year 2016. This evaluation was conducted by Richard S. Carson & Associates, Inc., under a contract with OIG.

### ***Audit Results:***

In FY 2016, DNFSB completed implementation of all recommendations from the FY 2014 evaluation. As implementation of these recommendations occurred less than 6 months ago, there was not sufficient information to measure their effectiveness. Therefore, there were no new findings or recommendations for FY 2016.

*(Addresses Management and Performance Challenge #2)*

---

## **Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing DNFSB**

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, 2016. 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 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:

1. Organizational culture and climate.
2. Management of security over internal infrastructure (personnel, physical, and cyber security) and nuclear security.
3. Human capital management.
4. Internal controls for technical and administrative/financial programs.

*(Addresses All Management and Performance Challenges)*

---

## *Audits In Progress*

### **Audit of DNFSB's Resident Inspector Program<sup>1</sup>**

DNFSB's mission is to provide independent analysis, advice, and recommendations to the Secretary of Energy, as operator and regulator of DOE's defense nuclear facilities, for the adequate protection of public health and safety. The enabling legislation of DNFSB authorizes its Board to assign staff to be stationed at any DOE defense nuclear facility to carry out the mission and functions of the agency. DNFSB's Board used this authority to establish and implement the Resident Inspector Program, which serves an essential function for the agency's safety oversight of DOE's defense nuclear facilities.

DNFSB resident inspectors relocate to a DOE site with defense nuclear facilities and perform direct oversight of the safety of operations. DNFSB currently has resident inspectors stationed at five DOE defense nuclear facilities. Resident inspectors advise the agency on the overall safety conditions at defense nuclear facilities and also act as DNFSB's liaison with local DOE and contractor management, state and local agencies, elected officials and their staff, stakeholder organizations, the media, and the public.

DNFSB resident inspectors serve a critical role as the Board relies on them to perform direct oversight of nuclear safety at their assigned DOE sites. Resident inspectors are expected to evaluate the physical conditions of the sites, identify and communicate safety issues to the Board and its headquarters staff, and participate in the planning and execution of safety reviews. The audit objective is to determine whether the Resident Inspector Program provides for the necessary onsite oversight of DOE facilities to adequately fulfill DNFSB's mission.

*(Addresses Management and Performance Challenge #4)*

### **Audit of DNFSB's Telework Program**

The *Telework Enhancement Act of 2010* (the Telework Act), was enacted into law with the goal of ensuring that Federal agencies more effectively integrate telework into their management plans and agency cultures. The Telework Act defines telework as a work-flexibility arrangement under which an employee performs the duties and responsibilities of his or her position from an approved worksite other than the location from which the employee would otherwise work. The Telework Act establishes requirements for agencies when implementing their telework policies. The head of each executive agency needs to establish and implement a policy under which employees shall be authorized to telework. Also, employees must enter into written agreements with their agencies before

---

<sup>1</sup> The title of this audit was changed from *Audit of DNFSB's Site Representative Program*, as noted in the FY 2017 DNFSB Annual Plan, to reflect a programmatic name change from site representatives to resident inspectors as instituted by DNFSB.



---

participating in telework. Moreover, the head of each executive agency must ensure that employees eligible to telework and managers of teleworking employees receive training on telework before the employee enters into a written telework agreement.

Currently, DNFSB has approximately 85 of 105 staff members participating in its telework program. Approximately six staff telework full-time.

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

*(Addresses Management and Performance Challenge #3)*

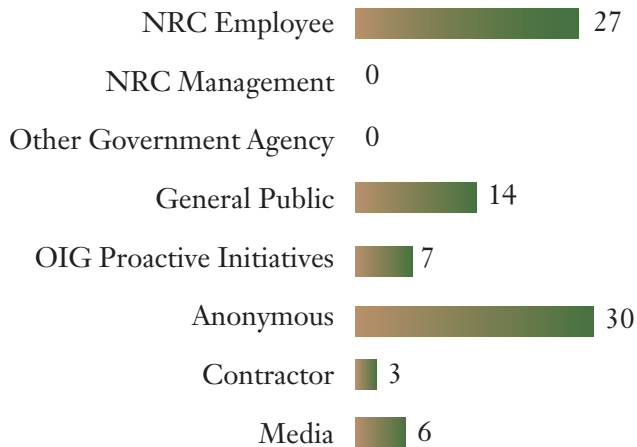
---

# SUMMARY OF NRC OIG ACCOMPLISHMENTS AT NRC

October 1, 2016, to March 31, 2017

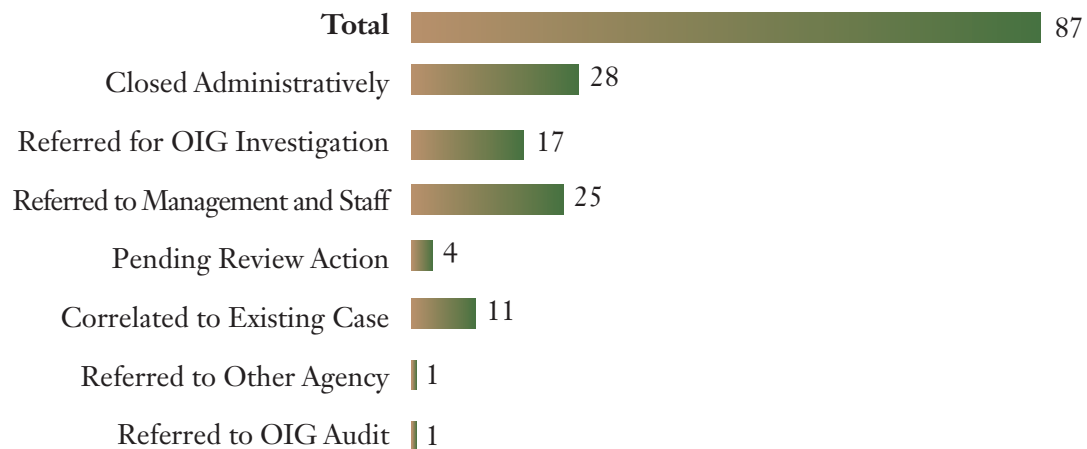
## *Investigative Statistics*

### Source of Allegations



Allegations resulting from the NRC OIG Hotline: 49 **Total: 87**

### Disposition of Allegations



## Status of Investigations

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

## Summary of Investigations

Classification of Investigations	Carryover Cases	Opened Cases	Closed Cases	Reports Issued <sup>2</sup>	Cases in Progress
Employee Misconduct	13	6	6	3	13
External Fraud	5	3	0	0	8
False Statements	1	0	1	0	0
Internal Fraud	0	1	0	0	1
Management Misconduct	16	5	6	2	15
Miscellaneous	5	1	0	0	6
Proactive Initiatives	3	1	0	0	4
Technical Allegations	8	1	2	1	7
Theft	0	1	0	0	1
<b>Total</b>	<b>51</b>	<b>19</b>	<b>15</b>	<b>6</b>	<b>55</b>

<sup>2</sup> 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*

<b>Date</b>	<b>Title</b>	<b>Audit Number</b>
02/22/2017	Audit of NRC's Oversight of Security at Decommissioning Reactors	OIG-17-A-09
02/16/2017	Audit of NRC's Oversight of Source Material Exports to Foreign Countries	OIG-17-A-08
12/19/2016	Audit of NRC's Foreign Assignee Program	OIG-17-A-07
11/30/2016	Digital Accountability and Transparency Act of 2014 Readiness Assessment for the Nuclear Regulatory Commission	OIG-17-A-06
11/16/2016	Independent Auditors' Report on the U.S. Nuclear Regulatory Commission's Closing Package Financial Statements as of and for The Year Ended September 30, 2016	OIG-17-A-05
11/15/2016	Results of the United States Nuclear Regulatory Commission's Financial Statements for Fiscal Years 2016 and 2015	OIG-17-A-04
11/08/2016	Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2016	OIG-17-A-03
10/03/2016	Audit of NRC's Oversight of Low-Level Radioactive Waste Disposal and Waste Blending	OIG-17-A-02
10/03/2016	Inspector General's FY 2017 Assessment of the Most Serious Management and Performance Challenges Facing the NRC	OIG-17-A-01

---

# AUDIT RESOLUTION ACTIVITIES

TABLE I

## OIG Reports Containing Questioned Costs<sup>3</sup>

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	\$1,647,715	0
B. Which were issued during the reporting period	0	0	0
<i>Subtotal (A + B)</i>	0	0	0
C. For which a management decision was made during the reporting period:			
(i) dollar value of disallowed costs	1	\$1,175,775	0
(ii) dollar value of costs not disallowed	1	\$471,940	0
D. For which no management decision had been made by the end of the reporting period	0	0	0

---

<sup>3</sup> 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<sup>4</sup>

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

---

<sup>4</sup>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**

<b>Date</b>	<b>Report Title</b>	<b>Number</b>
5/26/2003	Audit of NRC's Regulatory Oversight of Special Nuclear Materials	OIG-03-A-15

**Recommendation 1:** Conduct periodic inspections to verify that material licensees comply with material control and accounting (MC&A) requirements, including, but not limited to, visual inspections of licensees' special nuclear material (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 NRC OIG ACCOMPLISHMENTS AT DNFSB

October 1, 2016, to March 31, 2017

## *Investigative Statistics*

### Source of Allegations

DNFSB Employee  1

General Public  1

Allegations Received from the NRC OIG Hotline: 1 **Total: 2**

### Disposition of Allegations

**Total**  2

Referred for OIG Investigation  1

Pending Review Action  1

## Status of Investigations

DOJ Referrals. . . . .	0
Criminal Informations/Indictments . . . . .	0
Criminal Convictions. . . . .	0
Civil 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). . . . .	0

## Summary of Investigations

Classification of Investigations	Carryover Cases	Opened Cases	Closed Cases	Reports Issued <sup>5</sup>	Cases in Progress
Management Misconduct	4	1	1	1	4
Proactive Initiatives	3	1	0	0	3
<b>Total</b>	<b>7</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>7</b>

<sup>5</sup> 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*

<i>Date</i>	<i>Title</i>	<i>Audit Number</i>
12/08/16	Results of the Audit of the DNFSB's Financial Statements for FY 2016 and 2015	DNFSB-17-A-04
11/30/2016	Digital Accountability and Transparency Act of 2014 Readiness Assessment for the Defense Nuclear Facilities Safety Board	DNFSB-17-A-03
11/10/2016	Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2016	DNFSB-17-A-02
10/03/2016	Inspector General's FY 2017 Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board	DNFSB-17-A-01



# DNFSB AUDIT RESOLUTION ACTIVITIES

*TABLE I*

## OIG Reports Containing Questioned Costs<sup>6</sup>

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
<i>Subtotal (A + B)</i>	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

<sup>6</sup> 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<sup>7</sup>**

<b>Reports</b>	<b>Number of Reports</b>	<b>Dollar Value of Funds</b>
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

---

<sup>7</sup> 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-3-A-15	5/23/03	2	\$0	<p>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.</p> <p>NRC's regulations require that certain materials licensees have extensive material control and accounting programs as a condition of their license. However, all license applicants, including those requesting authorization to possess small quantities of SNM, must develop and implement plans and activities that demonstrate a commitment to accurately control and account for radioactive materials. Licensees are also required to allow NRC to inspect the materials, controls, and premises where SNM and source materials are used or stored. Additionally, NRC requires that materials licensees report information to the Nuclear Materials Management and Safeguards System (NMMSS). NMMSS is a computer database managed by the U.S. Department of Energy (DOE) and jointly used with NRC as the national system for tracking certain private and Government-owned nuclear materials.</p> <p>This audit objective was to determine whether NRC adequately ensures its licensees control and account for special nuclear material.</p> <p>The audit report made eight recommendations aimed at strengthening NRC's oversight of SNM.</p> <p>Agency management provided formal comments to this report. The recommendations remained unchanged and agreement was reached on a path forward for all recommendations.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2010	Audit of NRC's Telework Program	OIG-10-A-13	6/9/10	1	\$0	<p>In recent years, the Federal Government has taken steps to increase opportunities for employees to telework. Telework is defined as work arrangements in which an employee regularly performs officially assigned duties at home or other worksites geographically convenient to the employee's residence. Telework is also a tool that can be used to ensure continuity of essential Government functions in the event of national or local emergencies. NRC's, Office of Human Resources (now called the Office of the Chief Human Capital Officer) Employee/Labor Relations and Work Life Branch, has responsibility for implementing the NRC's telework program in accordance with telework guidelines stated in the Collective Bargaining Agreement (CBA) between NRC and the National Treasury Employees Union, which covers approximately 68 percent of NRC permanent employees. NRC recently renegotiated the telework program guidelines in the CBA, effective November 9, 2015.</p> <p>The audit objectives were to determine NRC's readiness to have staff telework under emergency situations, the adequacy of internal controls associated with the telework program, and if NRC's telework program complies with relevant law and OPM guidance. NRC has established a telework program that supports the agency's mission and work/life programs.</p> <p>The audit report made five recommendations to improve NRC's telework program including development of internal controls related to telework, ensuring compliance with applicable laws and ensuring telework readiness in case of an emergency.</p> <p>Agency management agreed with the report.</p>
2010	Audit of NRC's Vendor Inspection Program	OIG-10-A-20	9/28/10	3	\$0	<p>NRC endeavors to protect the public health and safety and the environment by overseeing vendor compliance with NRC's regulations for assuring the integrity of domestic and global parts and services supplied to nuclear power reactors. Vendors manufacture a range of components such as fasteners, pumps, valves, and reactor vessels, as well as provide design, engineering, and construction services. While most vendors do not hold NRC licenses, they are nonetheless bound through contracts with licensees, applicants, or other vendors to comply with NRC's quality assurance regulations contained in Appendix B to Title 10, CFR Part 50 (Appendix B). Vendors are also required to comply with 10 CFR Part 21 (Part 21). NRC conducts reactive and routine inspections of vendors' implementation of Appendix B and Part 21 requirements.</p> <p>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.</p> <p>The audit report made ten recommendations aimed at strengthening NRC's approach to vendor inspection.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
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	<p>NRC endeavors to protect the public health and safety and the environment through the regulation of the 100 operating nuclear power plants in the United States.</p> <p><i>The Energy Reorganization Act of 1974, as Amended, Section 206, Noncompliance</i>, 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, <i>Reporting of Defects and Noncompliance</i> (Part 21) to implement the provisions of Section 206. The primary NRC office responsible for Part 21 implementation among licensees with operating plants is NRR.</p> <p>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 <i>Energy Reorganization Act of 1974, as Amended, Section 206, Noncompliance</i>.</p> <p>The audit report made five recommendations to improve NRC's implementation of Part 21.</p> <p>Agency management agreed with the report.</p>



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	<p>The President of the United States 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.</p> <p>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.</p> <p>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."</p> <p>NRC staff can process electronic documents containing SUNSI in a variety of ways including on shared network drives. These shared drives include G:// drives accessible by staff within NRC program offices; an R:// drive, an agency wide drive with read-only access; and an S://drive, which allows all staff, whose user accounts are on the same file server, to add, read, edit, and delete documents unless documents are stored in folders configured to limit access to specific employees or groups of employees.</p> <p>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.</p> <p>The audit objective was to assess whether NRC effectively protects electronic documents containing Personally Identifiable Information (PII) and other types of SUNSI on NRC's shared network drives.</p> <p>The audit report made five recommendations to improve training, communication, coordination, and quality assurance controls to ensure SUNSI is appropriately managed.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2012	Audit of NRC's Management of the Baseline Security Inspection Program	OIG-12-A-10	3/8/12	3	\$0	<p>NRC's baseline security inspection program is the agency's primary means for ensuring that nuclear power plants across the United States are protected in accordance with Federal Government regulations. Specifically, the baseline security inspection program has six objectives:</p> <ul style="list-style-type: none"> <li>To gather sufficient, factual information to determine with high assurance if a licensee's security system and material control and accounting program can protect against radiological sabotage, and the theft or loss of special nuclear material.</li> <li>To determine a licensee's ability to identify, assess, and correct security issues in proportion with the significance of these issues.</li> <li>To determine if licensees, working with external agencies, are capable of deterring and protecting against the Design Basis Threat.</li> <li>To validate performance indicator data, which NRC uses in conjunction with inspection findings to assess the security performance of power reactor licensees.</li> <li>To help NRC monitor plants' security status and conditions.</li> <li>To identify significant issues that may have generic or crosscutting applicability to the safe and secure operation of licensees' facilities.</li> </ul> <p>To meet these objectives, NRC conducts routine inspections at nuclear power plants that focus on specific issue areas such as access controls, protective strategy, security training, and safeguards information controls.</p> <p>The objective of this audit was to evaluate NRC's management of the baseline security inspection program, including specific program features such as the Significance Determination Process.</p> <p>The report made five recommendations to improve NRC's management of the baseline security inspection program. Agency management agreed with the report.</p>

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	<p>The <i>Omnibus Budget Reconciliation Act of 1990</i> (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")].</p> <p>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 <i>Independent Offices Appropriation Act of 1952</i>, recover NRC's costs of providing special benefits to identifiable applicants and licensees. In FY 2012, the estimated 10 CFR Part 170 fees totaled \$345.2 million. 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.</p> <p>In FY 2012, the 10 CFR Part 171 fee collections required totaled \$555.8 million. In FY 2012 NRC's budget authority was \$1,038.1 million and non-fee items were \$27.5 million. The total amount of fees to recover in FY 2012 was \$909.5 million.</p> <p>On an annual basis, NRC amends the licensing, inspection, and annual fees. Additionally, NRC publishes the annual Fee Rule in the <i>Federal Register</i>.</p> <p>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.</p> <p>The audit report made four recommendations to further improve the license fee calculation process.</p> <p>Agency management agreed with the report.</p>
2013	Audit of NRC's Safeguards Information Local Area Network and Electronic Safe	OIG-13-A-16	4/1/13	5	\$0	<p>NRC developed its Safeguards Information Local Area Network and Electronic Safe (SLES) system to store and manage electronic Safeguards Information (SGI) documents.</p> <p>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.</p> <p>The adoption of these various techniques into SGI operations was intended to ensure that E-Safe will contain all SGI created or received by NRC, thereby eliminating the need to maintain separate, individual collections of SGI.</p> <p>The audit objective was to determine if SLES meets its operational capabilities and applicable security controls.</p> <p>The audit report made seven recommendations to improve the agency's SLES system.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2013	Audit of NRC's Budget Execution Process	OIG-13-A-18	5/7/13	1	\$0	<p>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.</p> <p>NRC's budget process consists of strategic planning; budget formulation; submission of the agency's budget to the OMB and Congress; approval of the budget by Congress; budget execution; and the reporting of budget and performance results.</p> <p>The budget execution phase refers generally to the time period during which the budget authority made through an appropriation remains available for obligation by NRC. NRC's task during the budget execution process is to spend appropriated funds to carry out its mission in accordance with fiscal statutes.</p> <p>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.</p> <p>The audit report made eight recommendations to improve the internal controls over the management of budget execution.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2014	Audit of NRC's Oversight of Active Component Aging	OIG-14-A-02	10/28/13	2	\$0	<p>The <i>Atomic Energy Act of 1954</i>, 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.</p> <p>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.</p> <p>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.</p> <p>NRR and the regional offices provide regulatory oversight of industry's active component aging activities. NRC addresses aging active component issues through a number of different regulations and guidance, to include Title 10 CFR Part 50.65, <i>Requirements for monitoring the effectiveness of maintenance at nuclear power plants</i> (the Maintenance Rule, as amended), 10 CFR Part 50, Appendix B, <i>Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants</i>, and 10 CFR 50.36, <i>Technical specifications</i>.</p> <p>The objective of this audit was to determine if NRC is providing effective oversight of industry's aging component programs.</p> <p>The audit report made two recommendations to improve the agency's oversight of aging active component activities.</p> <p>Agency management provided formal comments to the report. The recommendations remained unchanged and agreement was reached on a path forward for all recommendations.</p>



Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2014	Audit of NRC's Freedom of Information Act Process	OIG-14-A-17	6/16/14	1	\$0	<p>The Freedom of Information Act (FOIA) is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government.</p> <p>NRC's FOIA program is managed by the FOIA, Privacy, and Information Collections Branch (referred to in this report as the FOIA office) within the Office of Information Services, Customer Service Division.</p> <p>The FOIA process begins when the agency (1) receives—via mail, facsimile, or Internet—an incoming FOIA request, (2) assigns it a number, and (3) determines which NRC offices need to review their records to identify whether they have information pertinent to the request and sends a request to those offices. FOIA coordinators in responsive offices provide an estimate of the search, review, and duplication effort required to produce any documents identified as within the scope of the request.</p> <p>The FOIA office then estimates the associated processing fees (for which the requester may be responsible), advises the requester as to the amount due, and assigns the request to the appropriate offices to identify and provide to the FOIA office all relevant documents from their office within an assigned timeframe. To facilitate appropriate disclosure of records, the FOIA coordinators consult as needed with agency staff in the responding offices and/or OGC to prepare a response. The response is reviewed and signed by the FOIA officer, and sent to the requester.</p> <p>The audit objective was to determine whether the FOIA process is efficient and complies with the current laws.</p> <p>The audit report made nine recommendations to improve the efficiency of NRC's FOIA process.</p> <p>Agency management agreed with the report.</p>
2015	Audit of NRC's Oversight of Spent Fuel Pools	OIG-15-A-06	2/10/15	2	\$0	<p>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 spent fuel pools that currently store spent fuel.</p> <p>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.</p> <p>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.</p> <p>The report made four recommendation to improve oversight of spent fuel pools.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Process for Ensuring Integrity in Scientific Research	OIG-15-A-08	2/10/15	1	\$0	<p>The Federal Government disseminates a variety of scientific information, including statistical information; information about health, safety, and environmental risks; and technical information it creates or obtains in the course of developing regulations. Scientific information is based on scientific research, analyses, and data performed to support the agency's work.</p> <p>Scientific information is defined as factual inputs, data, models, analyses, technical information, or scientific assessments related to such disciplines as the behavioral and social sciences, public health and medical sciences, life and earth sciences, engineering, or physical sciences.</p> <p>Often, regulations are based on scientific, engineering, and economic analyses. Therefore, it is crucial that information disseminated by Federal agencies be objective, and have utility, quality, and integrity.</p> <p>To ensure information integrity, Federal agencies are required to adopt standards for information quality. These standards are set by the Office of Management and Budget.</p> <p>NRC has an Information Quality Program that involves many offices, including the Office of Information Services (OIS), the Office of Nuclear Regulatory Research (RES), and the Office of the Executive Director for Operations (OEDO). These three offices have a central role in implementing NRC's Information Quality Program. Additionally, other offices support OIS, RES, and OEDO in ensuring information integrity. These offices include NRR, the Office of Nuclear Material Safety and Safeguards, the Office of New Reactors, and the Office of Nuclear Security and Incident Response.</p> <p>RES plays a central role in the agency's information quality program because it leads peer review efforts of agency products.</p> <p>The audit objective was to determine whether NRC has controls in place to assure that scientific research is objective, credible, and transparent.</p> <p>The audit report made five recommendations to strengthen agency's information quality program.</p> <p>Agency management agreed with the report</p>
2015	Audit of NRC's Internal Controls Over Fee Revenue	OIG-15-A-12	3/19/15	4	\$0	<p>NRC is required by law to offset a substantial percent of its budget authority through fees billed to licensees and license applicants.</p> <p>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.</p> <p>Each fiscal year, NRC publishes a schedule of fees in 10 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.</p> <p>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.</p> <p>The audit report made seven recommendations to improve internal controls over the recordation of fee revenue.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Regulatory Analysis Process	OIG-15-A-15	6/24/15	2	\$0	<p><i>The Atomic Energy Act of 1954</i>, as amended (42 U.S.C. 2011), and Energy Reorganization Act of 1974, authorize NRC to develop regulations that licensees must follow to protect public health and safety and the environment, and to promote the common defense and security.</p> <p>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.</p> <p>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.</p> <p>The audit objective was to determine the adequacy of NRC's regulatory analysis process.</p> <p>The audit report made four recommendations to improve the regulatory analysis process.</p> <p>Agency management agreed with the report.</p>
2015	Audit of NRC's Reactor Business Lines' Compliance with Agency Non-Financial Internal Control Guidance	OIG-15-A-16	6/25/15	1	\$0	<p>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.</p> <p>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.</p> <p>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.</p> <p>The audit report made three recommendations that will increase compliance with agency programmatic, non-financial internal control guidance.</p> <p>Agency management agreed with the report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2015	Audit of NRC's Web-Based Licensing (WBL) System	OIG-15-A-17	6/29/15	3	\$0	<p>NRC's primary mission is to license and regulate the use of radioactive materials for civilian purposes to ensure adequate protection of public health and safety and the environment. NRC's recent Project Aim 2020 report noted that, although NRC accomplishes its mission, a lack of standardized processes is an obstacle to efficiency and agility.</p> <p>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.</p> <p>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.</p> <p>The audit report made four recommendations to improve NRC's use of WBL.</p> <p>Agency management agreed with the report.</p>
2015	Audit of NRC's Management of Change	OIG-15-A-19	9/1/15	1	\$0	<p>As Federal budgets grow and shrink, as economic and environmental forces shape energy policy, and as legislative requirements wax and wane, the NRC's regulatory responsibilities and the way it implements that oversight will be subject to change.</p> <p>Over the past 5 years, NRC has undertaken several significant change initiatives. For example, in 2010, NRC initiated a "Transforming Assets into Business Solutions" effort with the goal of making NRC more effective and efficient by consolidating and improving business practices. Additional expected change awaits NRC as the result of "Project Aim 2020," which analyzes potential organizational changes to enhance NRC's ability to perform its mission in the future.</p> <p>Change management research and best practices demonstrate that many change initiatives fail because managers often skip steps needed to implement change or they make critical mistakes while implementing change. Change management literature also points to the importance of organizations to manage change efficiently and effectively to increase the likelihood that change occurs as intended.</p> <p>While there is no one-size-fits-all process or absolute guarantee that change occurs as intended, an orderly approach to managing change increases the likely success of the intended change. Moreover, a good change management process is scalable, meaning that it takes a graded approach to each change. A scalable process encourages organizations to apply more structure, oversight, and effort to more significant and potentially difficult changes, while allowing flexibility to use a less rigorous approach for less significant changes.</p> <p>The audit objective was to assess the efficiency and effectiveness of NRC's management of change.</p> <p>The audit report made three recommendations to complete implementation of and promote the agency's change management framework and provide training to staff on the agency's approach to change management.</p> <p>Agency management agreed with the report.</p>

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	<p>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.</p> <p>OIS manages ADAMS staff and 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.</p> <p>OIG contracted with AEGIS.net, Inc., to evaluate if ADAMS meets its required operational capabilities and adequately provides the necessary functionality to serve as the agency's repository for Official Agency Records. This includes providing functionality such as document storage, document search and retrieval, usability, and other aspects such as availability, performance, contingency planning, and security.</p> <p>The evaluation objective was to determine if ADAMS meets its required operational capabilities and adequately provides for functionality.</p> <p>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.</p> <p>Agency management agreed with the report.</p>
2016	Audit of NRC's Network Security Operations Center	OIG-16-A-07	1/11/16	4	\$0	<p>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.</p> <p>The SOC is primarily staffed by contractors working under the Information Technology Infrastructure Support Services contract.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Agency management agreed with the report.</p>



Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of NRC's Personal Identity Verification (PIV) Card Access System	OIG-16-A-10	3/7/16	1	\$0	<p>The Personal Identity Verification (PIV) card is an identification card issued by a Federal agency that contains information unique to each employee and contractor. The main function of the card is to protect and to strengthen the security of both employees' and contractors' information and control physical access to secured areas.</p> <p>NRC uses the PIV card to control physical access at its headquarters and its regional offices. Federal policies require agencies to swiftly revoke physical access rights at termination of employment. NRC must collect and destroy PIV cards from Federal employees and contractors upon termination. Additionally, some areas within NRC are restricted to certain individuals. Each restricted area has a designated representative who must maintain an up-to-date access list of individuals needing access.</p> <p>The audit objective was to determine whether NRC's PIV card access system meets its operational requirements, and to assess the effectiveness of the PIV system coordination among offices that have a role in securing NRC's physical access.</p> <p>The audit report made seven recommendations to improve the PIV card access system, reduce physical security risk across the agency, and ensure continued compliance with Federal regulations and guidance.</p> <p>Agency management agreed with the report.</p>
2016	Audit of NRC's Technical Assistance Request Process	OIG-16-A-11	4/6/16	1	\$0	<p>A Technical Assistance Request (TAR) is a request for technical assistance from NRC headquarters or regional office, or an Agreement State. These requests are generally sent to the Office of Nuclear Material Safety and Safeguards (NMSS) and involve issues related to nuclear materials. The process of sending these requests, along with receipt of the ensuing responses, constitute the TAR process.</p> <p>The purpose of the TAR process is to support NRC organizations external (and sometimes internal) access to NMSS in the most efficient and effective manner. A TAR contains questions on subjects involving regulatory or policy interpretations, inspection findings, or a technical area in which NMSS possesses expertise or for which it has responsibility.</p> <p>The audit objective was to determine if NRC's TAR process facilitates effective and efficient responses.</p> <p>The audit report made three recommendations to improve the efficiency of NRC's TAR process through enhanced communication and documentation of the TAR process.</p> <p>Agency management agreed with the report.</p>

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	7	\$0	<p>NRC manages numerous publicly accessible Web applications to share nuclear information with licensees and the public. NRC's publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency information technology (IT) resources.</p> <p>NRC is a regular target of cyber-attacks because its technical and other sensitive information is highly sought after by potential adversaries.</p> <p>The NRC OIG joined other OIGs to conduct a Federal-wide review of publicly accessible Web applications and associated security controls. Each OIG assessed its own agency's Web applications program, allowing the OIG group to then develop Federal-wide recommendations and best practices to secure and manage publicly accessible Web applications.</p> <p>This evaluation was conducted by Richard S. Carson &amp; Associates, Inc. to assess NRC's publicly accessible Web applications as part of this crosscutting project.</p> <p>NRC perimeter security services (e.g., firewalls, intrusion detection/prevention systems) were configured to whitelist (i.e., monitor only, not block) the scanning platforms/hosts identified in the agreed upon rules of engagement.</p> <p>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.</p> <p>The audit report made seven recommendations to improve the security of NRC's publicly accessible Web applications. Agency management agreed with the report.</p>
2016	Audit of NRC's Decommissioning Funds Program	OIG-16-A-16	6/8/16	7	\$0	<p>NRC regulates the decommissioning of nuclear power plants, material sites, fuel cycle facilities, research and test reactors, and uranium recovery facilities, with the ultimate goal of license termination.</p> <p>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.</p> <p>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.</p> <p>The audit report makes nine recommendations to improve internal controls related to decommissioning funds reviews and strengthen the agency's decommissioning funds review process.</p> <p>Agency management agreed with the report.</p>

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 Classified Information Laws and Policies	OIG-16-A-17	6/8/16	2	\$0	<p>The <i>Reducing Over-Classification Act of 2010</i> mandated that the Inspectors General of all Federal agencies with original classification authority perform at least two evaluations over proper use of classified information.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The audit report makes three initiatives and to develop procedures and guidance to ensure effective records management and timely disposition and declassification of classified records at NRC.</p> <p>Agency management agreed with the report.</p>
2016	Cybersecurity Act of 2015 Audit for NRC	OIG-16-A-18	8/8/16	1	\$0	<p>The <i>Cybersecurity Act</i> was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States.</p> <p>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.</p> <p>NRC uses three different types of national security systems to process and store classified information: standalone systems, subscriber systems, and shared service systems. Federal policy requires that classified information may only be stored, processed, or transmitted using systems that have been granted an NRC authorization-to-operate for classified information processing.</p> <p>The audit objective was to assess NRC's information technology security policies, procedures, practices, and capabilities relative to covered systems for national security systems and systems that provide access to PII operated by or on behalf of NRC.</p> <p>This audit report makes two recommendations to improve security over NRC's national security systems information systems, ensure compliance with Federal policies through development of agency wide policies and procedures over classified information systems, and maintain an agency wide inventory of national security systems.</p> <p>Agency management agreed with the report.</p>

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	3	\$0	<p>The <i>Federal Managers' Financial Integrity Act</i> (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.</p> <p>NRC updated Management Directive (MD) 4.4, <i>Internal Control</i>, in 2012 to comply with FMFIA. MD 4.4 established a uniform process to assess internal control that meets FMFIA requirements.</p> <p>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.</p> <p>The audit report makes three recommendations to improve the effectiveness of NRC's process to assess internal control over program operations.</p> <p>Agency management agreed with the report.</p>
2016	Audit of NRC's Significance Determination Process for Reactor Safety	OIG-16-A-21	9/26/16	4	\$0	<p>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.</p> <p>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.</p> <p>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.</p> <p>The audit objective was to assess the consistency with which NRC evaluates power reactor safety inspection findings under the SDP.</p> <p>The audit report makes 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.</p> <p>Agency management agreed with the report.</p>

*Total unimplemented recommendations: 89*

## *DNFSB Unimplemented Recommendations*

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of the Defense Nuclear Facilities Safety Board's Information Security Program	DNFSB-16-A-02	10/28/15	2	\$0	<p>DNFSB is an independent organization within the Executive Branch that advises the President and the Secretary of Energy on public health and safety issues at DOE defense nuclear facilities. DNFSB reviews and evaluates the content and implementation of health and safety standards, as well as other requirements relating to the design, construction, operation, and decommissioning of DOE defense nuclear facilities.</p> <p>DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees.</p> <p>The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations.</p> <p>The audit report made three recommendations to improve DNFSB's information security guidance and Unclassified Controlled Nuclear Information access controls on its internal SharePoint site.</p> <p>DNFSB management stated their general agreement with the report.</p>
2016	Audit of DNFSB's Process for Developing, Implementing, and Updating Policy Guidance	DNFSB-16-A-05	6/24/16	2	\$0	<p>In January 2015, a Government Accountability Office audit highlighted the DNFSB had few written policies. Subsequently in June 2015, DNFSB updated its directives program, including assigning roles and responsibilities for the drafting, issuance, and implementation of directives and supplementary documents. DNFSB has increased its effort to establish directives and supplementary documents to support policies and procedures.</p> <p>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.</p> <p>The audit report made six recommendations to improve the processes for developing, implementing, and updating policy guidance.</p> <p>DNFSB management agreed with the recommendations in this report.</p>

Fiscal Year	Report Title	Report Number	Report Date	Number of Unimplemented Recommendations	Aggregate Potential Cost Savings	Summary
2016	Audit of DNFSB's Oversight of Nuclear Facility Design and Construction Projects	DNFSB-16-A-06	7/6/16	5	\$0	<p>Congress created DNFSB to identify the nature and consequences of potential threats to public health and safety at DOE defense nuclear facilities. The <i>Atomic Energy Act of 1954</i>, as amended, requires that DNFSB review the design and construction of new defense nuclear facilities to ensure the adequate protection of public health and safety during operation. DNFSB provides oversight of DOE defense nuclear facilities as well as those managed by the National Nuclear Security Administration. DNFSB provides oversight of design and construction activities at the following sites: Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Nevada National Security Site, Pantex, Sandia National Laboratories, Savannah River Site, Y-12 National Security Complex/Oak Ridge National Laboratory, Hanford, Idaho National Laboratory, and the Waste Isolation Pilot Plant.</p> <p>According to the DNFSB 2015 Annual Report to Congress, DNFSB is actively overseeing the design and construction of over a dozen new defense nuclear projects with a projected total cost exceeding \$25 billion.</p> <p>The audit objective was to assess the efficiency and effectiveness of DNFSB's oversight of nuclear facility design and construction projects.</p> <p>The audit report made five recommendations aimed at strengthening the efficiency and effectiveness of DNFSB's approach to oversight of defense nuclear facility design and construction projects. Recommendations address guidance, training, and lessons learned.</p> <p>DNFSB management agreed with the recommendations, but elected to provide formal comments.</p>
2016	Cybersecurity Act of 2015 Audit for DNFSB	DNFSB-16-A-07	8/8/16	2	\$0	<p>The <i>Cybersecurity Act of 2015</i> was enacted on December 18, 2015, and was designed to improve cybersecurity in the United States.</p> <p>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.</p> <p>DNFSB relies on the servicing organizations to properly protect the records, but must review the privacy impact assessment to determine they are using proper controls. However, DNFSB does not review the privacy impact assessment for external organizations.</p> <p>The audit objective was to evaluate DNFSB's information technology security policies, procedures, practices, and capabilities as defined in the <i>Cybersecurity Act of 2015</i> for national security systems and systems that provide access to personally identifiable information operated by or on behalf of DNFSB.</p> <p>The audit report made two recommendations to bring DNFSB into compliance with the <i>Privacy Act of 1974</i> and <i>E-Government Act of 2002</i>.</p> <p>DNFSB management stated their agreement with recommendations in this report.</p>

**Total unimplemented recommendations: 11**



---

# 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
AIGA	Assistant Inspector General for Audits
ASME	American Society of Mechanical Engineers
CBA	Centrally Billed Account
CFR	Code of Federal Regulations
CIGIE	Council of Inspectors General on Integrity and Efficiency
CO	Contracting Officer
CoC	Certificate of Compliance
COR	Contracting Officer's Representative
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
DRMA	Division of Resource Management and Administration
FAEC	Federal Audit Executive Committee
FAIMIS	Financial and Accounting Integrated Management Information System
FASAB	Federal Accounting Standards Advisory Board
FISMA	Federal Information Security Modernization Act of 2014
FMFIA	Federal Managers' Financial Integrity Act
FOIA	Freedom of Information Act
FPPS	Federal Personnel Payroll System
FSS	Facility Security Specialist
FY	Fiscal Year
IAM	Issue Area Monitor
IPERA	Improper Payments Elimination and Recovery Act
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
IT	Information Technology
LAN	Local Area Network
LLRW	Low Level Radioactive Waste
MD	Management Directive
NMMSS	Nuclear Materials Management and Safeguards System
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation
OCHCO	Office of the Chief Human Capital Officer
OEDO	Office of the Executive Director for Operations
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIP	Office of International Programs
OIS	Office of Information Services
OMB	Office of Management and Budget
OPM	Officer of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMDA	Program Management, Policy Development and Analysis
RES	Office of Nuclear Regulatory Research
ROE	Reactor Operations Engineer
SDP	Significance Determination Process
SGI	Safeguards Information
SLES	Safeguards Information Local Area Network and Electronic Safe
SNM	Special Nuclear Material
SOC	Security Operations Center
SRI	Senior Resident Inspector
SUNSI	Sensitive, Unclassified Non-Safeguards Information
TAR	Technical Assistance Request
WBL	Web-Based Licensing

---

# 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.*

<b>Citation</b>	<b>Reporting Requirements</b>	<b>Page</b>
Section 4(a)(2)	Review of legislation and regulations	7-8
Section 5(a)(1)	Significant problems, abuses, and deficiencies	11-20; 29-33; 36-38
Section 5(a)(2)	Recommendations for corrective action	11-20; 36-38
Section 5(a)(3)	Prior significant recommendations not yet completed	45
Section 5(a)(4)	Matters referred to prosecutive authorities	42, 48
Section 5(a)(5)	Listing of audit reports	43, 49
Section 5(a)(6)	Listing of audit reports with questioned costs or funds put to better use	none
Section 5(a)(7)	Summary of significant reports	11-20; 29-33; 36-38
Section 5(a)(8)	Audit reports — questioned costs	44, 50
Section 5(a)(9)	Audit reports — Funds put to better use	45, 51
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	52-70
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)(14-16)	Peer review information	74
Section 5(a)(17)	Investigations statistical tables	41-42; 47-48
Section 5(a)(18)	Description of metrics	42
Section 5(a)(19)	Investigations of senior Government officials where misconduct was substantiated	none
Section 5(a)(20)	Whistleblower retaliation	71
Section 5(a)(21)	Interference with IG independence	71
Section 5(a)(22)(a)	Audits not made public	none
Section 5(a)(22)(b)	Investigations involving senior Government officials where misconduct was not substantiated and report was not made public	29, 30, 32

---

# APPENDIX

## Peer Review Information

### *Audits*

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

### *Investigations*

The NRC OIG Investigative program was peer reviewed most recently by the Tennessee Valley Authority Office of Inspector General. The peer review final report, dated October 5, 2016, reflected that the system of internal safeguards and management procedures for the investigative function of the 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 Offices of Inspectors General with Statutory Law Enforcement Authority. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the planning, execution, and reporting of its investigations.

## **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](http://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 05 E13  
 11555 Rockville Pike  
 Rockville, MD 20852-2738

