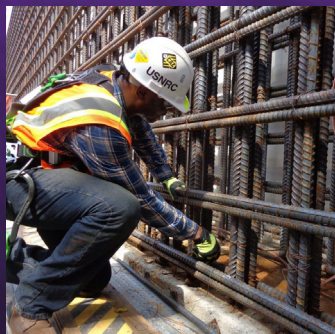


**OFFICE OF THE INSPECTOR GENERAL**  
**U.S. NUCLEAR REGULATORY COMMISSION**  
**DEFENSE NUCLEAR FACILITIES SAFETY BOARD**



# Semiannual Report to Congress

October 1, 2015–March 31, 2016





## 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**  
**TDD: 1-800-270-2787**  
7:00 a.m. – 4:00 p.m. (EST)  
After hours, please leave a message.



**Submit:**  
Online Form  
[www.nrc.gov](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





---

# 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, 2015, to March 31, 2016.



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

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

It was an active 6 months for my office in furtherance of its obligation to timely identify the most critical risks and vulnerabilities in NRC and DNFSB programs and operations to allow NRC and the DNFSB to take any necessary corrective action. The work highlighted in this report includes audits of NRC's operator licensing program for the AP1000 power reactor, Network Security Operations Center, and personal identity verification card access system. In addition, this report includes audits of DNFSB's implementation of the Federal Information Security Modernization Act of 2014 for FY 2015, and Information Security Program.

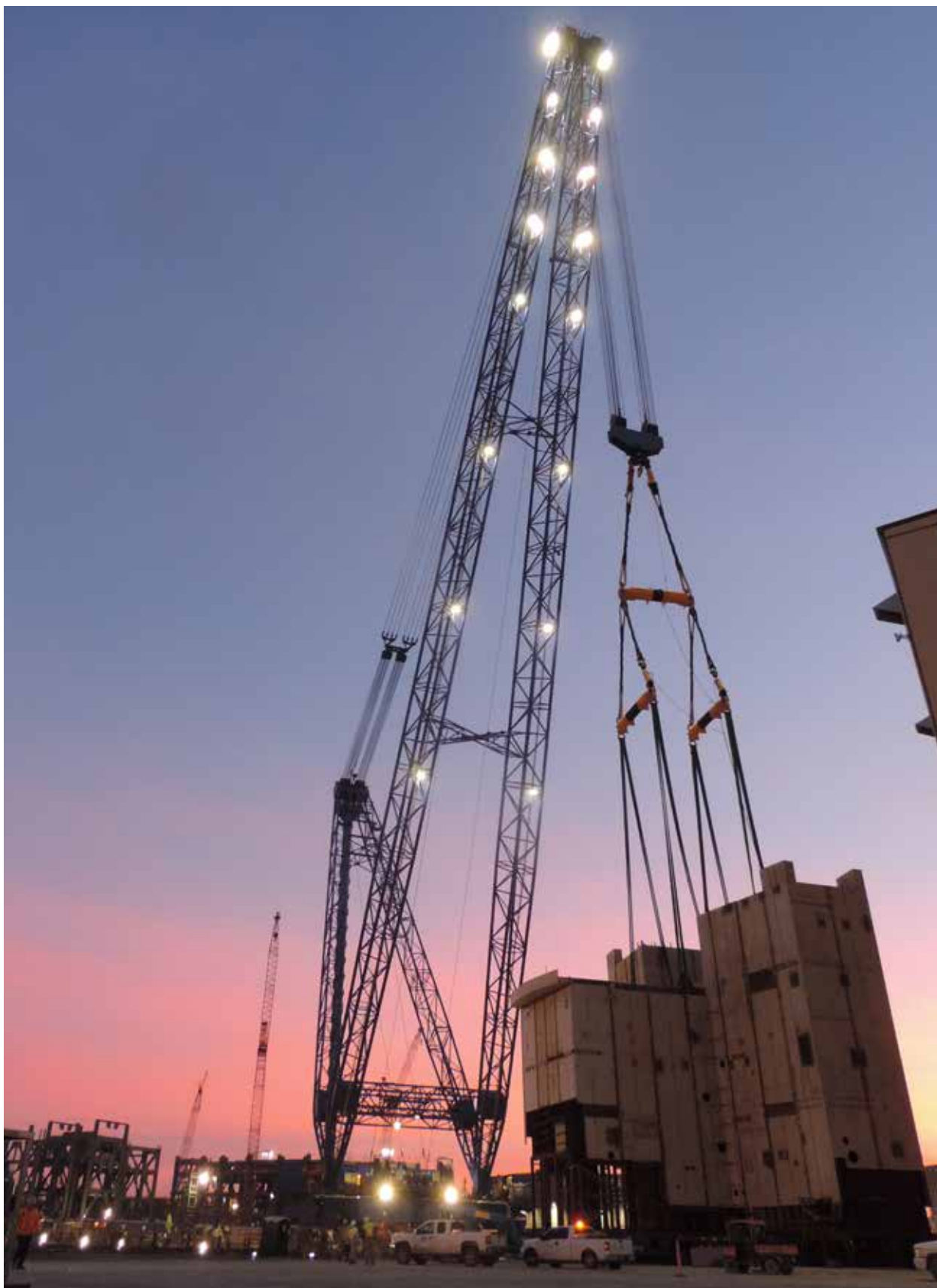
During this semiannual reporting period, OIG issued 10 NRC and 4 DNFSB audit reports. As a result of this work, OIG identified vulnerabilities in, and made a number of recommendations to improve the effective and efficient operation of, NRC's safety, security, and corporate management programs and those of the DNFSB. OIG also opened 21 investigations, and completed 20 cases. Four of the open cases were referred to the Department of Justice, and one allegation was referred to NRC management for action.

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

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

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



*Component placement at V.C. Summer. Photo courtesy of Southern Company*

---

# CONTENTS

|                                                    |      |
|----------------------------------------------------|------|
| <b>Highlights</b>                                  | v    |
| NRC Audits                                         | v    |
| Defense Nuclear Facilities Safety Board Audits     | vii  |
| NRC Investigations                                 | viii |
| <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 General Counsel Activities               | 8    |
| NRC OIG Obtains 2302 (c) Certification             | 8    |
| Other OIG Activities                               | 9    |
| NRC OIG Receives CIGIE Award for Excellence        | 9    |
| <b>NRC Management and Performance Challenges</b>   | 11   |
| <b>NRC Audits</b>                                  | 12   |
| Audit Summaries                                    | 12   |
| Audits in Progress                                 | 21   |
| <b>NRC Investigations</b>                          | 29   |
| Investigative Case Summaries                       | 29   |
| <b>Defense Nuclear Facilities Safety Board</b>     | 34   |
| <b>DNFSB Management and Performance Challenges</b> | 34   |
| <b>DNFSB Audits</b>                                | 35   |
| Audit Summaries                                    | 35   |
| Audits in Progress                                 | 38   |
| <b>Summary of NRC OIG Accomplishments at NRC</b>   | 41   |
| Investigative Statistics                           | 41   |
| NRC Audit Listings                                 | 44   |
| <b>Summary of NRC OIG Accomplishments at DNFSB</b> | 43   |
| Investigative Statistics                           | 43   |
| DNFSB Audit Listings                               | 45   |
| <b>Audit Resolution Activities</b>                 | 47   |
| <b>Abbreviations and Acronyms</b>                  | 50   |
| <b>Reporting Requirements</b>                      | 51   |
| <b>Appendix</b>                                    | 52   |



*Delivery of steam generator for Vogle Unit 4. Photo courtesy of Georgia Power Company*



---

# HIGHLIGHTS

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

## *NRC Audits*

- The Personal Identity Verification (PIV) card is an identification card issued by a Federal agency that contains information unique to each employee and contractor. The main function of the card is to protect and to strengthen the security of both employees' and contractors' information and physical access to secured areas. NRC utilizes the PIV card to control physical access at its headquarters and 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. 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.
- Before NRC licenses someone to operate controls of a commercial nuclear power reactor, this individual must complete extensive training and pass rigorous, site-specific written examinations and operating tests that are relevant to the design and construction of the facility they will operate. Four Advanced Passive 1000 (AP1000) Pressurized Water Reactors are under construction, two in South Carolina and two in Georgia. This is a new reactor design for which operators have never been licensed. An operator's license authorizes the license holder to manipulate the controls of the facility, which directly affect the reactivity or power level of the reactor. By the year 2020, approximately 70 licensed operators will be needed for the AP1000. The audit objective was to determine if NRC's program for licensing AP1000 reactor operators is efficiently and effectively implemented.
- 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. Robust SOC capabilities are particularly crucial given the sensitivity of the unclassified information processed on NRC's network, and the increasing volume of attacks carried out against Federal Government computer systems. The audit objective was to determine whether NRC's network SOC meets operational requirements, and to assess the effectiveness of SOC coordination with other organizations that have a role in securing NRC's network.
- The 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. NRC's Office of the Chief Information Officer manages ADAMS, and staff in

---

headquarters and regional offices use ADAMS for their day-to-day mission activities. The public uses NRC's Web site to access Web-based ADAMS. The evaluation objective was to determine if ADAMS meets its required operational capabilities and adequately provides for functionality.

- The 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 Federal Information Security Modernization Act of 2014 (FISMA 2014) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. The Office of Management and Budget (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's implementation of FISMA 2014 for FY 2015.
- NRC is responsible for overseeing the medical uses of nuclear material through its licensing, inspection, and enforcement programs. NRC issues medical use licenses to medical facilities, develops guidance and regulations for use by licensees, and maintains a committee of medical experts to obtain advice about the use of byproduct materials in medicine. This committee, the Advisory Committee on the Medical Uses of Isotopes, is an independent committee established by the NRC for the express purpose of advising NRC staff. When a medical facility has a potential problem using radioactive material, it may meet NRC's criteria for a medical event. These events may involve doses to a patient of the wrong amount, the wrong radioactive drug, incorrect administration of a drug, or dose to the wrong patient or wrong part of the body. There are about 40 medical events each year. The audit objective was to determine if NRC's oversight of medical uses of radioactive isotopes adequately protects public health and safety.
- 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, 2015. 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.



---

## *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 in accordance with applicable standards. The audit, conducted by Acuity Consulting, Inc., under a contract with OIG, includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. It also includes assessing the accounting principles used and significant estimates made by management as well as evaluating the overall financial statement presentation.
- 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 must also include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. OMB requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool. The evaluation objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015.
- DNFSB is an independent organization within the Executive Branch that advises the President and the Secretary of Energy on public health and safety issues at Department of Energy (DOE) defense nuclear facilities. DNFSB reviews and evaluates the content and implementation of health and safety standards, as well as other requirements relating to the design, construction, operation, and decommissioning of DOE defense nuclear facilities. DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees. The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations.
- 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 in FY 2016. The FY 2016 management and performance challenges are related to DNFSB's organizational culture and climate, security, human capital, and internal controls.

---

## *NRC Investigations*

- OIG initiated an investigation based on two specific issues raised by Congress as well as members of the public regarding safety concerns at the Palisades Nuclear Plant in Covert, MI. The investigation addressed concerns that NRC had, over a period of more than a year, “tolerated,” or otherwise inadequately responded to, a leak with the potential to grow and to affect safety related control room components. A second issue addressed in this investigation involved the adequacy of the NRC staff’s handling of identified safety culture concerns among Palisades’ employees.
- OIG initiated an investigation based on an NRC employee’s allegation that the program manager of an NRC independent verification and validation contract, was authorizing \$400,000 of expenses each month with no deliverables or explanation of services provided. It was also alleged that an individual associated with the contract was potentially releasing U.S. Government information without authorization.
- OIG conducted an investigation based on concerns that the NRC Office of Investigations (OI) did not conduct a thorough investigation into a St. Lucie Nuclear Power Plant employee’s claim that plant management retaliated against the employee for raising safety concerns at the plant.
- OIG conducted an investigation into an allegation by an Indian Point Energy Center (IPEC) employee that IPEC managers provided false information to OI during an OI investigation into the employee’s complaint that IPEC discriminated against the employee for raising safety concerns. The employee also questioned why NRC regional management had administratively closed a different allegation the employee had raised and requested that NRC continue the investigation.
- OIG conducted an investigation based on a series of anonymous allegations concerning hiring practices and vacancy promotion selections by NRC regional management. Specifically, the allegations questioned (1) the promotion selections of two individuals for branch chief positions; (2) the reassignment of two branch chiefs; (3) the promotion of an individual into a senior executive service position; and (4) the hiring of a family member by an NRC regional manager.

---

# OVERVIEW OF NRC AND OIG

## *NRC's Mission*

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

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

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



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

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



---

## *OIG History, Mission, and Goals*

### **OIG History**

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

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

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

---

## OIG Mission and Goals

NRC's OIG was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendment to the IG Act. NRC OIG's mission is to (1) independently and objectively conduct and supervise audits and investigations relating to NRC programs and operations; (2) prevent and detect fraud, waste, and abuse; and (3) promote economy, efficiency, and effectiveness in NRC programs and operations.

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

The plan identifies OIG's priorities and establishes a shared set of expectations regarding the goals OIG expects to achieve and the strategies that will be employed to do so. OIG's *Strategic Plan* features three goals, which generally align with NRC's mission and goals:

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



*Reactor vessel head.*



---

# NRC OIG PROGRAMS AND ACTIVITIES

## *Audit Program*

The OIG Audit Program focuses on NRC and DNFSB management and financial operations; economy or efficiency with which the NRC and DNFSB organizations, programs, or function are 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 NRC and DNFSB operations and promote greater economy and efficiency. Audits comprise four phases:

- **Survey phase**—An initial phase of the audit process is used to gather information, without detailed verification, on the agency’s organization, programs, activities, and functions. An assessment of vulnerable areas determines whether further review is needed.
- **Verification phase**—Detailed information is obtained to verify findings and support conclusions and recommendations.
- **Reporting phase**—The auditors present the information, findings, conclusions, and recommendations that are supported by the evidence gathered during the survey and verification phases. Exit conferences are held with management officials to obtain their views on issues in the draft audit report. Comments from the exit conferences are presented in the published audit report, as appropriate. Formal written comments are included in their entirety as an appendix in the published audit report.
- **Resolution phase**—Positive change results from the resolution process in which management takes action to improve operations based on the recommendations in the published audit report. Management actions are monitored until final action is taken on all recommendations. When management and OIG cannot agree on the actions needed to correct a problem identified in an audit report, the issue can be taken to the NRC and DNFSB Chairman for resolution.

Each October, OIG issues an NRC and DNFSB *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(s)*. OIG audit staff continually monitor specific issue 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 NRC and DNFSB programs and activities.

---

## *Investigation Program*

OIG's responsibility for detecting and preventing fraud, waste, and abuse within NRC and DNFSB includes investigating possible violations of criminal statutes relating to NRC and DNFSB programs and activities, investigating misconduct by NRC and DNFSB 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 and DNFSB 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 and DNFSB's mission is the protection of public health and safety, OIG's Investigative Program directs much of its resources and attention to investigating allegations of NRC and DNFSB staff conduct that could adversely impact matters related to health and safety. These investigations may address allegations of

- Misconduct by high-ranking and other NRC and DNFSB officials, such as managers and inspectors, whose positions directly impact public health and safety.
- Failure by NRC and DNFSB management to ensure that health and safety matters are appropriately addressed.
- Conflicts of interest involving NRC and DNFSB employees and contractors, including such matters as promises of future employment for favorable or inappropriate treatment and the acceptance of gratuities.
- Fraud in the NRC and DNFSB 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, MD's, 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, OIG requests a written reply from the agency within 90 days, with either a substantive reply or status of issues raised by OIG.

From October 1, 2015, to March 31, 2016, OIG reviewed a variety of agency documents including Commission papers (SECYs), Staff Requirements Memoranda, Federal Register Notices, MD's, regulatory actions, and statutes.

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

MD and Handbook (DH) 6.5, *NRC Participation in the Development and Use of Consensus Standards*. An overall OIG observation on the draft revised handbook was that it does not include guidance on a significant change to the Directive associated with a new body described as the "Technical Forum." The Technical Forum makeup and function is only generally addressed in the responsibilities section of the Directive, and no guidance is provided in the Handbook on the actual process for use of the Technical Forum nor is this term included in the glossary. Comments on specific sections of the draft inquired as to the basis of some deleted actions, notably, consultation with the General Counsel on standards issues, as well as the need for additional process and procedure clarification.

MD and DH 13.1, *Property Management*. OIG noted the authority of the Inspector General regarding approval of actions for OIG employees, and the need for updating the agency employee separation clearance form.

MD and DH 10.62, *Leave Administration*. OIG noted the need to reflect the authority of the Inspector General over actions involving OIG employees, as well as noting the need to clarify verification processes and approval determinations related to the authorization of absences.



---

## *Other OIG General Counsel Activities*

### **NRC OIG Obtains 2302 (c) Certification**

During this period, NRC OIG obtained “2302(c) Certification” from the Office of Special Counsel (OSC).

Congress enacted 5 U.S.C. § 2302(c) in response to reports of limited understanding in the Federal workforce concerning employees’ right to be free from prohibited personnel practices, especially retaliation for whistleblowing. Section 2302(c) requires agency heads to ensure, in consultation with the OSC that employees are informed of the rights and remedies available to them under the Civil Service Reform Act (CSRA), the Whistleblower Protection Act (WPA), and related laws. In 2002, OSC established a “2302(c) Certification Program” to provide agencies and agency components with a process for meeting this statutory requirement. In 2014, the White House directed agencies to take affirmative steps to complete OSC’s program.

OSC’s 2302(c) Certification Program verifies that Federal agencies have met the statutory obligation to inform their workforces about the rights and remedies available to them under the CSRA, the WPA, and the Whistleblower Protection and Enhancement Act.

---

## Other OIG Activities

### NRC OIG Receives CIGIE Award for Excellence

*The Council of the Inspectors General on Integrity and Efficiency (CIGIE) recognized the Nuclear Materials and Waste Safety Audit Team with the prestigious CIGIE Award for Excellence. The audit team was acknowledged by CIGIE for exceptional performance in identifying ways to improve NRC's oversight of spent fuel pools containing highly radioactive materials. The team consisted of Michael Blair, Audit Manager; Amy Hardin, Senior Auditor; Sherri Miotla, Team Leader; Kevin Nietmann, Senior Technical Advisor; and Regina Revinzon, Auditor.*

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 (also known as high-level radioactive waste). At the time of the audit, for both operating and permanently shutdown nuclear power plants in the United States, there were a total of 93 spent fuel pools that stored spent nuclear fuel. Spent fuel pools are deep pools of water that hold thermally hot and intensely radioactive spent (used) nuclear fuel after its removal from a nuclear reactor. The water in the spent fuel pools acts as a shield to reduce the radiation levels that people working outside the pool may be exposed to, and it also cools the spent fuel that continues to produce heat for several years after removal from the reactor.

The OIG audit team found that opportunities exist for the improvement of NRC's oversight of spent fuel pools and the nuclear fuel they contain, which would further enhance the protection of public health and safety and the environment. 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. To accomplish this, NRC's spent fuel pool oversight would be more effective for the long term with additional guidance for NRC staff and licensees in the following areas:

- Improved criticality analyses guidance and reviews to enhance the clarity and predictability of NRC's licensing process related to spent fuel pools.
- Enhanced reactor oversight process inspection guidance to call attention to spent fuel pools and their related systems.

To improve NRC's oversight of spent fuel pools, the OIG audit team made recommendations to develop and implement spent fuel pool inspection guidance at operating reactors, develop an enforceable neutron-absorbing material aging management program, and update a specific inspection procedure.

*The Council of the Inspectors General on Integrity and Efficiency (CIGIE) recognized this Spent Fuel Pool Audit as one of the most “newsworthy” from among all of the CIGIE award winners for excellence in audit.*



*OIG receives CIGIE award. Pictured left to right are Sherri A. Miotla, Team Leader; Stephen D. Dingbaum, Assistant Inspector General for Audits; Regina M. Ravinzon, Auditor; Michael A. Blair, Audit Manager; Hubert T. Bell, Inspector General; Amy L. Hardin, Senior Auditor; and David C. Lee, Deputy Inspector General. Not pictured are Kevin J. Nietmann, Senior Technical Advisor; and Steven E. Zane, Deputy Assistant Inspector General for Audits.*  
Source: NRC

Because of the audit team members' commitment and very strong work ethic, the team was able to successfully complete the audit in less than 6 months and issue a report with four recommendations to strengthen the agency's oversight of spent fuel pools. While this could have been a highly contentious report, the audit team worked hard to ensure that the report was accurate, clear, concise, and balanced. As a result, a variety of stakeholders (e.g., NRC, Union of Concerned Scientists, and the industry) agreed with the report findings and recommendations and praised the audit team for a job well done. NRC is currently working to implement actions in response to the OIG audit team's recommendations.

---

# NRC MANAGEMENT AND PERFORMANCE CHALLENGES

## **Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission\*** **as of October 1, 2015** *(as identified by the Inspector General)*

Challenge 1 *Regulation of nuclear reactor safety programs.*

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

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

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

Challenge 5 *Management of financial programs.*

Challenge 6 *Management of administrative functions.*

*\*For more information, see OIG-15-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing NRC  
<http://www.nrc.gov/docs/ML1527/ML15274A142.pdf>*



# NRC AUDITS

To help the agency improve its effectiveness and efficiency during this period, OIG completed 10 financial and performance audits or evaluations, which resulted in numerous recommendations to NRC management. A selection of these reports are summarized in this section. During this semiannual reporting period, the Defense Contract Audit Agency did not complete any contract audits for OIG.

## Audit Summaries

### Audit of NRC's Personal Identity Verification (PIV) Card Access System

*OIG Strategic Goal: Security*

#### Sample PIV Card With Expiration Date



The Personal Identity Verification (PIV) card is an identification card issued by a Federal agency that contains information unique to each employee and contractor. The main function of the card is to protect and to strengthen the security of both employees' and contractors' information and physical access to secured areas. NRC utilizes the PIV card to control physical access at its headquarters and regional offices.

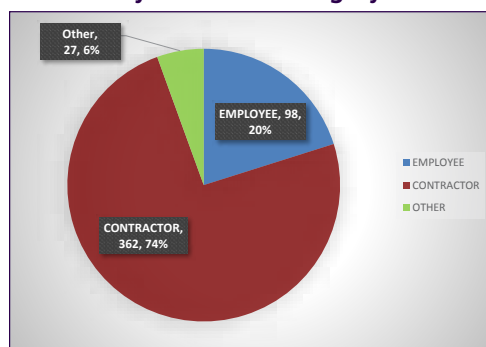
Federal policies require agencies to swiftly revoke physical access rights at termination of employment. NRC must collect and destroy PIV cards from Federal employees and contractors upon termination.

Additionally, some areas within NRC are restricted to certain individuals. Each restricted area has a designated representative who must maintain an up-to-date access list of individuals needing access.

The audit objective was to determine whether NRC's PIV card access system meets its operational requirements, and to assess the effectiveness of the PIV system coordination among offices that have a role in securing NRC's physical access.

#### Audit Results:

##### Percentage of PIV Cards Not Returned by Personnel Category



NRC's PIV card access system meets its operational requirements and there is some coordination among offices. However, opportunities exist to (1) strengthen processes to ensure a greater percentage of PIV card retrieval upon termination and (2) establish a uniform and effective way for the designated representative to notify security officials of changes to contractor and employee access rights for restricted areas.

PIV cards for terminated contractors and employees are not always retrieved. Despite having a process in place to prepare an employee to terminate from the agency, PIV card retrieval

---

does not always occur, and retrieval procedures have not been established to ensure collection. OIG identified that of 1,452 terminated PIV cards over a 22-month period (January 2014 through November 2015), approximately 33 percent were not physically collected or retrieved from the terminated contractor or employee. As a result, there is a risk of unauthorized physical access to NRC and other Federal facilities.

In addition, NRC receives inconsistent notification of (1) changes in staff/contractor access rights for restricted areas and (2) a change to the designated representative for a restricted area. Consequently, the potential exists for unauthorized physical access into a restricted area by a contractor or employee who should no longer have access.

*(Addresses Management and Performance Challenge #3)*

## **Audit of NRC's Operator Licensing Program for the AP1000 Power Reactor**

### ***OIG Strategic Goal: Safety***

NRC licenses the individuals who operate the controls or supervise operation of commercial nuclear power reactors. Before NRC licenses someone to operate controls of a commercial nuclear power reactor, this individual must complete extensive training and pass rigorous, site-specific written examinations and operating tests that are relevant to the design and construction of the facility they will operate.

Four Advanced Passive 1000 (AP1000) Pressurized Water Reactors are under construction, two at Virgil C. Summer Nuclear Station in South Carolina and two at Vogtle Electric Generating Plant in Georgia. This is a new reactor design for which operators have never been licensed. An operator's license authorizes the license holder to manipulate the controls of the facility, which directly affect the reactivity or power level of the reactor. By the year 2020, approximately 70 licensed operators will be needed for the AP1000.

The audit objective was to determine if NRC's program for licensing AP1000 reactor operators is efficiently and effectively implemented.

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

The efficiency and effectiveness in NRC's licensing of AP1000 reactor operators can be improved. Key questions concerning the new reactor operator licensing requirements governing the time interval between administration of the written examination and operating test are currently unresolved. Additionally, requirements for qualifying new simulators for use during the AP1000 operating test are unclear. In the meantime, one of the AP1000 licensees has administered the written exam to its operator candidates without having a simulator approved for use in the operating test.

**AP1000 Power Reactor Illustration**



*Source: Westinghouse*

---

These program weaknesses have occurred because NRC management and staff responsible for licensing operators have held differing interpretations of regulations and guidance pertaining to the AP1000 operator licensing process. In particular, headquarters and regional staff have not agreed on the extent to which existing regulations and guidance allow the Office of New Reactors to grant permission for exceeding the 30-day examination time interval. According to NRC management and staff, the fundamental disagreement is whether evolving developments associated with AP1000 operator licensing, including the status of licensee simulation facilities, justify requests to exceed the examination time interval in NUREG-1021 and, if so, under what conditions.

In addition, NRC management has not officially documented all operator licensing key decisions related to examination timing and simulator results.

*(Addresses Management and Performance Challenge #1)*

## **Audit of NRC's Network Security Operations Center**

### ***OIG Strategic Goal: Security***



NRC's Network Security Operations Center (SOC) is responsible for securing the agency's network infrastructure and monitoring the network for suspicious activity. The SOC accomplishes this through the use of automated security tools, analysis of network activity data, and participation in incident response efforts. The SOC is primarily staffed by contractors working under the Information Technology Infrastructure Support Services (ITISS) contract.

Robust SOC capabilities are particularly crucial given the sensitivity of the unclassified information processed on NRC's network, and the increasing volume of attacks carried out against Federal Government computer systems.

The audit objective was to determine whether NRC's network SOC meets operational requirements, and to assess the effectiveness of SOC coordination with other organizations that have a role in securing NRC's network.

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

NRC's network SOC currently meets operational security requirements stipulated in the ITISS contract. However, the current contract is not optimized to meet NRC's needs, and opportunities exist to improve the SOC's range of capabilities and coordination with other NRC stakeholders.

---

Performance-based contracting is the preferred approach to Federal contracting. In this approach, the Government customer defines its needs in terms of the results it is seeking, in addition to metrics for measuring contractor performance, rather than describing the process that the contractor will use.

NRC staff described several areas in which the SOC does not meet agency needs, including proactive analysis and timely, detailed reports. This occurs because although the contract performance criteria are aligned with National Institute of Standards and Technology and NRC internal guidance, the contract does not clearly define SOC performance goals and metrics that can be used to determine whether agency needs are being met.

Additionally, SOC staff and NRC stakeholders expressed differing expectations of SOC roles and responsibilities. This occurs due to a lack of adequate definitions in agency policies and undifferentiated functional descriptions between different entities responsible for securing NRC's network. Without a clear definition of organizational roles and responsibilities, successful coordination of SOC activities with NRC stakeholders depends heavily on interpersonal relationships. When relationships and communications fail, this can result in duplication of effort, redundant followup tasks, and extra meetings to discuss responsibilities and clarify expectations. Furthermore, contractor staff who run the SOC need clear guidance on their stakeholder support obligations to prioritize work and optimize use of limited resources.

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

## **Evaluation of NRC's Agencywide Documents Access and Management System Functional and Operational Capabilities**

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

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. NRC's Office of the Chief Information Officer manages ADAMS, and staff in headquarters and regional offices use ADAMS for their day-to-day mission activities. The public uses NRC's public site to access Web-based ADAMS.

The evaluation objective was to perform an independent evaluation of NRC's ADAMS to determine if it 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, ease-of-use (i.e., usability), and other aspects such as availability, performance, contingency planning, and security. This evaluation also includes a review of relevant NRC policies and procedures that define what and how documents are input, how and who can access them, and for how long they are stored since ADAMS efficacy is directly affected by these policies and procedures.



---

### *Evaluation Results:*

ADAMS has the capability to serve as the agency's repository for official agency records. However, opportunities exist to improve ADAMS' Federal and NRC records management, search and retrieval functionality, and management oversight over ADAMS operations.

**ADAMS does not currently satisfy records disposition objectives.** Currently, ADAMS does not transfer permanent records or destroy temporary records in accordance with NRC's Comprehensive Records Disposition Schedule. Although the system's record management software can be used to manage records retention scheduled, it was not configured to do so.

**ADAMS search and retrieval functionality occasionally returns irrelevant or incomplete results.** ADAMS users are generally dissatisfied with search and retrieval functionality due to issues connected with the use and population of ADAMS profiles and templates, which affects search effectiveness. For example, the profiling process that feeds into the ADAMS search functionality is not uniformly used across offices. In addition, information is not entered into ADAMS consistently.

**System shortfalls pertain to compliance with security standards and adherence to configuration management best practices.** Specifically, (1) ADAMS is operating without a current Authority to Operate, (2) ADAMS has not fully implemented National Institute of Standards and Technology Special Publication 800-53 Revision 4, (3) management of ADAMS system configurations and security documentation is not consistently implemented, and (4) many ADAMS planned security remediation activities are delayed.

*(Addresses Management and Performance Challenge #4)*

## **Results of the Audit of the United States Nuclear Regulatory Commission's Financial Statements for Fiscal Years 2015 and 2014**

### *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.

***Audit Results:***

**Financial Statements:** The auditors expressed an unqualified opinion on the agency's FY 2014 and FY 2015 financial statements.

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

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

*(Addresses Management and Performance Challenge # 5)*

## **Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2015**

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

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

The evaluation objective was to perform an independent evaluation of NRC's implementation of FISMA 2014 for FY 2015.

### ***Evaluation Results:***

While the agency has continued to make improvements in its information technology (IT) security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the evaluation identified the following IT security program weaknesses:

- There is a repeat finding from the FY 2014 FISMA evaluation: continuous monitoring is not performed as required.

- 
- There is a repeat finding from previous FISMA evaluations: configuration management procedures are still not consistently implemented.
  - There is a repeat finding from several previous FISMA evaluations: plan of action and milestone management still needs improvement.
  - There is a repeat finding from previous FISMA evaluations: the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

There were no new findings for FY 2015. 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 Challenges # 3 and #4)*

## **Audit of NRC's Oversight of Medical Uses of Nuclear Material**

### ***OIG Strategic Goal: Safety***

#### **Gamma Knife uses beams of radiation to treat cancerous brain tumors**



Source: NRC

NRC is responsible for overseeing the medical uses of nuclear material through its licensing, inspection, and enforcement programs. The types of medical uses regulated by NRC include diagnostic, therapeutic, and research. NRC issues medical use licenses to medical facilities, develops guidance and regulations for use by licensees, and maintains a committee of medical experts to obtain advice about the use of byproduct materials in medicine.

This committee, the Advisory Committee on the Medical Uses of Isotopes (ACMUI), is an independent committee established by the NRC for the express purpose of advising NRC staff. ACMUI provides NRC staff with advice, technical assistance, and

consulting services, and brings key issues to the attention of NRC staff for appropriate action.

When a medical facility has a potential problem using radioactive material, it may meet NRC's criteria for a medical event. These events may involve doses to a patient of the wrong amount, the wrong radioactive drug, incorrect administration of a drug, or dose to the wrong patient or wrong part of the body. There are about 40 medical events each year.

The audit objective was to determine if NRC's oversight of medical uses of radioactive isotopes adequately protects public health and safety.

---

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

NRC provides adequate oversight of the medical uses of radioactive isotopes to protect public health and safety; however, opportunities for improvement exist with regard to clarifying NRC's medical event policy, periodically assessing medical event reporting, and providing better feedback to ACMUI.

Medical event reporting requirements are inconsistently understood by licensees and NRC staff. Specifically, OIG learned that several licensees either underreported, or reported and later retracted, medical events. Furthermore, a specific interim guidance document had to be written to help address some of the confusion. This inconsistent understanding is due to a general lack of clarity surrounding NRC's requirements and purpose for reporting medical events. Furthermore, NRC provides insufficient medical event data to medical licensees. As a result, NRC is not effectively achieving all the possible benefits of medical event reporting.

NRC has not conducted a periodic self-assessment of its medical events reporting requirements to determine if they are effectively meeting their intended purpose. As a result, NRC is not in a position to make any informed conclusions regarding the effectiveness of its approach to collecting information on medical events.

NRC does not routinely provide sufficiently detailed feedback to ACMUI despite relying on it as a key advisory body. This lack of sufficiently detailed feedback is a result of NRC not having current, formalized policies and procedures that clearly articulate the expectations for providing feedback to ACMUI. As a result, the benefits of having the ACMUI provide expert advice may not be fully realized and the potential for miscommunication and misunderstanding remains.

*(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, 2015. 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 Decommissioning Funds Program**

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

Under 10 CFR Part 50.75, NRC must receive reasonable assurances from nuclear reactor licensees that funds will be available for the decommissioning process. As of the prior biennial reporting and review period (as of December 31, 2012), the Decommissioning Trust Funds dedicated to NRC requirements for decommissioning and radiological decontamination totaled \$45.7 billion. During the spring of calendar year 2015, NRC reviewed biennial decommissioning reports submitted by licensees that include information as of December 31, 2014.

It is important to understand NRC actions to ensure that the licensees have reasonable plans in place to make up any shortfalls that exist between the current funded amount and the amount estimated as needed by NRC's two-tiered formula. (The formula can be found in 10 CFR 50.75(c).) OIG and the Government Accountability Office previously reported that NRC's decommissioning formula was developed in 1986 and may not reliably estimate adequate decommissioning costs (see Audit Report OIG-06-A-07, dated February 6, 2006, and GAO-12-258, dated April 2012).

The audit objectives are to (1) identify opportunities for program improvement, and (2) determine the adequacy of NRC's processes for coordinating with licensees to address possible shortfalls.

*(Addresses Management and Performance Challenge #5)*

### **Audit of NRC's Financial Managers' Financial Integrity Act Process**

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

NRC is mandated by the Federal Managers' Financial Integrity Act (FMFIA) with the responsibility to establish and maintain effective internal control over its operations. OMB Circular A-123, "Management's Responsibility for Internal Control," provides Federal agencies with guidance for complying with FMIA and defines management's responsibility for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.

MD 4.4, Internal Control, was revised to comply with FMFIA requirements. MD 4.4 specifies procedures for establishing a uniform, agencywide process which meets FMIA requirements. The MD handbook provides a general framework for implementing the entire internal control process. It is management's responsibility to develop the detailed internal control policies, procedures, and practices that best fit each business need.

---

OIG has completed an annual review of FMFIA assurance statements every year since 2008. This year, OIG plans to review the supporting documentation for the statements of assurance submitted by NRC business line managers.

The audit objectives are to (1) assess NRC's 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 statement of assurance as published in the agency's Performance and Accountability Report.

*(Addresses All Management and Performance Challenges)*

## **Survey of NRC's Safety Culture and Climate**

### ***OIG Strategic Corporate Management***

In 1998, 2002, 2006, 2009, and 2012, OIG contracted with an independent contractor to conduct surveys that evaluated the organizational safety culture and climate of the agency's workforce and identified agency strengths and opportunities for improvements. Comparisons were made to the previous surveys as well as to national and Government norms. In response to the survey results, the agency evaluated the key areas for improvement and developed strategies for addressing them.

A clear understanding of NRC's current safety culture and climate will facilitate identification of agency strengths and opportunities for improvement as it continues to experience significant challenges. These challenges include the licensing of new nuclear facilities, disposal of high-level waste, the loss of valuable experience from retirements, operating under continuing resolutions, and legislation that froze Federal civilian employee pay rates.

The survey objectives are to (1) measure NRC's safety culture and climate to identify areas of strength and opportunities for improvement, (2) compare the results of this survey against the survey results that OIG reported previously, and (3) provide, where practical, benchmarks for the qualitative and quantitative findings against other organizations.

*(Addresses All Management and Performance Challenges)*

## **Audit of NRC's Technical Assistance Request Process**

### ***OIG Strategic Goal: Safety***

The Technical Assistance Request (TAR) process is used to address questions or concerns raised within the NRC regarding regulatory compliance and safety oversight programs. The process should ensure that questions or concerns raised by NRC organizations are resolved in a timely manner and the resolutions are appropriately communicated.

---

A TAR is a written request submitted to the Office of Nuclear Material Safety and Safeguards for technical assistance. A TAR can be originated by a region, an Office of Nuclear Material Safety and Safeguards division, or another NRC office. A TAR contains questions pertaining to regulatory or policy interpretations, inspection findings, or technical areas; for example, a TAR might be used to seek information on a specific facility or vendor licensing basis, applicable staff positions on an issue, regulatory requirements, or the safety or risk significance of particular facility configurations or operating practices. A TAR request may also be used to obtain information on an allegation-related issue. Ensuring that adequate, appropriate, and timely feedback is provided to NRC staff is central to the agency's mission to protect public health and safety and the environment.

The audit objective is to determine if the agency's TAR process facilitates effective and efficient responses.

*(Addresses Management and Performance Challenge #2)*

## **Audit of NRC's Reactor Oversight Process**

### ***OIG Strategic Goal: Safety***

NRC provides oversight of commercial nuclear power plants through the Reactor Oversight Process (ROP) to verify that the plants are being operated in accordance with NRC rules, regulations, and license requirements. Generally, the ROP uses both performance indicators and NRC inspections—including baseline-level inspections—to assess the safety performance and security measures of each plant. The NRC determines its regulatory response to performance issues in accordance with an action matrix that provides for a range of actions commensurate with the significance of performance indicators and inspection results. The actions of the matrix are graded such that, as licensee performance declines, NRC oversight increases and the agency may perform supplemental inspections and take additional actions to ensure that significant performance issues are addressed.

Recently, safety-significant issues have arisen that did not garner regulatory attention until after NRC oversight was increased under ROP. For example, one nuclear power plant received increased NRC scrutiny in the aftermath of inadequate flood preparations and an electrical fire, and a significant number of safety-related components were subsequently discovered to be in service past their recommended service life.

The audit objective is to assess the effectiveness of the ROP in discovery of plant performance issues.

*(Addresses Management and Performance Challenge #1)*



---

## **Audit of NRC's Implementation of 10 CFR 50.59 (Changes, Tests and Experiments)**

### ***OIG Strategic Goal: Safety***

10 CFR 50.59 establishes the conditions under which licensees may make changes to their facility or procedures and conduct tests or experiments without prior NRC approval. NRC is responsible for consistently and effectively overseeing licensee implementation of 10 CFR 50.59. The Office of Nuclear Reactor Regulation's Generic Communications Branch, as the agency's 10 CFR 50.59 process owner and subject matter expert, assists regional inspectors and headquarters staff in resolving 10 CFR 50.59-related questions.

Under the provisions of 10 CFR 50.59, a licensee is allowed to make changes to the facility and its operation as described in the final safety analysis report (as updated) or conduct tests or experiments not described in the final safety analysis report without prior NRC approval, provided a change in the technical specifications (TS) incorporated into the license is not involved, and the change does not satisfy any of the eight criteria for prior NRC approval specified in Paragraph (c)(2). These criteria must be used to determine whether plant safety, safety limits, or design basis are impacted. If a change to the TS is required, or if any of the criteria in Paragraph (c)(2) are met, the licensee must apply for and obtain a license amendment per 10 CFR 50.90 prior to implementing the change, test, or experiment. The licensee must maintain records of such changes, supported by a safety evaluation that provides the basis for the determination that prior NRC approval was not required, and report such changes to the NRC.

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

*(Addresses Management and Performance Challenge #1)*

## **Audit of NRC's Significance Determination Process for Reactor Safety**

### ***OIG Strategic Goal: Safety***

NRC developed the Significance Determination Process (SDP) to characterize the safety significance of inspection findings at operating nuclear power reactors. NRC intends the SDP to provide a decision logic that remains constant across inspection findings, thereby minimizing risk that SDP results will be influenced by individual judgments. NRC believes this objectivity is achieved when different individuals using SDP tools arrive at the same result given the same inputs, conditions, and assumptions.

In response to a 2013 Government Accountability Office report (*Analysis of Regional Differences and Improved Access to Information Could Strengthen NRC Oversight*), NRC

---

noted it believes existing internal controls ensure consistent SDP results but would still consider enhancements to improve consistency.

The audit objective is to assess the consistency with which NRC evaluates power reactor safety inspection findings under the SDP.

*(Addresses Management and Performance Challenge #1)*

## **Evaluation of NRC's Security Over Publicly Accessible Web Applications**

### ***OIG Strategic Goal: Security***

NRC manages numerous publicly accessible Web applications to share nuclear information with licensees and the public. NRC's publicly accessible Web applications consist mainly of Web sites, but also include Web-based login portals and administrative systems that provide authorized personnel remote access to agency information technology resources. NRC is a regular target of cyber attacks because it maintains technical and other sensitive information highly sought by criminals.

The evaluation objective is to determine the effectiveness of NRC's efforts to secure its publicly accessible Web applications.

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

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

### ***OIG Strategic Goal: Security***

According to the President, protecting national security information and demonstrating our commitment to open government through the proper application of classification standards are equally important and compatible priorities. The National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission) concluded that over-classification and inadequate information sharing contributed to the Government's failure to prevent the attacks of September 11, 2001.

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

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

---

## Audit of NRC's Covered Systems

### *OIG Strategic Goal: Security*

The Cybersecurity Act of 2015 requires Inspectors General to report on covered systems. The act defines covered systems as a national security system, or a Federal computer system that provides access to personally identifiable information. The act stipulates that the Inspector General shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report on covered systems not later than August 24, 2016,—240 days after the date of enactment of the act. The report is to include

- A description of the logical access policies and practices used by NRC to access covered systems, including whether appropriate standards were followed.
- A description and list of the logical access controls and multifactor authentication used by NRC to govern access to covered systems by privileged users.
- A description of information security management practices used by NRC.
- A description of NRC's policies and procedures relative to ensuring that entities, including contractors, that provide services to NRC are implementing information security management practices used by NRC.

The audit objective is to assess NRC's information technology security policies, procedures, practices, and capabilities relative to covered systems as defined in the Cybersecurity Act of 2015.

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



*Security gates at Calvert Cliffs Power Plant.*





*Fire equipment inspection by NRC Resident Inspector.*



---

# NRC INVESTIGATIONS

*During this reporting period, OIG received 124 allegations, initiated 21 investigations, and closed 20 cases. In addition, the OIG made one referral to NRC management and four to the Department of Justice.*

## *Investigative Case Summaries*

### **Potential Lack of Oversight of Water Leakage and Safety Culture at Palisades Nuclear Power Plant by Region III**

#### ***OIG Strategic Goal: Safety and Security***

OIG conducted an investigation based on two specific issues raised by Congress and members of the public regarding safety concerns at the Palisades Nuclear Plant in Covert, MI. The first issue involved the NRC response to the May 2011 discovery of a water leak in the control room at Palisades. This ultimately resulted in a June 2012 forced maintenance outage to inspect and repair leakage that was found to originate from the Safety Injection Refueling Water Tank (SIRWT). The investigation addressed concerns that NRC had, over a period of more than a year, “tolerated,” or otherwise inadequately responded to, a leak with the potential to grow and to affect safety related control room components. The second issue addressed in this investigation involved the adequacy of the NRC staff’s handling of identified safety culture concerns among Palisades’ employees.

#### ***Investigative Results:***

OIG did not develop evidence to substantiate that the NRC staff failed to act appropriately or in a timely manner when dealing with the May 2011 discovery of leakage from the SIRWT affecting the Palisades control room. NRC staff was notified on the day the leak was first detected in the control room, promptly relayed this information to regional management, and initiated regular monitoring of licensee followup. OIG found no evidence that water had leaked into the control room in sufficient quantities to cause safety related equipment failures. The NRC staff learned that the “catacombs” area, below the tank and above the control room, in which the leakage apparently originated, had not been inspected in over 20 years, and issued a green finding addressing this issue in August 2011. OIG found that, under the Technical Specifications of the plant, such leakage would not, in and of itself, require that the SIRWT be declared inoperable and the reactor shut down. OIG and the NRC Office of Investigations developed information that between June 2011 and February 2012, the licensee staff inaccurately told NRC staff that their findings were “inconclusive” as to whether the source of the leakage was the SIRWT or other sources, such as rain. The licensee acknowledged in February 2012 that the source of the leak was the SIRWT and initiated repairs when the plant was in a scheduled shutdown condition in April 2012.

OIG found that after the tank was repaired during the scheduled outage and refilled in June 2012, a new, higher rate leak began, and again affected the control room. This leakage was found to have occurred due to welding problems and stresses on

---

the tank bottom associated with the April 2012 repairs. This new leakage affected a wider portion of the catacombs area as well as resuming within the control room. Again, NRC staff responded promptly to confirm that the leakage did not affect safety related equipment. On June 12, 2012, the licensee determined that the leakage rate had reached the NRC supported limit, rendering the tank inoperable and requiring a forced shutdown. NRC issued a second green finding for the licensee's failure to adequately evaluate the SIRWT leakage and for initially seeking to set a less conservative limit on acceptable leakage, based upon that inadequate evaluation. The NRC also issued a July 2012 Confirmatory Action Letter (CAL) to the licensee in connection with continuing water leak issues from the SIRWT. This CAL required the licensee to institute continuous monitoring of the leakage, with shutdown required if leakage exceeded set levels, and provided the licensee with specific requirements for the repair of the tank and associated supporting structures. The CAL was closed out after additional 2013 repairs during which the licensee replaced large sections of the tank bottom and support structures beneath the SIRWT and above the control room. No further SIRWT leakage incidents have been documented since 2013.

Regarding safety culture, OIG found no evidence that the NRC failed to act appropriately or in a timely manner when dealing with the safety culture issues disclosed in 2010 and 2011 at Palisades. The underlying incidents that gave rise to the safety culture concerns at the plant were addressed by NRC consistently with regulatory requirements. The 2010 incident was addressed in part through NRC issuance of a confirmatory order, one of whose requirements was a survey by an outside safety culture contractor. The results of this survey were shared with NRC after it was completed in April 2012. NRC staff engaged in continued monitoring of safety culture issues, as demonstrated by the history of followup inspections between 2012 and 2014, which showed improvements in safety culture among Palisades technical and operations staff.

*(Addresses Management and Performance Challenge #1)*

## **Mismanagement of Office of Information Services Contract**

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

OIG conducted an investigation based on an NRC employee's allegation that an NRC employee involved with managing an NRC independent verification and validation (IV&V) contract, was authorizing \$400,000 of expenses each month with no deliverables or explanation of services provided and that an individual associated with the contract was potentially releasing U.S. Government information without authorization.

### ***Investigative Results:***

OIG did not substantiate mismanagement or misappropriation of funds relating to the various IV&V task order activities in which the NRC employee participated.

---

Overall, NRC managers expressed that the work completed as a result of the IV&V contract was beneficial to the agency. Further, during the contract period of 34 months, the IV&V contract averaged expenses of \$69,749 per month; the highest month was \$205,735 and the lowest actual expensed month was \$1,176, and there were 5 months with no expenses.

OIG found that the NRC employee provided internal agency information, specifically, the names and titles of incumbent contractor employees to individuals outside of NRC without authorization and who lacked an official need to know. OIG also found e-mail communications and attachments were disclosed by the NRC employee to her ex-husband and to her daughter, concerning an NRC evaluation of IT vendors capabilities and NRC internal IT strategy and future service requirements, respectively. The United States Attorney's Office declined prosecution of the matter.

*(Addresses Management and Performance Challenges #1 and #5)*

## **Concerns Pertaining to NRC Office of Investigations Case Involving Pressurizer Safety Valve Leak at St Lucie Nuclear Power Plant**

### ***OIG Strategic Goal: Safety and Security***

OIG conducted this investigation based on concerns that the NRC Office of Investigations did not conduct a thorough investigation into a St. Lucie Nuclear Power Plant (SLNPP) employee's claim that plant management retaliated against him for raising safety concerns at the plant.

### ***Investigative Results:***

OIG found that in reviewing the SLNPP employee's concerns OI staff members followed its process and exercised investigative judgment, which is allowed under OI's process.

Nevertheless, OIG identified several areas where potential evidence could have been pursued in greater detail. As a result of the OIG investigation, the OI Director directed the OI staff to follow up on certain investigative steps relative to the case and initiated measures, including revising harassment and intimidation investigation training for all agents, increased oversight responsibilities for Special Agents in Charge and headquarters operations staff, and documentation of all investigative decisions during the investigative process.

*(Addresses Management and Performance Challenge #1)*

---

## **Concern Pertaining to Promotion Selection Process by NRC Region II Management**

### ***OIG 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 to the Office of Investigations During Its Harassment and Intimidation Investigation of Licensee**

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

OIG conducted an investigation into an allegation by an Indian Point Energy Center (IPEC) employee that IPEC managers provided false information to the NRC Office of Investigations (OI) during an OI investigation into the employee's complaint that IPEC discriminated against the employee for raising safety concerns. The IPEC employee claimed, in part, that IPEC managers had provided inaccurate information pertaining to the employee being unprofessional. The employee also questioned why the NRC region had administratively closed a different allegation and requested that NRC continue the investigation.

OIG reviewed the OI investigation pertaining to whether the IPEC employee was discriminated against for raising safety concerns. The employee alleged

---

that after raising safety concerns to IPEC security management, his 2011 job performance was rated as unsatisfactory, which resulted in the employee being placed on a Performance Improvement Plan (PIP) and this subsequently affected the employee's salary and bonus. The OI investigation did not conclude that the IPEC employee was discriminated against for raising safety concerns.

***Investigative Results:***

OIG found that the investigation conducted by OI was adequate. OI's investigation concluded that based on the totality of the documentation and testimony obtained during its investigation, there was insufficient evidence to conclude that the IPEC employee was discriminated against for raising safety concerns. The OI investigation found that the employee received a letter for failing to maintain certain qualifications in accordance with plant procedures and that the employee's supervisor was having performance issues with the employee. With regard to the examples provided by the employee involving his professionalism, OI discovered that although IPEC management could not produce evidence the employee had been unprofessional with vendors, the employee was unprofessional with IPEC staff during the relevant performance rating period, which resulted in the individual being placed on a PIP.

With regard to the employee's question as to why the NRC region had administratively closed a different allegation, OIG found that Region I had informed the employee that NRC would keep the employee's file open to monitor the Department of Labor (DOL) process. The NRC region administratively closed the allegation after it was informed by DOL that since the employee elected to proceed in the U.S. District Court, DOL was dismissing the complaint.

*(Addresses Management and Performance Challenge #7)*



---

# DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created DNFSB as an independent agency within the Executive Branch to identify the nature and consequences of potential threats to public health and safety at the 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, 2015** *(as identified by the Inspector General)*

*Challenge 1 Organizational culture and climate.*

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

*Challenge 3 Human capital management.*

*Challenge 4 Internal controls for technical and administrative/financial programs.*

*\*For more information, see DNFSB-16-A-01, Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing DNFSB*

---

# DNFSB AUDITS

## *Audit Summaries*

### **Results of the Audit of DNFSB's Financial Statements for FYs 2015 and 2014**

The Accountability for Tax Dollars Act of 2002, requires the IG or an independent external auditor, as determined by the IG, to annually audit DNFSB's financial statements in accordance with applicable standards. The audit, conducted by Acuity Consulting, Inc., under a contract with OIG, includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. It also includes assessing the accounting principles used and significant estimates made by management as well as evaluating the overall financial statement presentation.

#### ***Survey Results:***

**Financial Statements:** The auditors expressed an unmodified opinion on the agency's FY 2014 and FY 2015 financial statements.

**Internal Controls Over Financial Reporting:** The auditors expressed an unqualified opinion on DNFSB's internal controls over financial reporting.

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

*(Addresses Management and Performance Challenge #4)*

### **Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014) for FY 2015**

FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

FISMA 2014 requires the annual evaluation to be performed by the agency's OIG or by an independent external auditor. OMB requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

---

The evaluation objective was to perform an independent evaluation of DNFSB's implementation of FISMA 2014 for FY 2015.

***Audit Results:***

While DNFSB has made progress in addressing the findings from the FY 2014 FISMA evaluation, it has not completed implementation of any of the recommendations.<sup>1</sup> There are no new findings; however, the four findings from the FY 2014 evaluation remain:

- Continuous monitoring is not performed as required.
- The security assessment and authorization of DNFSB's general support system did not follow the National Institutes of Standards and Technology risk management framework.
- DNFSB's plan of action and milestones management is inadequate.
- Oversight of systems operated by contractors or other agencies is inadequate.

*(Addresses Management and Performance Challenge #2)*

## **Audit of DNFSB's Information Security Program**

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.

DNFSB uses classified and sensitive unclassified information to conduct agency business in support of its mission. Safeguarding both classified and sensitive unclassified information is necessary for protecting national security interests, as well as the safety, security, and privacy of DNFSB employees.

The audit objective was to determine if DNFSB handles classified and sensitive unclassified information in accordance with Federal regulations.

***Audit Results:***

DNFSB has appropriate security controls for classified information and some types of sensitive unclassified information such as Personally Identifiable Information. However, opportunities exist to improve DNFSB's internal information security

---

<sup>1</sup> *OIG notes that since the November 12, 2015, issuance of the FY 2015 FISMA 2014 evaluation, DNFSB has completed implementation of five of the nine FY 2014 FISMA evaluation recommendations.*

---

guidance, and to improve access controls over Unclassified Controlled Nuclear Information (UCNI) that is stored on DNFSB's internal SharePoint site.

Federal guidance recommends that documentation of internal controls should be clear and readily available. However, DNFSB's main information security guidance is incomplete and does not address key points for protecting sensitive unclassified information. This occurred because DNFSB has not updated its primary information security guidance since May 2000. DNFSB staff need current and complete guidance to help them carry out their information security responsibilities.

Additionally, Federal regulations require a "need to know" as a condition for routine access to UCNI. However, general computer network access rights allow users to access and manipulate some UCNI documents saved on the agency's internal SharePoint site without establishing a need to know. This occurs because technical controls are not required to manage access to UCNI documents stored on SharePoint. As a result, security-related information is at greater risk of unauthorized disclosure or compromise.

*(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 in FY 2016. The FY 2016 management and performance challenges are 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 and DNFSB is responding positively to recommendations to improve the efficiency and effectiveness of its programs. The FY 2016 management and performance challenges are as follows:

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 Policy Guidance**

Like other Federal agencies, DNFSB should have a clear, organized strategy with well-defined documentation processes to support its activities that contain an audit trail, verifiable results, and specify documentation retention periods. These requirements are set forth primarily in Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control and other Federal criteria.

Prior work conducted by other audit entities at DNFSB suggests that while DNFSB had some formal documentation to support agency activities, the policy documentation for the primary mission related activities within the agency was lacking.

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

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

### **Audit of DNFSB's Oversight of Nuclear Facility Construction Projects**

DNFSB's enabling legislation assigns specific functions to the Board for accomplishing its safety oversight mission. Specifically, it states that DNFSB shall (1) review and evaluate the content and implementation of standards relating to the design, construction, operation, and decommissioning of defense nuclear facilities, and (2) review the design of a new defense nuclear facility before construction begins and shall recommend modifications of the design to ensure adequate protection of public health and safety. Furthermore, during the construction of any such facility, DNFSB shall periodically review and monitor the construction and shall submit to the Secretary, within a reasonable time, such recommendations relating to the construction of that facility.

DNFSB has articulated a strategic goal of strengthening safety in design in its 2014-2018 Strategic Plan and identified two strategic objectives for accomplishing this strategic goal. The objectives include (1) accomplish independent oversight to strengthen the use of approved nuclear standards in the design and construction of defense nuclear facilities and major modifications to existing facilities, and (2) accomplish independent safety oversight to enhance the clear and deliberate implementation of the principles and core functions of integrated safety management in the design, construction, and upkeep of safety systems in defense nuclear facilities.



---

In the FY 2014 budget, Congress authorized design and construction projects for new DOE defense nuclear facilities with an estimated cost of \$20 billion. Therefore, it is imperative that DNFSB effectively and efficiently oversee the construction of new nuclear facility construction projects in order to meet its legislated safety oversight mission and strategic objectives.

The audit objective is to assess the efficiency and effectiveness of DNFSB's oversight of nuclear facility construction projects.

*(Addresses Management and Performance Challenge #2)*

## **Audit of DNFSB's Covered Systems**

The Cybersecurity Act of 2015 requires Inspectors General to report on covered systems, i.e., a national security system, or a Federal computer system that provides access to personally identifiable information (PII.) The act stipulates that the Inspector General shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report on covered systems not later than August 14, 2016,—240 days after the date of enactment of the act. The report is to include

- A description of the logical access policies and practices used by DNFSB to access covered systems, including whether appropriate standards were followed.
- A description and list of the logical access controls and multifactor authentication used by DNFSB to govern access to covered systems by privileged users.
- A description of information security management practices used by DNFSB.
- A description of DNFSB's policies and procedures relative to ensuring that entities, including contractors, that provide services to DNFSB are implementing information security management practices used by DNFSB.

The audit objective is to assess DNFSB's information technology security policies, procedures, practices, and capabilities relative to covered systems as defined in the Cybersecurity Act of 2015.

*(Addresses Management and Performance Challenge #2)*



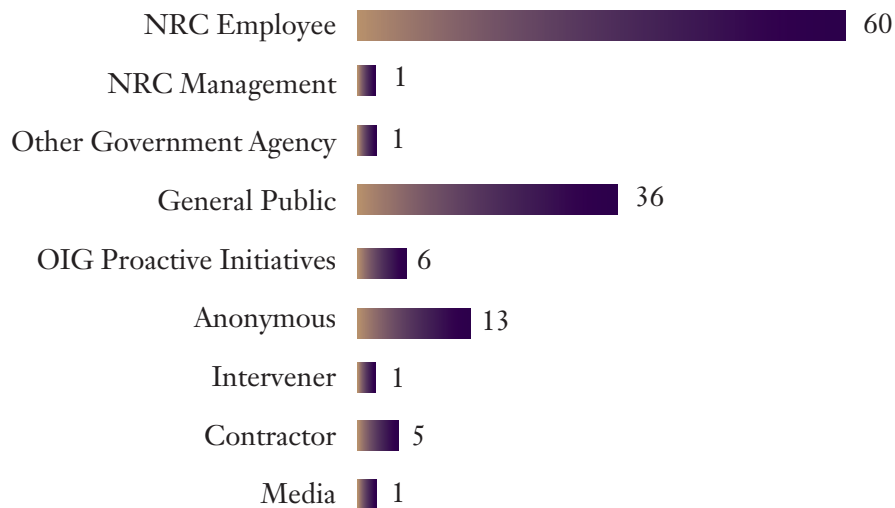
---

# SUMMARY OF NRC OIG ACCOMPLISHMENTS AT NRC

October 1, 2015, to March 31, 2016

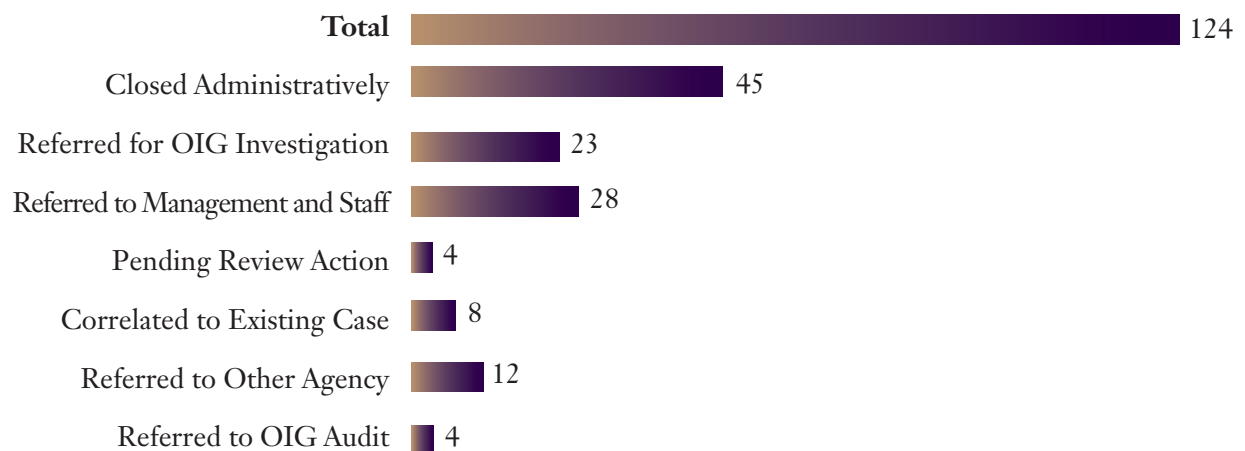
## *Investigative Statistics*

### Source of Allegations



Allegations resulting from the NRC OIG Hotline: 72 **Total: 124**

### Disposition of Allegations





## Status of Investigations

|                                                                 |   |
|-----------------------------------------------------------------|---|
| DOJ Referrals . . . . .                                         | 4 |
| DOJ Acceptance . . . . .                                        | 3 |
| DOJ Pending . . . . .                                           | 0 |
| DOJ Declinations. . . . .                                       | 1 |
| Criminal Convictions. . . . .                                   | 0 |
| Criminal Penalty Fines . . . . .                                | 0 |
| Civil Recovery. . . . .                                         | 0 |
| NRC Administrative Actions:                                     |   |
| Counseling and Letter of Reprimand. . . . .                     | 0 |
| Terminations and Resignations . . . . .                         | 0 |
| Suspensions and Demotions. . . . .                              | 0 |
| Other (Letter from Chairman Review of Policy, and ADR). . . . . | 0 |
| State Referrals. . . . .                                        | 0 |
| State Declinations. . . . .                                     | 0 |
| State Accepted. . . . .                                         | 0 |
| PFCRA Referral . . . . .                                        | 0 |
| PFCRA Acceptance. . . . .                                       | 0 |
| PFCRA Declinations . . . . .                                    | 0 |

## Summary of Investigations

| Classification of Investigations | Carryover Cases | Opened Cases | Closed Cases | Cases in Progress |
|----------------------------------|-----------------|--------------|--------------|-------------------|
| Employee Misconduct              | 9               | 7            | 7            | 9                 |
| External Fraud                   | 9               | 5            | 3            | 11                |
| False Statements                 | 2               | 0            | 1            | 1                 |
| Management Misconduct            | 8               | 5            | 2            | 11                |
| Miscellaneous                    | 5               | 1            | 2            | 4                 |
| Internal Fraud                   | 0               | 1            | 0            | 1                 |
| Proactive Initiatives            | 6               | 0            | 1            | 5                 |
| Technical Allegations            | 9               | 2            | 4            | 7                 |
| <b>Grand Total</b>               | <b>48</b>       | <b>21</b>    | <b>20</b>    | <b>49</b>         |

---

# SUMMARY OF NRC OIG ACCOMPLISHMENTS AT DNFSB

October 1, 2015, to March 31, 2016

## *Investigative Statistics*

### Source of Allegations

DNFSB Employee  1

General Public 0

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

### Disposition of Allegations

**Total**  1

Closed Administratively 0

Referred for OIG Investigation 0

Pending Review Action 0

Referred to Other Agency 0

Referred to OIG Audit 0

Correlated to existing case  1



---

## *NRC Audit Listings*

| Date       | Title                                                                                                                                                                                                 | Audit Number |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 03/07/2016 | Audit of NRC's Personal Identity Verification (PIV) Card Access System                                                                                                                                | OIG-16-A-10  |
| 02/09/2016 | Transmittal of the Independent Auditor's Report on the Summary Financial Statements                                                                                                                   | OIG-16-A-09  |
| 02/08/2016 | Audit of NRC's Operator Licensing Program for the AP1000 Power Reactor                                                                                                                                | OIG-16-A-08  |
| 01/11/2016 | Audit of NRC's Network Security Operations Center                                                                                                                                                     | OIG-16-A-07  |
| 11/30/2015 | Evaluation of NRC's Agencywide Documents Access and Management System (ADAMS) Functional and Operational Capabilities                                                                                 | OIG-16-A-06  |
| 11/17/2015 | Independent Auditors' Report on the U.S. Nuclear Regulatory Commission's Closing Package Financial Statements as of September 30, 2015 and 2014, and for the Years Then Ended dated November 17, 2015 | OIG-16-A-05  |
| 11/13/2015 | Results of the Audit of the United States Nuclear Regulatory Commission's Financial Statements for FY 2015 and 2014                                                                                   | OIG-16-A-04  |
| 11/12/2015 | Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2015                                                                              | OIG-16-A-03  |
| 10/08/2015 | Audit of NRC's Oversight of Medical Uses of Nuclear Material                                                                                                                                          | OIG-16-A-02  |
| 10/01/2015 | Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission                                                                     | OIG-16-A-01  |

---

## *DNFSB Audit Listings*

| Date       | Title                                                                                                                                       | Audit Number  |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 11/16/2015 | Results of the Audit of the Defense Nuclear Facilities Safety Board's Financial Statements for FY 2015 and 2014                             | DNFSB-16-A-04 |
| 11/12/2015 | Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2015                  | DNFSB-16-A-03 |
| 10/28/2015 | Audit of the Defense Nuclear Facilities Safety Board's Information Security Program                                                         | DNFSB-16-A-02 |
| 10/01/2015 | Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board | DNFSB-16-A-01 |

---

## **NRC Contract Audit Reports**

OIG did not receive any contract audit reports for this reporting period.

# AUDIT RESOLUTION ACTIVITIES

*TABLE I*

## OIG Reports Containing Questioned Costs<sup>2, 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                 | 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                                                          | 1                 | \$69,058                   | 0                           |
| (ii) dollar value of costs not disallowed                                                     | 0                 | 0                          | 0                           |
| D. For which no management decision had been made by the end of the reporting period          | 1                 | \$1,647,715                | 0                           |

<sup>2</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.

<sup>3</sup> These questioned costs are all attributable to NRC. DNFSB had no questioned costs.

---

*TABLE II*

**OIG Reports Issued with Recommendations  
That Funds Be Put to Better Use<sup>4, 5</sup>**

| <b>Reports</b> |                                                                                            | <b>Number of<br/>Reports</b> | <b>Dollar Value<br/>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                      | 1                            | \$160,000                        |
|                | (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.

<sup>5</sup> This data is attributable to NRC. DNFSB had no reports issued with recommendations that funds be put to better use.



---

### TABLE III

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

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

---

# ABBREVIATIONS AND ACRONYMS

|        |                                                               |
|--------|---------------------------------------------------------------|
| ACMUI  | Advisory Committee on the Medical Uses of Isotopes            |
| ADAMS  | Agencywide Documents Access and Management Systems            |
| AP1000 | Advanced Passive 1000                                         |
| CAL    | Confirmatory Action Letter                                    |
| CFR    | Code of Federal Regulations                                   |
| CIGIE  | Council of the Inspectors General on Integrity and Efficiency |
| CSRA   | Civil Service Reform Act                                      |
| DH     | Directive Handbook                                            |
| DNFSB  | U.S. Defense Nuclear Facilities Safety Board                  |
| DOE    | U.S. Department of Energy                                     |
| DOJ    | U.S. Department of Justice                                    |
| DOL    | U.S. Department of Labor                                      |
| FMFIA  | Financial Managers' Financial Integrity Act                   |
| FISMA  | Federal Information Security Management Act                   |
| FY     | fiscal year                                                   |
| IAM    | Issue Area Monitor                                            |
| IG     | Inspector General                                             |
| IPEC   | Indian Point Energy Center                                    |
| IT     | information technology                                        |
| ITISS  | information technology infrastructure support services        |
| IV&V   | independent verification and validation                       |
| MD     | Management Directive                                          |
| OI     | Office of Investigations (NRC)                                |
| OIG    | Office of the Inspector General                               |
| OMB    | Office of Management and Budget                               |
| OSC    | Office of Special Counsel                                     |
| NRC    | U.S. Nuclear Regulatory Commission                            |
| PIP    | Performance Improvement Plan                                  |
| PIV    | Personal Identification Verification                          |
| ROP    | Reactor Oversight Process                                     |
| SDP    | Significance Determination Process                            |
| SIRWT  | Safety Injection Refueling Water Tank                         |
| SLNPP  | St. Lucie Nuclear Power Plant                                 |
| SOC    | Security Operations Center                                    |
| TAR    | Technical Assistance Request                                  |
| TS     | technical specifications                                      |
| UCNI   | Unclassified Controlled Nuclear Information                   |
| WPA    | Whistleblower Protection Act                                  |

---

# REPORTING REQUIREMENTS

*The Inspector General Act of 1978, as amended (1988), specifies reporting requirements for semiannual reports. This index cross-references those requirements to the applicable pages where they are fulfilled in this report.*

| Citation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Reporting Requirements                                                                                          | Page                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---------------------|
| Section 4(a)(2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Review of Legislation and Regulations                                                                           | 7                   |
| Section 5(a)(1)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Significant Problems, Abuses, and Deficiencies                                                                  | 12–20; 29–33; 35–39 |
| Section 5(a)(2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Recommendations for Corrective Action                                                                           | 12–20; 35–39        |
| Section 5(a)(3)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Prior Significant Recommendations Not Yet Completed                                                             | 49                  |
| Section 5(a)(4)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Matters Referred to Prosecutive Authorities                                                                     | 42                  |
| Section 5(a)(5)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Information or Assistance Refused                                                                               | None                |
| Section 5(a)(6)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Listing of Audit Reports                                                                                        | 44                  |
| Section 5(a)(7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Summary of Significant Reports                                                                                  | 12–20; 29–33; 35–39 |
| Section 5(a)(8)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Audit Reports — Questioned Costs                                                                                | 47                  |
| Section 5(a)(9)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Audit Reports — Funds Put to Better Use                                                                         | 48                  |
| Section 5(a)(10)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Audit Reports Issued Before Commencement of the Reporting Period for Which No Management Decision Has Been Made | None                |
| Section 5(a)(11)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Significant Revised Management Decisions                                                                        | None                |
| Section 5(a)(12)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Significant Management Decisions With Which the OIG Disagreed                                                   | None                |
| <i>Sec. 989C. of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111-203) requires Inspectors General to include the results of any peer review conducted by another Office of Inspector General during the reporting period; or if no peer review was conducted, a statement identifying the date of the last peer review conducted by another Office of Inspector General; and a list of any peer review conducted by the Inspector General of another Office of the Inspector General during the reporting period.</i> |                                                                                                                 |                     |
| Section 989C.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Peer Review Information                                                                                         | 52                  |

---

# APPENDIX

## Peer Review Information

### *Audits*

The NRC OIG Audit Program was peer reviewed most recently by the Federal Communications Commission Office of Inspector General on September 17, 2015. NRC OIG received an external peer review rating of pass. This is the highest rating possible based on the available options of pass, pass with deficiencies, or fail.

### *Investigations*

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

## **OIG STRATEGIC GOALS**

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





## The NRC OIG Hotline

The Hotline Program provides NRC and DNFSB employees, other Government employees, licensee/utility employees, contractors, and the public with a confidential means of reporting suspicious activity concerning fraud, waste, abuse, and employee or management misconduct. Mismanagement of agency programs or danger to public health and safety may also be reported. We do not attempt to identify persons contacting the Hotline.

### What should be reported:

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

## Ways To Contact the OIG



**Call:**  
**OIG Hotline**  
**1-800-233-3497**  
**TDD: 1-800-270-2787**  
7:00 a.m. – 4:00 p.m. (EST)  
After hours, please leave a message.



**Submit:**  
Online Form  
[www.nrc.gov](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

