Semiannual Report to Congress
October 1, 2021—March 31, 2022

Office of the Inspector General
U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

THE OIG VISION

Advancing nuclear safety and security through audits, evaluations, and investigations.

THE OIG MISSION

Providing independent, objective audit and investigative oversight of the operations of the Nuclear Regulatory Commission and the Defense Nuclear Facilities Safety Board, in order to protect people and the environment.

COVER PHOTO:

North Anna Nuclear Power Station

A MESSAGE FROM THE INSPECTOR GENERAL

On behalf of the Office of the Inspector General, U.S. Nuclear Regulatory Commission and Defense Nuclear Facilities Safety Board, it is my pleasure to present this Semiannual Report to Congress, covering the period from October 1, 2021 to March 31, 2022. I continue to be grateful for the opportunity to lead this extraordinary group of managers, auditors, investigators, and support staff, and I'm extremely proud of their exceptional work.

During this reporting period, we issued eleven audit and evaluation reports, and recommended several ways to improve NRC and DNFSB safety, security, and corporate management programs. We also opened seven investigative cases and completed twelve, two of which were referred to the Department of Justice, and six of which were referred to NRC management for action.

Our reports are intended to strengthen the NRC's and the DNFSB's oversight of their myriad endeavors and reflect the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse. Summaries of the reports herein include reviews of the NRC's counterfeit, fraudulent and suspect items oversight; permanent change of station program review; financial statements evaluation; compliance with the Federal Information Security Modernization Act; compliance with the Digital Accountability and Transparency Act; top management and performance challenges facing the NRC; DNFSB compliance with the Federal Information Security Modernization Act; financial statements review; planning and implementation oversight activities process; DNFSB compliance with the Digital Accountability and Transparency Act; and, top management and performance challenges facing the DNFSB. Further, this report includes summaries of cases involving license applications handling concerns, reactor evaluation plan concerns, reasonable accommodations process issues, employee conflict of interest, falsification of inspection reports, and a special inquiry into counterfeit, fraudulent, and suspect items.

Our team dedicates their efforts to promoting the integrity, efficiency, and effectiveness of NRC and DNFSB programs and operations, and I greatly appreciate their commitment to that mission. Our success would not be possible without the collaborative efforts between my staff and those of the NRC and the DNFSB, to address OIG findings and implement corrective actions in a timely manner. I thank them for their dedication, and I look forward to continued cooperation as we work together to ensure the integrity and efficiency of agency operations.

Robert J. Feitel

Robert J. Feitel

Highlights

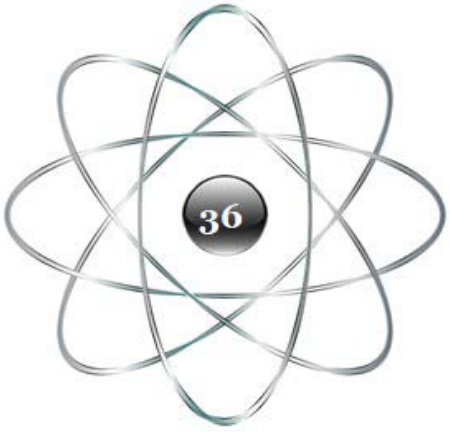
OFFICE of AUDITS

5

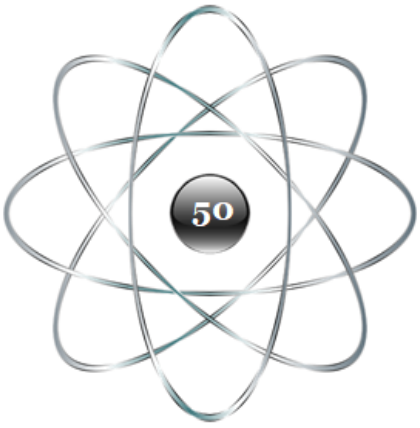
DNFSB

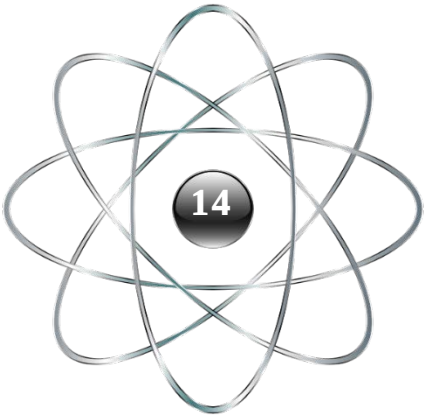
6

NRC

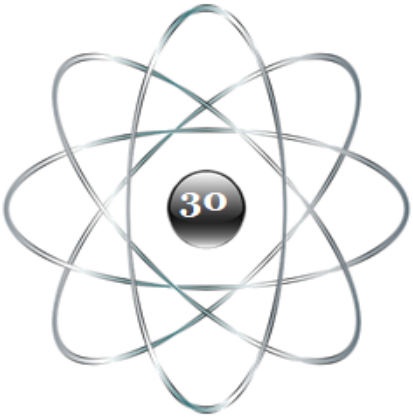


Recommendations Made





Recommendations Closed



Highlights

OFFICE of INVESTIGATIONS

1
Conviction

2
Criminal Matters Referred for Prosecution

1
Sentencing

Open Investigations

7

Closed Investigations

12

In Progress Investigations

18

CONTENTS

The NRC Headquarters Complex

HIGHLIGHTS

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

Audits

Nuclear Regulatory Commission

- The U.S. Nuclear Regulatory Commission (NRC) requires nuclear power plants to use products and services exhibiting the highest quality in agency-regulated activities. Vendors, suppliers, and nuclear power plants operators must verify the quality of items destined for safety-related functions in NRC-regulated facilities. Verification includes inspections of an item's critical physical characteristics and performance testing to provide reasonable assurance that parts will perform their intended safety functions. The Office of the Inspector General (OIG) assessed whether the NRC's oversight activities reasonably assure nuclear power reactor licensees' programs are adequately positioned to mitigate the risk of counterfeit, fraudulent, and suspect items in operating reactors, those under construction, and those completed but not yet online.

- A federal employee is eligible for subsistence and transportation allowances for permanent change of station (PCS) travel if an agency specifically authorizes relocation expenses under the Federal Travel Regulation (FTR). The NRC provides employees with the necessary guidance to relocate to a permanent official duty station and to claim reimbursement for the allowable expenses. In addition, the NRC provides the policies and procedures for the staff's use of relocation incentives. The OIG assessed whether the NRC has established and implemented an effective system of internal control over the permanent change of station program.

- The Federal Information Security Modernization Act (FISMA) was enacted in 2014 and outlined the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. Additionally, the FISMA includes provisions,

such as those requiring the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security. The OIG contracted with SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the NRC's overall information security program and practices in response to the fiscal year (FY) 2021 Inspector General FISMA Reporting Metrics.

- The Chief Financial Officers Act of 1990, as amended (CFO Act), requires the Inspector General (IG) or an independent external auditor, as determined by the IG, to annually audit the NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with Grant Thornton (GT) to conduct this annual audit. GT examined the NRC's FY 2021 Agency Financial Report, which includes financial statements for FY 2021.

- The Digital Accountability and Transparency Act of 2014 (DATA Act) was enacted in 2014 and requires federal agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury and the Office of Management and Budget (OMB). The DATA Act requires IGs to review the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality, and accuracy of this information. The OIG contracted with CliftonLarsonAllen (CLA) to conduct an independent audit of the NRC's implementation of the DATA Act.

- The Reports Consolidation Act of 2001 requires the OIG to annually update our assessment of the NRC's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. This year, the OIG identified nine areas representing challenges the NRC must address to accomplish its mission better. We have compiled this list based on our audit, evaluation, and investigative work; general knowledge of the agency's operations; and, evaluative reports of others, including the U.S. Government Accountability Office (GAO), and input from NRC management.

Defense Nuclear Facilities Safety Board

- The CFO Act requires the IG or an independent external auditor, as determined by the IG, to annually audit the Defense Nuclear Facilities Safety Board's (DNFSB) financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with GT to conduct this annual audit. GT examined the DNFSB's FY 2021 Agency Financial Report, which includes financial statements for FY 2021.

- The OIG contracted with SBG to conduct an independent evaluation of the DNFSB's overall information security program and practices to respond to the FY 2021 FISMA Reporting Metrics. The FISMA was enacted in 2014 and outlined the information security management requirements for agencies, including the requirement for an annual independent assessment by the agency IG. Additionally, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems.

- The DNFSB's day-to-day oversight of defense nuclear facilities is carried out by staff in the Office of the Technical Director (OTD). The OTD staff follow a work planning process to create an annual work plan that details activities to be carried out in the next fiscal year. The OIG assessed whether the DNFSB's planning and implementation of oversight activities are effective in helping the DNFSB accomplish its mission.

- The DATA Act was enacted in 2014 and requires federal agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury and the OMB. The DATA Act requires IGs to review the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality and accuracy of this information. The OIG contracted with CLA to conduct an independent audit of the DNFSB's implementation of the DATA Act.

- The Reports Consolidation Act of 2001 requires the OIG to annually update its assessment of the DNFSB's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. This year, the OIG identified five areas representing challenges the DNFSB must address to accomplish its mission better. We have compiled this list based on our audit, evaluation, and investigative work; general knowledge of the agency's operations; and, evaluative reports of others, including the GAO, and input from DNFSB management.

Investigations

Nuclear Regulatory Commission

During this reporting period, the OIG completed investigations on the following concerns:

- An NRC employee alleged that his supervisor retaliated against him by charging him with lack of candor when he denied raising safety concerns directly to a licensee.

- A member of the public alleged that the NRC had failed to address concerns with Seabrook Station's emergency plan.

- An NRC employee claimed his Regional Administrator and a Human Resources specialist were not following the reasonable accommodation process by not signing the acknowledgement block on his exception request regarding the COVID-19 vaccine mandate. The employee also alleged the Regional Administrator harassed him and created a chilled working environment by telling the employee he could not discuss his request with other senior managers in the region.

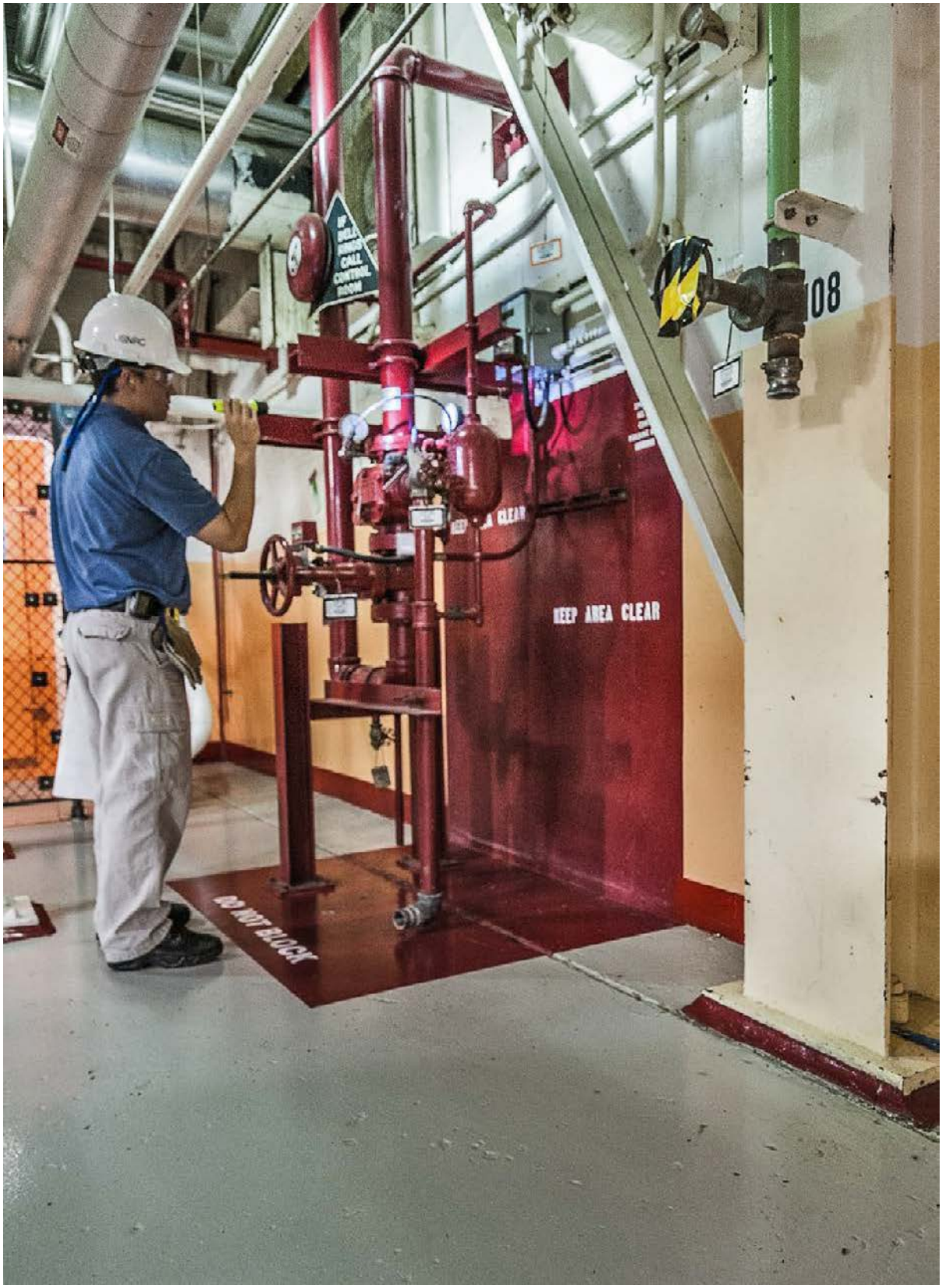
- An alleger reported that a retired NRC employee violated conflict-of-interest laws when he represented other public interest groups before the NRC with intent to influence the NRC in a license renewal proceeding involving a nuclear plant. Subsequently, an organization that represents whistleblowers alleged that the licensee unlawfully attempted to deter the retired employee from presenting evidence in the license renewal proceeding.

- Allegers reported concerns that an NRC senior resident inspector had not adequately performed the inspections documented in a quarterly inspection report.

- Allegers reported concerns that counterfeit, fraudulent, and suspect items (CFSI) are present in U.S. nuclear power plants, that the NRC has lowered the oversight standards for CFSI, and that the NRC failed to address CFSI allegations. This inquiry examined the adequacy of the NRC's oversight of CFSI in U.S. operating nuclear power plants and addressed the allegations.

Defense Nuclear Facilities Safety Board

The OIG did not close any DNFSB investigations during this reporting period.



Fire equipment inspection at Calvert Cliffs nuclear power plant

OVERVIEW OF THE NRC AND THE OIG

The NRC's Mission

The NRC began operations in 1975 as an independent agency within the executive branch with responsibility for regulating 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. The NRC's mission is to license and regulate the nation's civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. The 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** – Use of nuclear materials in medical, industrial, and academic settings, and facilities that produce nuclear fuel; and,

- **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, the NRC has the following main regulatory functions: (1) establish standards and regulations; (2) issue licenses, certificates, and permits; (3) ensure compliance with established standards and regulations; and, (4) conduct research, adjudication, and risk and performance assessments to support regulatory decisions. These regulatory functions include regulating nuclear power plants, fuel cycle facilities, and other civilian uses of radioactive materials. Civilian uses include nuclear medicine programs at hospitals, academic activities at educational institutions, research, and such industrial applications as gauges and testing equipment.

The NRC maintains a current website and a public document room at its headquarters in Rockville, Maryland; 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. It also had to provide an independent voice for economy, efficiency, and effectiveness within the federal government that would earn and maintain the trust of the American people.

In response, Congress passed the landmark legislation known as the Inspector General Act, which President Jimmy Carter signed into law in 1978. The IG Act created independent IGs, 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. 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 ensuring that thousands of wrongdoers are held accountable for their actions. The IG concept and its principles of good governance, accountability, and monetary recovery have been adopted by foreign governments as well, contributing to improved governance in many nations.

OIG Mission and Goals

The NRC OIG was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendment to the IG Act. The NRC OIG's mission is to provide independent, objective audit and investigative oversight of the operations of the Nuclear Regulatory Commission and the Defense Nuclear Facilities Safety Board, in order to protect people and the environment.

The OIG is committed to ensuring the integrity of NRC programs and operations. Developing an effective planning strategy is a critical aspect of meeting this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, the OIG developed a Strategic Plan that includes the major challenges and critical risk areas facing the NRC. The plan identifies the OIG's priorities and establishes a shared set of expectations regarding the OIG's goals and the strategies it will employ to achieve these goals. As it relates to the NRC, the OIG's Strategic Plan features three goals, which generally align with the NRC's mission and goals:

(1) Strengthen the NRC's efforts to protect public health and safety, and the environment;

(2) Strengthen the NRC's security efforts in response to an evolving threat environment; and,

(3) Increase the economy, efficiency, and effectiveness with which the NRC manages and exercises stewardship over its resources.

Inspection of construction at V.C. Summer Nuclear Power Station

OIG PROGRAMS AND ACTIVITIES

Audit Program

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

- **Survey** – An initial phase of the audit process is used to gather information on the agency's organization, programs, activities, and functions. An assessment of vulnerable areas determines whether further review is needed;

- **Fieldwork** – Auditors gather detailed information to develop findings and support conclusions and recommendations;

- **Reporting** – The auditors present the information, findings, conclusions, and recommendations that are supported by the evidence gathered during the survey and fieldwork phases. The auditors hold exit conferences with management officials to obtain their views on issues in the draft audit report and present those comments in the published audit report, as appropriate. The published audit reports include formal written comments in their entirety as an appendix; and,

- **Resolution** – Positive change results from the resolution process in which management takes action to improve operations based on the recommendations in the published audit report. Management actions are monitored until final action is taken on all recommendations. When management and the OIG cannot agree on the actions needed to correct a problem identified in an audit report, the issue can be taken to the NRC Chairman or DNFSB Chairperson for resolution.

Each October, the OIG issues an *Annual Plan* that summarizes the audits planned for the coming fiscal year. Unanticipated high-priority issues may arise that generate audits not listed in the *Annual Plan*. OIG audit staff continually monitor specific issue areas to strengthen the OIG's internal coordination and overall planning process. Under the OIG Issue Area Monitor (IAM) program, staff designated as IAMs are assigned responsibility for keeping abreast of major agency programs and activities. The broad IAM areas address nuclear reactors, nuclear materials, nuclear waste, international programs, security, information management, and financial management and administrative programs.

Investigative Program

The OIG's responsibility for detecting and preventing fraud, waste, and abuse within the NRC and the DNFSB includes investigating possible violations of criminal statutes relating to agency programs and activities, investigating misconduct by employees and contractors, interfacing with the U.S. Department of Justice on OIG-related criminal and civil matters, and coordinating investigations and other OIG initiatives with federal, state, and local investigative agencies, and other OIGs.

Investigations may be initiated as a result of allegations or referrals from private citizens; licensee employees; government 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 the NRC's mission is to protect the health and safety of the public, the OIG's Investigative Program directs much of its resources and attention to investigating allegations of NRC staff conduct that could adversely impact matters related to health and safety. These investigations may address allegations of:

- Misconduct by high-ranking NRC officials and other NRC officials, such as managers and inspectors, whose positions directly impact public health and safety;

- Failure by NRC management to ensure that health and safety matters are appropriately addressed;

- Failure by the NRC to provide sufficient information to the public and to openly seek and consider the public's input during the regulatory process;

- Conflicts of interest involving NRC employees, contractors, and licensees, including such matters as promises of future employment for favorable regulatory treatment, and the acceptance of gratuities; and,

- Fraud in the NRC's procurement programs involving contractors violating government contracting laws and rules.

The 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. The 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

Under the Inspector General Act, 5 U.S.C. App. 3, Section 4(a)(2), the OIG reviews existing and proposed legislation, regulations, policy, and implementing NRC Management Directives (MD) and DNFSB Directives, and makes recommendations to the agency concerning their impact on the economy and efficiency of its programs and operations.

Regulatory review is intended to help the agency avoid formal implementation of potentially flawed regulations or policies. The OIG does not concur or object to the agency actions reflected in the regulatory documents, but rather offers comments.

Comments provided in the regulatory review process reflect the OIG's objective analysis of the language of proposed statutes, regulations, directives, and policies. The OIG review is structured to identify vulnerabilities and offer additional or alternative choices. As part of its reviews, the OIG focuses on ensuring that agency policy and procedures do not negatively affect the OIG's operations or independence.

From October 1, 2021 to March 31, 2022, the OIG reviewed a variety of regulatory documents. In its reviews, the OIG remained cognizant of how the proposed rules or policies could affect the OIG's functioning or independence. The OIG also considered whether the rules or policies could significantly affect NRC or DNFSB operations or be of high interest to NRC or DNFSB staff and stakeholders. In conducting its reviews, the OIG applied its knowledge and awareness of underlying trends and overarching developments at the agencies and in the areas they regulate.

For the period covered by this Semiannual Report, the OIG did not identify any issues that would significantly compromise our independence or conflict with our audit or investigatory functions. We did, however, identify certain proposed staff polices that might affect, to some extent the work of the OIG. In these cases, the OIG proposed edits or changes that would mitigate the impacts and requested responses from the staff. Agency staff either accepted the OIG's proposals or offered a well-supported explanation as to why the proposed changes were not accepted. These reviews are described in further detail below.

NRC Management Directives

- MD 4.7, Budget Formulation, which describes how the NRC prepares and submits its annual budgets to the President and Congress. The OIG reviewed revisions to this MD to ensure they accurately described the budget-formulation process and the role of the OIG, which is responsible for preparing its own budget. The OIG offered substantive comments to clarify certain provisions in the MD, better explain how the MD applies to the OIG, and ensure a list of relevant legal authorities included the Inspector General Act.
- MD 9.2, Organization and Functions, Office of the Inspector General, which outlines the roles and responsibilities of personnel in the OIG. This periodic update to the MD, initiated by the OIG, clarified the responsibilities of certain personnel in the OIG. This revision also updated certain position titles, citations, and references in the MD. The OIG sought input from the NRC's Office of the General Counsel and its Office of the Chief Human Capital Officer, which the OIG incorporated in the MD revisions.
- MD 12.3, NRC Personnel Security Program, which provides guidance on the NRC's implementation of its program as it pertains to site access, information security, and drug testing. The OIG offered substantive comments in several areas, including a recommendation that language be added clarifying that employees have an obligation to promptly report allegations of suspected wrongdoing to either the OIG or their supervisors. The OIG also recommended adding language clarifying that certain provisions in the MD applied not only to classified information, but also to safeguards information (information authorized to be protected under section 147 of the Atomic Energy Act). In addition, the OIG recommended updating various references or titles in the MD. The NRC incorporated the OIG's recommendations in the revised MD.

DNFSB Directives

Directive D-1.1, "Directives Program." This directive provides guidance on reporting suspected wrongdoing to the OIG and describes management responsibilities in handling OIG investigative referrals. The OIG provided a limited number of comments on the revision to this Directive. The comments, which were incorporated in the Directive revision, were intended to clarify the roles of certain OIG personnel, the

steps the OIG will take to preserve the anonymity of allegers, and the scope of the OIG's investigative authority.

Other OIG Activities

NRC OIG Employee Receives Prestigious Inspector General's Meritorious Service Award

Communications Officer Christine V. Arroyo receives the Inspector General's Meritorious Service Award.

The Inspector General recognizes with appreciation the valuable contributions made by all OIG employees over the course of their OIG career. In March 2022, Inspector General Feitel presented Christine V. Arroyo, Communications Officer, with the prestigious Inspector General's Meritorious Service Award, in recognition of her meritorious service and achievement in advancing the objectives of the OIG.


THE
INSPECTOR GENERAL'S
MERITORIOUS SERVICE AWARD

Presented To
CHRISTINE V. ARROYO
COMMUNICATIONS OFFICER
OFFICE OF THE INSPECTOR GENERAL
U.S. NUCLEAR REGULATORY COMMISSION &
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

IN GRATEFUL RECOGNITION OF YOUR MERITORIOUS SERVICE AND ACHIEVEMENT IN ADVANCING THE OBJECTIVES OF THE OFFICE OF THE INSPECTOR GENERAL

YOU CONTINUE TO DEMONSTRATE EXCEPTIONAL PROFESSIONALISM, BOLD INITIATIVE, AND SELFLESS DEVOTION TO OUR OVERSIGHT MISSION AS YOU CONSISTENTLY UPHOLD THE HIGHEST TRADITIONS OF THE OFFICE OF THE INSPECTOR GENERAL

MARCH 17, 2022

Ms. Arroyo enthusiastically agreed to assume the newly created role of Communications Officer, and has brought a great deal of innovation, and sound judgment to that position. Upon assuming the position of Communications Officer, Ms. Arroyo, in consultation with the Inspector General and pertinent OIG staff, immediately took the initiative to implement a wholesale rebranding of the Office of the Inspector General, highlighting the Office's mission, work products, expertise, and independence.

Newly Appointed OIG General Counsel

Michael Clark, Esquire joined the OIG in December 2021 as General Counsel to the Inspector General.

Mr. Clark has worked for the NRC for over 15 years, serving in both supervisory and non-supervisory roles in the Office of the General Counsel. Mr. Clark's NRC background includes extensive experience in administrative law, ethics, civil enforcement actions, and administrative litigation. Mr. Clark comes to the OIG following a rotation as a legal advisor in the office of Chairman Christopher T. Hanson.

Before joining the NRC, Mr. Clark worked as an attorney for both the Occupational Safety and Health Review Commission and the Social Security Administration. He has also served as a Special Assistant United States Attorney for the U.S. Attorney's Office for the District of Columbia.

Mr. Clark holds a Bachelor of Arts degree in political science from the University of Rochester and a Juris Doctor degree from the University of Michigan Law School.

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

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in FY 2022*   ***(As identified by the Inspector General)***
Challenge 1: *Ensuring safety while transforming into a modern, risk-informed regulator.*
Challenge 2: *Regulatory oversight of the decommissioning process and the management of decommissioning trust funds.*
Challenge 3: *Using the COVID-19 lessons learned to strengthen NRC readiness to respond to future mission-affecting disruptions.*
Challenge 4: *Readiness to license and regulate new technologies in reactor design, fuels, and plant controls, and maintaining the integrity of the associated intellectual property.*
Challenge 5: *Ensuring the safe and effective acquisition, management, and protection of information technology and data.*
Challenge 6: *Strategic workforce planning during transformation and industry change.*
Challenge 7: *Oversight of materials, waste, and the National Materials Program.*
Challenge 8: *Management and transparency of financial and acquisitions operations.*
Challenge 9: *NRC readiness to address cyber threats to critical national infrastructure sectors impacting the NRC's public health and safety mission and/or NRC licensees.*

** For more information on these challenges, see OIG-22-A-01, "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC." https://nrcoig.oversight.gov/top-management-challenges*

NRC AUDITS

Audit Summaries

Audit of the NRC's Oversight of Counterfeit, Fraudulent, and Suspect Items at Nuclear Power Reactors

OIG Strategic Goal: Safety

Counterfeit, fraudulent, and suspect items (CFSI) are generally defined, respectively, as items that are (1) intentionally manufactured or altered to imitate legitimate products without the legal right to do so; (2) intentionally misrepresented with intent to deceive; and, (3) suspected of being, but not yet verified to be, counterfeit or fraudulent.

The NRC requires nuclear power plants to use products and services exhibiting the highest quality in agency-regulated activities. Vendors, suppliers, and nuclear power plant operators must verify the quality of items destined for safety-related functions in NRC-regulated activities. Verification includes inspections of each item's critical physical characteristics and performance testing to provide reasonable assurance that parts will perform their intended safety functions.

The objective of this audit was to assess whether the NRC's oversight activities reasonably assure nuclear power reactor licensees' programs are adequately positioned to mitigate the risk of CFSI in operating reactors, those under construction, and those completed but not yet online.

Audit Results:

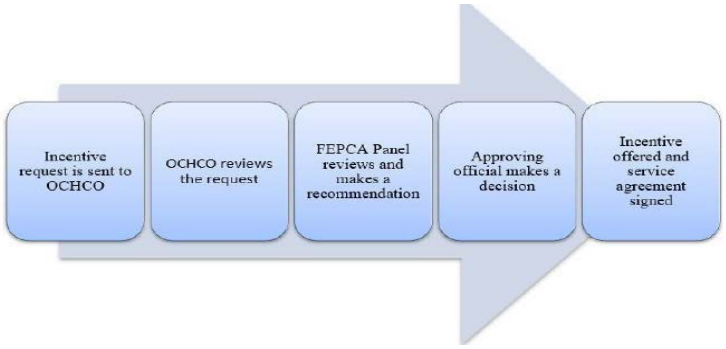
The OIG found that the NRC should improve its oversight of CFSI by clarifying and communicating how the agency collects, assesses, and disseminates information regarding CFSI, and by improving staff awareness of CFSI and its applicability to reactor inspections.

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

Audit of the NRC's Permanent Change of Station Program

OIG Strategic Goal: Corporate Management

A federal employee is eligible for subsistence and transportation allowances for PCS travel if an agency specifically authorizes relocation expenses under the FTR. In addition to subsistence and transportation allowances for PCS travel, 5 C.F.R. Section 575.206 establishes that an authorized agency official retains sole and exclusive discretion to approve a relocation incentive for an employee hired for a position that was difficult to fill.



Steps of Relocation Incentive.

The Office of the Chief Financial Officer provides NRC employees with the necessary guidance to relocate to a permanent official duty station, and to claim reimbursement for the allowable expenses. The Office of the Chief Human Capital Officer (OCHCO) provides the policies and procedures for the NRC's use of relocation incentives.

The audit objective was to determine whether the NRC has established and implemented an effective system of internal control over the permanent change of station program.

Audit Results:

The OIG found that the NRC has established and implemented an adequate system of internal control over the permanent change of station program. However, opportunities for improving its effectiveness exist. Specifically, the NRC's policies and procedures for relocation allowances and incentives need to be updated to reflect current federal guidance.

(Addresses Management and Performance Challenge #8)

Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021

OIG Strategic Goal: Corporate Management

The FISMA outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General.

Additionally, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security.

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

The OIG contracted with SBG to conduct an independent evaluation of the NRC's overall information security program and practices in response to the FY 2021 IG FISMA Reporting Metrics.

The evaluation objective was to evaluate the effectiveness of the information security policies, procedures, and practices at the NRC.

Evaluation Results:

The NRC's information security program was "Effective" according to Department of Homeland Security criteria specified in the FY 2021 IG FISMA Reporting Metrics. While effective, the OIG identified areas that need to be improved to optimize the NRC's information security program.

(Addresses Management and Performance Challenge #5)

Results of the Audit of the NRC's Financial Statements for Fiscal Year 2021

OIG Strategic Goal: Corporate Management

The CFO Act requires the IG or an independent external auditor, as determined by the IG, to annually audit the NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with GT to conduct this annual audit. GT examined the NRC's FY 2021 Agency Financial Report, which includes financial statements for FY 2021.

The objective of a financial statement audit is to determine whether the audited entity's financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation.

Audit Results:

In GT's opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the NRC as of September 30, 2021, and its net cost, changes in net position, and budgetary resources for the year then ended, in accordance with accounting principles generally accepted in the United States. Also, in GT's opinion, because of the effect of a material weakness in internal controls, the NRC had not maintained effective internal control over financial reporting as of September 30, 2021.

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Corporate Management

The DATA Act requires federal agencies to report financial and payment data in accordance with data standards established by the U.S. Department of Treasury and the OMB. The data reported is displayed on a public website. In addition, the DATA Act requires IGs to review the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality, and accuracy of this information. The OIG contracted with CLA to conduct an independent audit of the NRC's implementation of the DATA Act.

The audit objectives were to assess (1) the completeness, accuracy, timeliness, and quality of the third quarter FY 2020 financial and award data submitted for publication on USASpending.gov; and, (2) the NRC's implementation and use of the government-wide financial data standards established by the OMB and the U.S. Department of the Treasury.

Audit Results:

CLA found that the NRC's third quarter FY 2020 submission was generally complete, accurate, and timely. CLA also determined that the NRC's data were of excellent quality overall.

(Addresses Management and Performance Challenge #8)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC in Fiscal Year 2021

OIG Strategic Goal: Safety, Security, and Corporate Management

The Reports Consolidation Act of 2001 requires the IG to annually update its assessment of the NRC's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. In this report, we summarized what we considered to be the most critical management and performance challenges facing to the NRC, and we assessed the agency's progress in addressing those challenges. Congress left the determination and threshold of what constitutes a most serious management and performance challenge to the Inspector General's discretion. We identified management challenges as those that meet at least one of the following criteria:

(1) The issue involved an operation critical to the NRC mission or an NRC strategic goal;
(2) There was a risk of fraud, waste, or abuse of NRC or other government assets;
(3) The issue involved strategic alliances with other agencies, the OMB, the Administration, Congress, or the public; and,
(4) The issue involved the risk of the NRC not carrying out a legal or regulatory requirement.

This year, we identified nine areas representing challenges the NRC must address to better accomplish its mission. We have compiled this list based on our audit, evaluation, and investigative work; general knowledge of the agency's operations; and, the evaluative reports of others, including the GAO, and input from NRC management.

(Addresses Management and Performance Challenges #1-9)

Audits in Progress

Audit of the NRC's Information Technology Services and Support

OIG Strategic Goal: Security

The NRC offers various information technology (IT) services and support to employees. These services are acquired under the Global Infrastructure and Development Acquisition (GLINDA) initiative/contract. Commencing in June 2017, GLINDA is a blanket purchase agreement (BPA) with six awardees with a total of 11 BPA calls issued against them for various Information Technology (IT) services and support. The total obligated dollar value of all BPA calls under GLINDA is approximately $5,337,586.

The NRC obtained funds from the Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act, to use on IT services and support for mandatory telework as a result of the COVID-19 pandemic. It is essential to monitor these funds to ensure they are being spent effectively in helping employees meet the agency's mission.

The audit objective is to determine if the NRC's IT services and support are efficient and effective in meeting the agency's current and future IT needs.

(Addresses Management and Performance Challenge #8)

Audit of the NRC's Strategic Workforce Planning Process

OIG Strategic Goal: Corporate Management

Strategic workforce planning (SWP) addresses two critical needs: (1) aligning an organization's human capital program with its current and emerging mission and programmatic goals, and (2) developing long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals. Strategic workforce planning is critical to the NRC because it will help maintain focus on longer-term workforce development and accomplish organizational goals in a period of agency transformation and industry change.

The NRC's enhanced SWP is a structured, data-driven process. The SWP process develops short- and long-term strategies and action plans that enable the NRC to recruit, retain, and develop a skilled and diverse workforce with the competencies and agility to address emerging needs and workload fluctuations. The SWP process takes place on an annual cycle to develop strategies to address workforce needs in a budget execution year +5.

The audit objective is to assess the effectiveness of the NRC's Strategic Workforce Planning process.

(Addresses Management and Performance Challenge #6)

Audit of the NRC's Drop-In Meeting Policies and Procedures

OIG Strategic Goal: Safety

External stakeholders have expressed concern about the frequency of senior agency management interactions with nuclear power industry representatives, some of which coincide with regulatory decisions such as backfit appeal. The NRC's policies require staff to avoid discussing specific details of regulatory matters with industry representatives in non-public interactions, although staff are permitted to discuss general information pertaining to agency activities.

The audit objective is to determine whether NRC policies and procedures for non-public interactions with industry stakeholders are adequate to prevent compromise of the independence of agency staff or the appearance of conflicts of interest.

(Addresses Management Performance Challenge #1)

Audit of the NRC's Internal Controls of Materials Exports

OIG Strategic Goal: Safety

The regulations in 10 C.F.R. Part 110, Import and Export of Nuclear Equipment and Material, prescribe licensing, enforcement, and rulemaking procedures and criteria, under the Atomic Energy Act, for

the export of nuclear equipment and material. The NRC's Office of International Programs (OIP) provides overall coordination for the NRC's international activities and develops and implements programs to carry out policies in the international arena, including export and import licensing responsibilities. In addition, the OIP establishes and maintains working relationships with regulators in individual countries and international nuclear organizations, as well as other involved U.S. government agencies.

The OIP also participates in international activities including International Atomic Energy Agency coordination, bilateral discussions with foreign nations on items of interest, and import and export notifications on nuclear materials and special nuclear materials transfers. Additionally, in conjunction with the office of Nuclear Security and Incident Response (NSIR), the OIP conducts physical protection and non-proliferation reviews of export license applications and foreign technical assistance requests.

The audit objective is to assess the effectiveness of the NRC's management controls of materials exports licensing.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Process for Licensing Emerging Medical Technologies

OIG Strategic Goal: Safety

Subpart K of 10 C.F.R Part 35 prescribes standards for licensing a new medical use of byproduct material or radiation from byproduct material (i.e., an emerging medical technology) that is not covered by other provisions in Part 35. When licensing emerging medical technologies, the Office of Nuclear Material Safety and Safeguards (NMSS) staff coordinate within the NRC to determine whether the emerging technology is already addressed in the regulations in 10 C.F.R Part 35, Subparts D through H. If the emerging medical technology is not specifically addressed in these subparts, the staff develops licensing guidance describing an acceptable approach for meeting NRC regulations.

In recent years, NMSS staff have issued specific licensing guidance and made determinations for 11 emerging medical technologies under Part 35. Due to the growth in medical applications of radioisotopes and advancements in medical technologies for use in diagnosis, therapy, and medical research, it is anticipated that the number of emerging medical technologies licensed by the NRC will increase. Approximately 15 more technologies are anticipated to be reviewed by the end of fiscal year 2023.

The audit objective is to determine the NRC's efficiency in licensing the use of emerging medical technologies, including developing technology specific guidance for licensing the use of emerging medical technologies covered under 10 C.F.R. 35 Subpart K.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Fiscal Year 2021 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

The Payment Integrity Information Act of 2019 (PIIA) requires each agency to estimate its improper payments annually. In addition, the PIIA requires federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments.

The audit objective is to assess the NRC's compliance with the PIIA Act and report any material weaknesses in internal control.

(Addresses Management and Performance Challenge #8)

Cooling tower at Limerick Nuclear Power Plant ***Photo courtesy of Exelon Corp.***

NRC INVESTIGATIONS

Investigative Summaries

Concerns Pertaining to the NRC's Handling of a License Application

OIG Strategic Goal: **Safety**

Allegation:
We received an allegation from an NRC employee that his supervisor retaliated against him by charging him with lack of candor when he denied raising safety concerns directly to a licensee.

Background:
The employee felt that concerns he raised with NRC leadership were not being addressed. The employee reached out to the licensee directly to voice his concerns, which violated NRC policy. Licensee representatives informed the NRC of the employee's contact. The employee's supervisor reviewed and verified the alleged contact and questioned the employee about it.

While we did not investigate the retaliation allegation because the employee chose to pursue the matter with the Office of Special Counsel, we did investigate the validity of the agency's review into the employee's alleged contact with the licensee and the lack of candor charge.

Investigative Results:
We verified that the supervisor did review the employee's contact with the licensee in accordance with NRC MD 10.99, Disciplinary and Adverse Actions, having consulted with the OCHCO and the OGC throughout the review. The supervisor also obtained emails and conducted external interviews, which supported a conclusion that the employee had violated NRC policy.

We also found, however, inconsistent administrative actions for comparable violations involving other NRC employees with similar alleged misconduct (lack of candor), and that the NRC does not have a table of penalties to assist NRC managers who are faced with suspension decisions for employee misconduct. We identified that

there are differences of opinion about implementing a table of penalties, even though an NRC senior manager recommended that the agency develop such administrative discipline support guidance and training. The senior manager suggested that such support would assist working supervisors who, if inexperienced with handling misconduct by employees, are tasked with proposing suspension in such situations.

Impact:
We requested the Office of the Executive Director for Operations to respond regarding what actions were taken to address the lack of administrative guidance for disciplining employees and to confirm the review of policies and procedures on this issue.

(Addresses Management and Performance Challenge #4)

Concerns Over the Adequacy of the Evacuation Plan for Seabrook Station

OIG Strategic Goal: Safety

Allegation:
The OIG received an allegation that the NRC had failed to address concerns with Seabrook Station's emergency evacuation plan. Specifically, the alleger stated that in the summer months, it would be impossible to evacuate within the 10-mile radius of the plant because of the increased population of the Hampton Beach, New Hampshire, area. The alleger said, "There is no way to implement Seabrook Station's Evacuation Plan safely and timely in the event of a nuclear disaster." Local government officials also expressed similar concerns to us.

Investigative Results:
The OIG investigation determined that the staff followed NRC policy, and that Seabrook Station's emergency plan aligns with relevant regulations, and is updated regularly. The OIG found that the NRC did address the alleger's concern regarding Seabrook's emergency plan for the Hampton Beach, New Hampshire, area during the summer months and does have policies in place to ensure the safety of the station. For example, the NRC wrote the alleger numerous letters that detailed specific activities performed by NRC inspectors during previous biennial emergency preparedness inspections, and the NRC's Region I Office, which is responsible for the geographic area that includes

Seabrook, and also communicated with Massachusetts state officials regarding the alleger's concern.

Impact:
As a result of our investigation, Region I management has made commitments that highlight the importance of reviewing the Seabrook evacuation plan in response to public concerns regarding the ability to evacuate the area during the summer season. Region I committed to sampling the Hampton Beach, New Hampshire, and Amesbury, Massachusetts, areas for potential changes in the emergency planning zone populations during the next planned inspection, which is scheduled for August 2023. The region also committed to soliciting questions on emergency preparedness from state and local officials and the public, requesting support as appropriate from the Federal Emergency Management Agency, and answering those questions during its Seabrook Annual Assessment meeting, tentatively planned for Spring 2022.

(Addresses Management and Performance Challenge #1)

Issue Regarding COVID-19 Reasonable Accommodations Process

OIG Strategic Goal: Corporate Management

Allegation:
We initiated this investigation based on information provided by an NRC employee who claimed his Regional Administrator and the agency's Reasonable Accommodation Coordinator (RAC) were not following the reasonable accommodation process because they did not sign the acknowledgement block on NRC Form 726, Confirmation of Request for Reasonable Accommodation, that the employee submitted as part of his religious exception package to the COVID-19 vaccine mandate. The employee also alleged that the Regional Administrator harassed and intimidated him during a teleconference, and that the Regional Administrator created a chilled working environment by telling the employee he could not discuss his request for a religious exception with other senior managers in the region.

Investigative Results:
The OIG did not substantiate violations of the NRC's reasonable accommodation procedures because those procedures do not require

the RAC or any designee to sign Form 726; they only require that he or she acknowledge the request. To fulfill that acknowledgement requirement, the RAC emailed the employee on October 7, 2021, acknowledging receipt of his religious exception request to the COVID-19 vaccine mandate. On October 8, 2021, the employee was made aware the NRC would soon be issuing an NRC vaccination exception form soon. On November 9, 2021, an announcement was sent to all NRC employees regarding the new NRC Form 799, Request for a Religious Exception to the COVID-19 Vaccination Requirement, instructing exception requestors to submit as soon as possible.

We also did not substantiate violations of the NRC's Anti-Harassment Policy. The NRC's Anti-Harassment Policy states harassment is behavior that reasonably could be considered to affect the work environment adversely, and the policy did not consider all rude, uncivil, or disrespectful behavior in the workplace to be harassing conduct. There was no evidence to suggest that the regional administrator's conduct regarding this issue adversely affected the work environment.

We also found that the employee was able to communicate with another regional senior manager about this issue in a timely manner, and that senior manager also passed along the complaint to the OIG. Regarding the chilled work environment, the NRC's Allegation Manual states that a definitive conclusion cannot be made related to a concern from one individual that he/she was chilled. The only response to a single individual's assertion of a chilling effect is to evaluate the occurrence and determine if a reasonable person would find the occurrence to be chilling in nature. The OIG analyzed all the information discovered during this investigation and determined that a reasonable person would not find the occurrence to be chilling.

(Addresses Management and Performance Challenge #3)

Alleged Conflict of Interest by a Former NRC Employee

OIG Strategic Goal: Safety

Allegation:

We investigated an allegation that a retired NRC employee violated conflict of interest laws when he represented other public interest groups before the NRC with intent to influence the NRC in a license renewal proceeding at a nuclear plant. Subsequently, an organization

that represents whistleblowers alleged that the licensee unlawfully attempted to deter the retired NRC employee from presenting evidence in the license renewal proceeding.

Investigative Results:

The OIG found that neither the retired employee nor the licensee violated any regulations. The same month the subject employee retired, the licensee applied to the NRC for subsequent license renewal, and two public interest groups filed a hearing request challenging the licensee's application for subsequent license renewal over concerns of risk posed by a hypothetical failure of a dam nearby the plant. Attached to the petition was a declaration by the retired employee stating that while he was an employee of the NRC, he conducted risk analysis and reviews that support the potential risk to the plant posed by a hypothetical failure of the dam. On October 4, 2021, the Chief Judge of the Atomic Safety and Licensing Board Panel established a three-judge Board to adjudicate issues related to the groups' hearing request, and on October 22, 2021, the licensee and the NRC staff filed separate responses opposing the hearing request.

It was alleged the retired employee violated 18 U.S.C. § 207(a)(1) and MD 7.12 by preparing the declaration with the knowledge and intent to influence the NRC on behalf of the groups. Separately, the OIG received a whistleblower complaint on behalf of the retired employee, asserting he is protected from the alleged ethics violation by the Whistleblower Protection Act (WPA) at 5 U.S.C. 2302(b)(8)-(9). It also alleged the licensee unlawfully tried to deter the retired employee from giving evidence (the declaration) in violation of the WPA and 18 U.S.C. § 1512(d)(4) when the licensee petitioned the Board to deny the hearing request and when it alleged the conflict of interest.

We did not identify any information that would substantiate that the retired employee or the licensee violated applicable statutes or policy. Additionally, we referred our findings to the U.S. Attorney's Office, District of Maryland, Southern Division, which declined prosecution of all alleged violations.

(Addresses Management and Performance Challenge #1)

Falsification of Inspection Reports by Resident Inspector

OIG Strategic Goal: Safety

Allegation:
We received information that Gregory Croon, a former NRC Senior Resident inspector at the North Anna Power Station, had not adequately performed the inspections documented in a quarterly inspection report, and had lied about his inspections.

Investigative Results:
Our investigation revealed the following three findings:

- Croon falsified at least three 2017 quarterly inspection reports, claiming to have conducted at least five inspections of components that no inspector conducted;
- Croon's falsification of inspection reports caused the NRC to incorrectly report to the public that it completed its baseline inspection program for 2017; and,
- NRC management failed to address its own significant concerns regarding Croon's performance and conduct once he requested and received a medical accommodation for a transfer to a new assignment. This enabled Croon to report to a new management team that had no knowledge of the previous team's performance or conduct concerns.

In addition, we found the NRC lacks several policy controls that could help NRC management maintain visibility of resident offices, allow for greater transparency by updating and creating records retention policies and using digital signatures for concurrence, and by adding 18 U.S.C. § 1001, Statements or entries generally, certification language to concurrence pages.

Impact:
On December 13, 2021, Croon pleaded guilty in the United States District Court for the Western District of Virginia to one count of a violation of 18 U.S.C. § 1001 before the Honorable Norman K. Moon, who sentenced Croon on March 7, 2022, to 1 year of probation and a $100 special assessment.

(Addresses Management and Performance Challenge #1)

Special Inquiry into Counterfeit, Fraudulent, and Suspect Items in Operating Nuclear Power Plants

OIG Strategic Goal: Safety

Allegation:
We initiated this inquiry in response to information from allegers who were concerned that counterfeit, fraudulent, and suspect items (CFSI) are present in U.S. nuclear power plants; that the NRC has lowered the oversight standards for CFSI; and that the NRC failed to address CFSI allegations.

Concurrently with this investigation, the OIG completed an audit (OIG-22-A-06, Audit of the Nuclear Regulatory Commission's Oversight of Counterfeit, Fraudulent, and Suspect Items at Nuclear Power Reactors) that assessed whether the NRC's oversight activities reasonably assure nuclear power reactor licensees' programs can mitigate the risk of CFSI in operating reactors, those under construction, and those completed but not yet online. The audit found the NRC should improve its oversight of CFSI by clarifying and communicating how the agency collects, assesses, and disseminates information regarding CFSI, and by improving staff awareness of CFSI and its applicability to inspections.

This inquiry examined the adequacy of the NRC's oversight of CFSI in U.S. operating nuclear power plants and addressed the allegations.

Investigative Results:
We found that CFSI are present in operating plants. We sampled a nuclear power plant in each of the NRC's four regions and found data to support that CFSI are being used in a plant in Region III. In addition, a well-placed NRC principal told us about two CFSI component failures at Region I plants that the licensee determined to be CFSI. The OIG's audit report also revealed that CFSI are present at operating nuclear plants.

Although we are aware that the NRC staff does not have a direct role in identifying CFSI and preventing their introduction into a plant, the extent of CFSI in operating plants is unknown because the NRC does not usually require licensees to track CFSI unless a situation rises to the level of being a significant condition adverse to quality or a reportable issue under 10 C.F.R. Part 21, Reporting of Defects and

Noncompliance (Part 21). We also learned that CFSI are not specifically tracked in regional corrective action programs, and if done at all, tracking is voluntary, and methods and data quality vary among licensees.

We did not substantiate that the NRC has lowered CFSI standards, but found several examples that could potentially give such an appearance, including lack of inspection violations issued, a downward trend in Part 21 reports, and termination of a Part 21 rulemaking in 2016 that addressed CFSI oversight concerns identified by an NRC working group. Although some third-party organizations reported fewer than 10 potential CFSI cases since 2016, this investigation revealed that the CFSI total could be greater. We found that U.S. Department of Energy staff identified more than 100 incidents involving CFSI in FY 2021 alone, including 5 incidents involving safety-significant components in its nuclear facilities. Additionally, as recently as 2019, the International Atomic Energy Agency published a report regarding its concerns about CFSI in nuclear power plants worldwide.

Although the NRC's Allegation Manual includes provisions for handling counterfeit/fraudulent parts, we found that the NRC did not investigate or pursue any substantive actions regarding an alleger's concerns about the presence of CFSI, nor did the NRC process any of the information provided by the alleger over the last 10 years through its Allegation Review Boards. In addition, the NRC's publications about the allegation process omit information regarding non-allegations, which is how this alleger's concerns were classified, and could be construed as misleading to the public.

Agency Response:
We requested the NRC Chairman to confirm the agency's review of applicable policies and procedures and notify the OIG of what action(s), if any, would be taken based on the results of this inquiry.

Impact:
This special inquiry generated media and congressional attention.

(Addresses Management and Performance Challenge #1)

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created the Defense Nuclear Facilities Safety Board (DNFSB) as an independent agency within the executive branch to identify the nature and consequences of potential threats to public health and safety involving the U.S. Department of Energy's (DOE) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. The DNFSB is the only independent technical oversight body for the nation's defense nuclear facilities. The DNFSB is composed of experts in the field of nuclear safety with demonstrated competence and knowledge relevant to its independent investigative and oversight functions.

The Consolidated Appropriations Act of 2014 provided that, notwithstanding any other provision of law, the Inspector General of the NRC was authorized in 2014, and subsequent years, to exercise the same authorities with respect to the DNFSB, as determined by the Inspector General of the NRC, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the NRC.

DNFSB MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in FY 2021*   ***(As identified by the Inspector General)***
Challenge 1: *Managing a productive organizational culture and climate.*
Challenge 2: *Ensuring the safe and effective acquisition and management of mission-specific infrastructure, including cyber, physical, and personnel security, and data.*
Challenge 3: *Ensuring a systematic safety focus in the DNFSB's technical oversight and reviews.*
Challenge 4: *Using the COVID-19 lessons learned to strengthen the DNFSB's readiness to respond to future mission-affecting disruptions.*
Challenge 5: *Managing the DNFSB's efforts to elevate its visibility and influence and to assess and improve its relationship with the DOE.*

** For more information on the challenges, see DNFSB-22-A-01, "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB"* https://nrcoig.oversight.gov/top-management-challenges

DNFSB AUDITS

Audit Summaries

Audit of the DNFSB's Fiscal Year 2021 Financial Statements

OIG Strategic Goal: Corporate Management

The CFO Act requires the IG or an independent external auditor, as determined by the IG, to annually audit the DNFSB's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with GT to conduct this annual audit. GT examined the DNFSB's FY 2021 Agency Financial Report, which includes financial statements for FY 2021.

The objective of a financial statement audit is to determine whether the audited entity's financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessments of the accounting principles used and significant estimates made, by management, as well as evaluating the overall financial statement presentation

Audit Results:

In GT's opinion, the financial statements present fairly, in all material respects, the financial position of the DNFSB, as of September 30, 2021, and its net cost, changes in net position, and budgetary resources for the year then ended, in accordance with accounting principles generally accepted in the United States. In addition, in GT's opinion, because of the effect of a material weakness, GT identified deficiencies in the agency's internal control over financial reporting.

(Addresses Management and Performance Challenge #2)

Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2021

OIG Strategic Goal: Corporate Management

The FISMA outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agencies' Inspectors General. In addition, the FISMA includes provisions such as those requiring the development of minimum standards for agency systems, which are aimed at further strengthening the security of federal government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and develop strategies and best practices for improving information security.

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

The evaluation objective was to conduct an independent assessment of the DNFSB's implementation of the FISMA for fiscal year 2021.

Evaluation Results:

While the DNFSB established an effective agencywide information security program and practices, we identified weaknesses that may impact the agency's ability to adequately protect the DNFSB's systems and information.

(Addresses Management and Performance Challenge #2)

Audit of the DNFSB's Process for Planning and Implementing Oversight Activities

OIG Strategic Goal: Safety

The DNFSB is led by presidentially appointed Board members. Oversight is carried out by staff in the Office of the Technical Director (OTD). The OTD staff follows a work planning process to create an annual work plan that details activities to be carried out in the next fiscal year. The work plan is carefully developed based on the Board's strategic direction and staff input. The specific activities that will be completed are also determined based on the availability and expertise of current staff.

The audit objective was to determine whether the DNFSB's planning and implementation of oversight activities are effective in helping the DNFSB accomplish its mission.

Audit Results:

The OIG found that the DNFSB's planning and implementation of oversight activities are effective in helping the DNFSB accomplish its mission. However, opportunities exist for improvement with regard to the Board providing more clear and specific strategic direction during the early phases of work planning, as well as addressing subject matter expert areas that lack depth. Staff need more clear and specific strategic direction from the Board. Management should internally communicate the necessary quality information to achieve the entity's objectives; moreover, work planning direction from the Board is generic and could be timelier. As a result, reviews may not be aligned with the Board's priorities, and may cause interruptions during work plan execution.

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

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

OIG Strategic Goal: Corporate Management

The DATA Act requires federal agencies to report financial and award data in accordance with the established government-wide financial data standards. In May 2015, the OMB and the Department of the Treasury published 57 data definition standards and required federal agencies to report financial and award data in accordance with these standards for DATA Act reporting starting in January 2017. Subsequently, and in accordance with the DATA Act, the Department of Treasury began displaying federal agencies' data on USASpending.gov for taxpayers and policy makers in May 2017.

The DATA Act also requires the IG of each federal agency to audit a statistically valid sample (for non-COVID-19-related obligations) and non-statistically valid sample (for COVID-19 outlays) of the spending data submitted by its federal agency and to submit to Congress a publicly available report assessing the completeness, accuracy, timeliness, and quality of the data sampled, and the implementation and use of the government-wide financial data standards by the federal agency.

The objectives of this audit were to assess:

(1) The completeness, accuracy, timeliness, and quality of the fourth quarter FY 2020 financial and award data submitted by the DNFSB for publication on USASpending.gov; and,

(2) The DNFSB's implementation and use of the governmentwide financial data standards established by the Office of Management and Budget and the Department of the Treasury.

Audit Results:

The OIG found that the DNFSB's fourth quarter FY 2020 submission was not timely, complete, or accurate. It was determined that the DNFSB's data was of lower quality overall. Additionally, the OIG also found that the DNFSB, for the quarter reviewed, was not in compliance with government-wide financial data standards established by the Office of Management and Budget and the Department of the Treasury.

(Addresses Management and Performance Challenge #2)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB in Fiscal Year 2021

OIG Strategic Goal: Safety, Security, and Corporate Management

The Reports Consolidation Act of 2001 requires the IG to annually update our assessment of the DNFSB's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. In this report, we summarize what we consider to be the most critical management and performance challenges to the DNFSB, and we assess the agency's progress in addressing those challenges. Congress left the determination and threshold of what constitutes a most serious management and performance challenge to the Inspector General's discretion. We identify management challenges as those that meet at least one of the following criteria:

(1) The issue involves an operation critical to the DNFSB mission or a DNFSB strategic goal;
(2) There is a risk of fraud, waste, or abuse of DNFSB or other government assets;
(3) The issue involves strategic alliances with other agencies, the Office of Management and Budget, the Administration, Congress, or the public; and,
(4) The issue involves the risk of the DNFSB not carrying out a legal or regulatory requirement.

This year, we have identified five areas representing challenges the DNFSB must address to better accomplish its mission. We have compiled this list based on our audit, the evaluation, and investigative work; general knowledge of the agency's operations; and, evaluative reports of others, including the GAO, and input from DNFSB management.

(Addresses Management and Performance Challenges # 1-5)

Audits in Progress

Audit of the DNFSB's Fiscal Year 2021 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

The Payment Integrity Information Act (PIIA) requires each federal agency to annually estimate its improper payments annually. In addition, the PIIA requires federal agencies to periodically review all programs and activities that the agency administers, and identify all programs and activities that may be susceptible to significant improper payments.

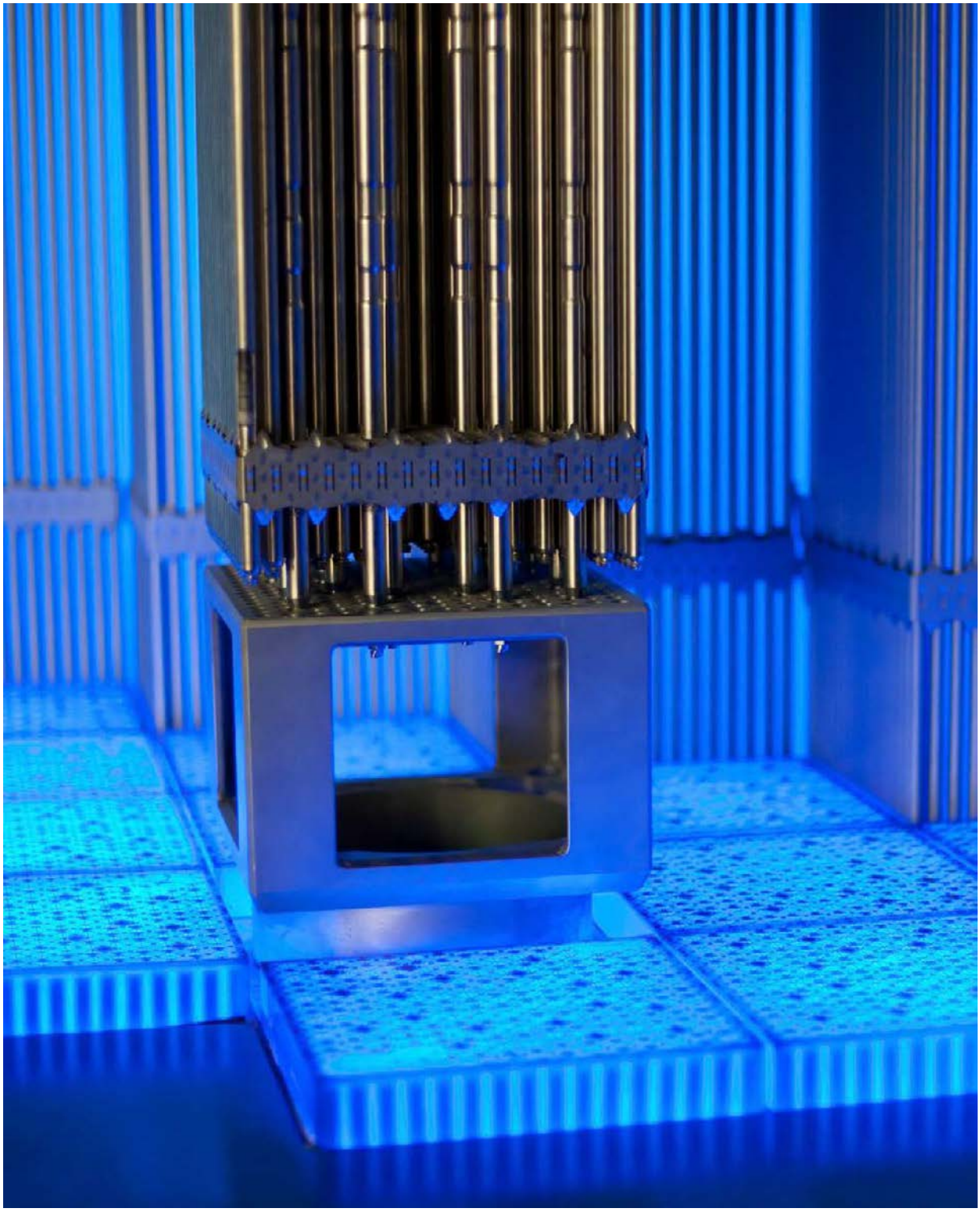
The objective of this audit is to assess the DNFSB's compliance with the PIIA and report any material weaknesses in internal control.

(Addresses Management and Performance Challenge #2)

DNFSB INVESTIGATIONS

Investigative Case Summaries

The OIG did not close any DNFSB investigations during this reporting period.



Fuel Rod Assembly

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

October 1, 2021 – March 31, 2022

Allegations Received: 114 (47 received from the NRC OIG Hotline)

Investigative Statistics

Source of Allegations

NRC Employee	35
NRC Management	20
OIG Investigation	1
General Public	16
Other Government Agency	2
Anonymous	34
Contractor	3
Regulated Industry (Licensee/Utility)	2

Disposition of Allegations

Reviewed (no additional Action needed)	60
Correlated to Existing OIG Investigation	9
Referred to Other Agency	1
Referred to New OIG Investigation	8
Referred to NRC Management	30
Pending Disposition	6
TOTAL:	**114**

Status of Investigations

Federal

DOJ Referrals	2
DOJ Declinations	2
Arrests	1
Search Warrant Executed	1
DOJ Pending	1
Criminal Information/Indictments	1
Criminal Convictions	1
Criminal Penalty Fines	1

State and Local

State and Local Referrals	0
Criminal Convictions	0
Penalty Fines	0

NRC Administrative Actions

Review of Agency Process	2
Change of Issue Process	1
Pending Agency Action	2
Suspensions and Demotions	1

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	4	1	4	0	1
Event Inquiry	2	1	1	1	2
Special Inquiry	0	0	0	1	0
Internal Fraud	1	0	0	0	1
Management Misconduct	6	3	4	2	5
Miscellaneous	1	0	0	0	1
Proactive Initiatives	1	0	0	0	1
Technical Allegations	8	0	3	3	5
Critical Risk – Hight	0	2	0	0	2
TOTAL:	**23**	**7**	**12**	**7**	**18**

**Number of reports issued represents the number of closed cases for which allegations were substantiated and the results were reported outside of the OIG.*

NRC Audits Completed

Date	Title	Audit Number
02/09/2022	Audit of the NRC's Oversight of Counterfeit, Fraudulent, and Suspect Items at Nuclear Power Reactors	OIG-22-A-06
01/19/2022	Audit of the NRC's Permanent Change of Station Program	OIG-22-A-05
12/20/2021	Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2021	OIG-22-A-04
12/10/2021	Results of the Audit of the United States Nuclear Regulatory Commission's Financial Statements for Fiscal Year 2021	OIG-22-A-03
10/28/2021	Audit of the NRC's Compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act)	OIG-22-A-02
10/12/2021	The Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in Fiscal Year 2022	OIG-22-A-01

NRC Contract Audit Reports

OIG Issue Date	Contractor/Title/ Contractor No.	Questioned Costs	Unsupported Costs

None for this period.

NRC Audit Resolution Activities

Table I

OIG Reports Containing Questioned Costs*†

Reports	Number of Reports	Questioned Costs ($)	Unsupported Costs ($)
A. For which no management decision had been made by the commencement of the reporting period	4	$2,013,928	0
B. Which were issued during the reporting period	0	0	0
Subtotal (A + B) ‡	0	$2,013,928	0
C. For which a management decision was made during the reporting period:			
i. Dollar value of disallowed costs	0	0	0
ii. Dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	4	$2,013,928	0

* *The OIG questions costs if there is 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.*

† Certain *questioned costs that pertained to another agency were included in the previous Semiannual Report to Congress and have been removed.*

‡ *The agency cannot make a management decision on questioned costs for QiTech or Advanced Systems Technology Management due to ongoing litigation.*

Table II

OIG Reports Issued with Recommendations that Funds Be Put to Better Use*

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

**A "recommendation that funds be put to better use" is an OIG recommendation that funds could be used more efficiently if NRC management took actions to implement and complete the recommendation.*

Table III

NRC Significant Recommendations Described in Previous Semiannual Reports for which Corrective Action Has Not Been Completed

No Data to report

SUMMARY OF OIG ACCOMPLISHMENTS AT THE DNFSB

October 1, 2021 – March 31, 2022

Source of Allegations

Allegations Received from the DNFSB OIG Hotline: 0

Investigative Statistics

Source of Allegations

DNFSB Employee	n/a
DNFSB Management	n/a
Intervenor	n/a
General Public	1
Other Government Agency	n/a
Anonymous	1
Contractor	n/a
Regulated Industry (Licensee/Utility)	n/a
OIG Self-Initiated	n/a
TOTAL:	**2**

Disposition of Allegations

Closed Administratively	n/a
Referred to OIG Investigations	n/a
Referred to OIG Audit	1
Referred to Other Agency	1
Referred to DNFSB Management	n/a
Pending Review Action	n/a
Processing	n/a
TOTAL:	**2**

Status of Investigations

Federal	
DOJ Referrals	n/a
DOJ Declinations	n/a
DOJ Pending	n/a
Criminal Information/Indictments	n/a
Criminal Convictions	n/a
Criminal Penalty Fines	n/a
Civil Recovery	n/a
Other Recovery	n/a
State and Local	
State and Local Referrals	n/a
State Accepted	n/a
Criminal Information/Indictments	n/a
Criminal Convictions	n/a
Criminal Penalty Fines	n/a
Civil Recovery	n/a
DNFSB Administrative Actions	
Counseling and Letter of Reprimand	n/a
Terminations and Resignation	n/a
Suspensions and Demotions	n/a
Other (e.g., PFCRA)	n/a

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	1	0	0	0	1
Management Misconduct	1	0	0	0	1
Proactive Initiatives	1	0	0	0	1
TOTAL:	**3**	**0**	**0**	**0**	**3**

**Number of reports issued represents the number of closed cases for which allegations were substantiated and the results were reported outside of the OIG.*

DNFSB Audits Completed

Date	Title	Audit Number
01/31/2022	Results of the Audit of the DNFSB's Financial Statements for Fiscal Year 2021	DNFSB-22-A-05
12/21/2021	Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for FY 2021	DNFSB-22-A-04
12/20/2021	Audit of the DNFSB's Process For Planning and Implementing Oversight Activities	DNFSB-22-A-03
11/05/2021	Audit of the DNFSB's Compliance Under the Digital Accountability and Transparency Act of 2014 (DATA Act)	DNFSB-22-A-02
10/16/2021	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB in Fiscal Year 2021	DNFSB-22-A-01

DNFSB Audit Resolution Activities

Table I

OIG Reports Containing Questioned Costs*

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

** The OIG questions costs if there is an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; a finding that, at the time of the audit, such costs are not supported by adequate documentation; or, a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.*

Table II

OIG Reports Issued with Recommendations that Funds Be Put to Better Use*

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

** A "recommendation that funds be put to better use" is an OIG recommendation that funds could be used more efficiently if DNFSB management took actions to implement and complete the recommendation.*

UNIMPLEMENTED AUDIT RECOMMENDATIONS

NRC
Audit of the NRC's Safeguards Information Local Area Network and Electronic Safe (OIG-13-A-16) **1 of 7 recommendations open since April 1, 2013** **Recommendation 3:** Evaluate and update the current folder structure to meet user needs.
Audit of the NRC's Decommissioning Funds Program (OIG-16-A-16) **2 of 9 recommendations open since June 8, 2016** **Recommendation 1:** Clarify guidance to further define "legitimate decommissioning activities" by developing objective criteria for this term. **Recommendation 2**: Develop and issue clarifying guidance to NRC staff and licensees specifying instances when an exemption is not needed.
Audit of the NRC's Implementation of Federal Classified Information Laws and Policies (OIG-16-A-17) **1 of 3 recommendations open since June 8, 2016** **Recommendation 1(b):** Complete the current inventories of classified information in safes and secure storage areas.

Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019 (OIG-20-A-06)

5 of 7 recommendations open since April 29, 2020

Recommendation 2: Use the fully defined ISA to:
(a) assess enterprise, business process, and information system level risks;
(b) formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions;
(c) conduct an organization-wide security and privacy risk assessment;
(d) conduct a supply chain risk assessment; and,
(e) identify and update NRC risk management policies, procedures, and strategy.

Recommendation 4: Perform an assessment of role-based privacy training gaps.

Recommendation 5: Identify individuals having specialized role-based responsibilities for PII or activities involving PII and develop role-based privacy training for them.

Recommendation 6: Based on NRC's supply chain risk assessment results, complete updates to the NRC's contingency planning policies and procedures to address supply chain risk.

Recommendation 7: Continue efforts to conduct agency and system level business impact assessments to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

Independent Evaluation of the NRC's Potential Compromise of Systems (Social Engineering) (OIG-20-A-09)

3 of 13 recommendations open since June 2, 2020

Recommendation 3: Within the next year, perform follow-on telephone tests to gauge the efficacy of the updated training.

Recommendation 9: Within the next year, perform follow-on checks to determine if passwords are being protected.

Recommendation 11: Perform periodic spot checks for employees away during the 15 minute window before the screen locks to ensure that PCs are being protected from unauthorized viewing.

Audit of the NRC's Drug-Free Workplace Program Implementation (OIG-20-A-13)

2 of 4 recommendations open since July 8, 2020

Recommendation 1: Revise the NRC Drug-Free Workplace Plan to reflect the most up-to date U.S. Department of Health and Human Services requirements.

Recommendation 2: Revise the NRC Drug Testing Manual to reflect the most up-to-date U.S. Department of Health and Human Services Requirements.

Audit of NRC's Property Management Program (OIG-20-A-17)

7 of 7 recommendations open since September 30, 2020

Recommendation 1: Modify the definition of accountable property to align with the agency's procedures for accounting for property under the property management program. This encompasses defining and addressing the accountability of items not tracked in the Space and Property Management System (SPMS) including pilferable property.

Recommendation 2: Include the receipt, management, and proper disposal of IT assets planned and currently tracked in Remedy within the property management program. This may include, but is not limited to, actions such as:
(a) updating MD 13.1, Property Management, to designate Remedy as the property tracking system specifically for IT assets;
(b) updating MD 13.1 to include the NRC IT Logistics Index policy for inputting IT assets greater than or equal to $2,500, or which contain NRC information or data within the property management program;
(c) specify in the updated MD 13.1, the use of unique identifiers to track and manage those IT assets within the NRC property management program;
(d) Specify in the updated MD 13.1, the methods and documentation of periodic inventories using unique identifiers within the NRC property management program;
(e) provide appropriate acquisition information in excess property reporting for IT assets that contain NRC information or data; and,
(f) ensure IT assets in the property disposal process comply with documenting media sanitation in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1: *Guidelines for Media Sanitization*.

Recommendation 3: Update and implement property receipt and tagging processes and procedures for the Facilities, Operations, and Space Management Branch (FOSMB),warehouse personnel, and property custodians, that will address:
(a) decentralized property receipt and tagging functions; and,

(b) providing property staff with acquisition information such as the cost and shipping information necessary to perform their property-related duties through automated notification.

Recommendation 4: Limit the regional and the Technical Training Center (TTC) property item assignments to regional property custodians.

Recommendation 5: Consolidate the notification of stolen NRC property to one NRC form.

Recommendation 6: Digitize the property process to facilitate reconciliation and property management workflow.

Recommendation 7: Self-reassess the risk to the agency for the policy changes of the tracking threshold increase and removal of cell phones, laptops, and tablets from the sensitive items list, for loss or theft of property items.

Results of the Audit of the NRC's Financial Statements for FY 2020 (OIG-21-A-02)
5 of 5 recommendations open since November 16, 2020

Recommendation 1: Perform a more robust review of the future lease payments schedule to ensure it reflects all changes and updates to occupancy agreements. This review should include a documented review by the group responsible for negotiating and signing occupancy agreements, since they would be most familiar with all current occupancy agreements.

Recommendation 2: Perform a more robust review of leasehold improvements and require accurate communication from accountable property managers to ensure that, as occupancy agreements change, projects begin, or projects are completed, any impact to leasehold improvements in the financial statements is recorded timely and accurately. This review should also include the timely and complete documenting of the status of leasehold improvements in process.

Recommendation 3: Strengthen its internal control to ensure that funds are de-obligated timely, including identifying amounts to be de-obligated and posting the de-obligation to the accounting system.

Recommendation 4: Maintain adequate documentation, including correspondence, for the reasons why an aged, unliquidated obligation should not be de-obligated.

Recommendation 5: Review the process for generating the unliquidated obligation subsidiary details report (management report); ensure that amounts that are not ULOs, are not included in the management report; and reconcile the management report to the general ledger.

Audit of the NRC's Material Control and Accounting Inspection Program for Special Nuclear Material (OIG-21-A-04)

3 of 3 recommendations open since March 9, 2021

Recommendation 1: Develop and implement enhancements to the existing MC&A communications process to sustain recurring communications between headquarters MCAB and Region II DFFI.

Recommendation 2: Develop and implement a strategy to get staff qualified for MC&A in a timely fashion.

Recommendation 3: Review and update the MC&A inspector qualification program guidance to include a strategy to address emergent MC&A inspection program needs.

Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2020 (OIG-21-A-05)

11 of 13 recommendations open since March 19, 2021

Recommendation 2: Use the fully defined ISA to:

(a) assess enterprise, business process, and information system level risks;
(b) if necessary, update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions;
(c) conduct an organization-wide security and privacy risk assessment, and implement a process to capture lessons learned, and update risk management policies, procedures, and strategies;
(d) consistently assess the criticality of POA&Ms to support why a POA&M is, or is not, of a high or moderate impact to the Confidentiality, Integrity and Availability (CIA) of the information system, data, and mission; and,
(e) assess the NRC supply chain risk, and fully define performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.

Recommendation 4: Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems, (findings noted in bullets 1, 3, and 4 above) by continuing efforts to implement these capabilities using automated tools.

Recommendation 5: Update user system access control procedures to include the requirement for individuals to complete a non-disclosure agreement as part of the clearance waiver process, prior to the individual being granted access to NRC systems and information. Additionally, incorporate the requirement for contractors and employees to complete non-disclosure agreements as part of the agency's on-boarding procedures, prior to these individuals being granted access to the NRC's systems and information.

Recommendation 6: Continue efforts to identify individuals having additional responsibilities for PII or activities involving PII, and develop role-based privacy training for them to be completed annually.

Recommendation 7: Implement the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training, as applicable.

Recommendation 8: Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.

Recommendation 9: Implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or non-reportable incident to US-CERT.

Recommendation 10: Conduct an organizational level BIA to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

Recommendation 11: For low availability categorized systems complete an initial BIA and update the BIA whenever a major change occurs to the system or mission that it supports. Address any necessary updates to the system contingency plan based on the completion of, or updates to, the system level BIA.

Recommendation 12: Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.

Recommendation 13: Implement automated mechanisms to test system contingency plans, then update and implement procedures to coordinate contingency plan testing with ICT supply chain providers, and implement an automated mechanism to test system contingency plans.

Audit of the NRC's Nuclear Power Reactor Inspection Issue Screening (OIG-21-A-07)

3 of 4 recommendations open since March 29, 2021

Recommendation 1: Clarify guidance for inputting inspection results into the RPS that involve TE actions, such as escalated enforcement actions, notices of violation, and licensee identified violations, etc.

Recommendation 3: Improve quality assurance processes implemented in 2021 to identify and fix RPS data entry reporting errors.

Recommendation 4: Conduct periodic training regarding RPS data input.

Audit of the NRC's Pandemic Oversight of Nuclear Power Plants (OIG-21-A-13)

1 of 1 recommendation open since August 4, 2021

Recommendation 1: Conduct an assessment that presents agency management with options for modifying inspection program documents and procedures to give staff flexibility for conducting inspections under irregular conditions.

Audit of the NRC's Oversight of the Adequacy of Decommissioning Trust Funds (OIG-21-A-14)

3 of 4 recommendations open since August 19, 2021

Recommendation 1: Improve process controls to ensure all annual reviews of decommissioning status reports are complete and have undergone the review process.

Recommendation 2: Update LIC-205 to clarify DFS report reviewer roles and responsibilities, procedures for closeout letters, and procedures for tracking DFS report analyses.

Recommendation 4: Periodically assess, through communication with cognizant regulators or by other means, trustee compliance with the master trust fund agreements in accordance with investment restrictions in 10 C.F.R 50.75.

Audit of COVID-19's Impact on Nuclear Materials and Waste Oversight (OIG-21-A-15)

5 of 5 recommendations open since September 23, 2021

Recommendation 1: Revise NRC materials and waste inspection guidance to include instructions on how to respond to prolonged work disruptions, including those that result in required maximum telework or a lack of access to inspection sites.

Recommendation 2: Formally designate WBL as the official system to manage materials and waste inspections data.

Recommendation 3: Provide guidance on how to record data consistently in WBL, including specific information on how and when to populate inspection-related information fields.

Recommendation 4: Review and reconfigure WBL to include mechanisms for recording complete inspections data.

Recommendation 5: Update and implement training for NRC staff to consistently employ the mechanisms developed by the NRC to record the inspections data in WBL.

Audit of the NRC's Implementation of the Enterprise Risk Management Process (OIG-21-A-16)

8 of 8 recommendations open since September 28, 2021

Recommendation 1: Develop and implement a process to periodically communicate a consistently understood agency risk appetite.

Recommendation 2: Revise agency policies and guidance to:
(a) Designate the official agency risk profile document and remove references to it as a U.S. Office of Management and Budget (OMB) deliverable in Management Directive 4.4, Enterprise Risk Management and Internal Control and Office of the Executive Director for Operations Procedure 0960, Enterprise Risk Management Reporting Instructions; and,
(b) Fully address the risk profile components and elements in accordance with OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

Recommendation 3: Implement an enterprise risk management maturity model approach by selecting an appropriate model, assessing current practices per the model, and making progress in advancing the model.

Recommendation 4: Establish and monitor implementation of procedures to ensure that Quarterly Performance Review (QPR) practices are fully performed, such as completion of the QPR Dashboard entries, and recordation of all management decisions of risk in the QPR meeting summaries and the Executive Committee on Enterprise Risk Management meeting minutes.

Recommendation 5: Reconcile the business lines structure with the Office of the Chief Financial Officer to have a common business lines structure list. (Deviations from the common business lines structure list for either the Quarterly Performance Review or reasonable assurance processes may be clarified with applicable justification noted).

Recommendation 6: Update policies and guidance to address Management Directive 4.4, Enterprise Risk Management and Internal Control, and Management Directive 6.9, Performance Management, links to the Quarterly Performance Review (QPR) and reasonable assurance processes to accurately reflect that both agency processes address different aspects of enterprise risk management (ERM). This includes, but is not limited to:
(a) Updating Management Directive 6.9 for the expanded risk responsibilities added to the QPR process;
(b) Explaining the role of the Programmatic Senior Assessment Team (PSAT) in the QPR process in Management Directive 6.9;
(c) Specifying the Executive Committee on ERM (ECERM) role in decision-making of PSAT risks and ECERM focus areas in Management Directive 4.4;
(d) Cross-referencing Management Directive 4.4 to Management Directive 6.9 to clearly show that ERM implementation activities through the QPR process eventually lead to the ERM focus areas and the reporting of ERM in the Integrity Act statement; and,
(e) Including Management Directive 4.4 and Office of the Executive Director for Operations (OEDO) Procedure - 0960 in Management Directive 6.9, "Section VI. References."

Recommendation 7: Update policies and guidance to clarify the effective date of the quarterly risks in the Quarterly Performance Review (QPR) process.

Recommendation 8: Require enterprise-risk-management-specific training that addresses U.S. Office of Management and Budget Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control requirements and current best practices, and periodically provide them to NRC personnel with ERM responsibilities.

Audit of the NRC's Prohibited Security Ownership Process (OIG-21-A-17)

6 of 6 recommendations open since September 30, 2021

Recommendation 1: Clarify roles and responsibilities for completion, tracking, and retention of security ownership forms.

Recommendation 2: Develop and implement quality assurance measures for the prohibited securities process to ensure staff adherence to timeliness metrics and ethics guidance.

Recommendation 3: Develop and implement quality assurance measures to ensure adequate monitoring of prohibited securities records including record retention and external audit capability.

Recommendation 4: Revise MD 7.7, Security Ownership, to include roles and responsibilities clarifications, and remove inconsistencies and outdated information.

Recommendation 5: Develop, finalize, and implement the prohibited securities desk guide.

Recommendation 6: Require all NRC employees to complete annual training on the prohibited securities process, including waiver and extension requests, and require covered employees to sign annual security ownership certification forms.

Audit of the NRC's Compliance with the Digital Accountability and Transparency Act of 2014 (DATA Act) (OIG-22-A-02)

1 of 1 recommendation open since October 28, 2021

Recommendation 1: NRC should improve controls around information in STAQS to ensure data in file D1 included in USAspending.gov is accurate. The control should ensure contract information agrees to STAQS summary information submitted to FPDS-NG.

Results of the Audit of the NRC's Financial Statements for FY 2021 (OIG-22-A-03)

19 of 19 recommendations open since December 10, 2021

Recommendation 1: NRC management should enhance their controls processes over the compilation and preparation of the Agency's quarter-end and year-end financial statements to prevent or timely detect errors to their financial statements and the related note disclosures. Thorough and robust review of the financial statements and related note disclosures should be completed considering the latest requirements of OMB A-136.

Recommendation 2: Accounts Payable Calculation Process
(a) NRC management should update the instructions for the Accounts Payable AccrualEstimation Reconciliation to more clearly indicate that the validated amounts should be used rather than the previously estimated accrual amounts.
(b) NRC management should review the accounts payable reconciliation in insufficient detail to detect errors in the application of the estimation methodology.

Recommendation 3: Accounts Receivable, Net – Calculation Processes
(a) NRC management should update the instructions for the Computation of Allowances for Losses portion of the Unbilled Revenue Accrual and Reconciliation Checklist to include more detailed descriptions of the parameters needed when generating reports used in the calculation process;
(b) NRC management should conduct its review of the calculation of Accounts Receivable – Non-Federal – Allowance for Uncollectable Accounts in sufficient detail to detect errors in the calculation; and,
(c) NRC management should implement stronger controls over the Unbilled Accounts Receivable calculation process and related reviews.

Recommendation 4: NRC management should develop the ability to generate a complete and accurate listing of ULOs in a format which allows for appropriate oversight and review. The report should contain all ULOs at the individual obligation level and be reconciled to the GL with any reconciling items supported by appropriate documentation.

Recommendation 5: Overstatement of New Obligations
(a) NRC management should implement controls to prevent postings in FAIMIS resulting in a negative obligation;
(b) NRC management should increase management review and scrutiny over correcting entries before entries are posted; and,
(c) NRC management should review the financial statements in sufficient detail to detect similar errors in future periods.

Recommendation 6: NRC management should perform reviews of all software, including fully amortized IUS, throughout the year to verify the accuracy of the information reported and ensure disposals of property are recorded in a timely manner.

Recommendation 7: Imputed Financing Calculation Process
(a) NRC management should enhance its review procedures to include which documentation should be used in the imputed financing calculations;and,
(b) NRC management should perform the review of the imputed costs calculation and related disclosures in sufficient detail to detect any errors.

Recommendation 8: Leasehold Improvement Reconciliation and Depreciation
(a) NRC management should enforce the execution of its existing control activities to document explanations for identified variances;and,
(b) NRC management should implement processes and controls which verify that

leasehold improvements are depreciated using the appropriate useful life and in operation date, in accordance with the management's policy.

Recommendation 9: NRC management should enhance its fluctuation analysis control by requiring the explanations documented are supported by underlying business events, therefore connecting changes in the agency's accounting records to its business environment and operations.

Recommendation 10: Inaccurate and Unsupported Undelivered Orders
(a) NRC management should improve its processes for reviewing and adjusting aged/stale obligations.
(b) NRC management should improve its processes to only record an obligation in the accounting system when a legal obligation exists and appropriately retain supporting documentation.

Recommendation 11: Periodically review the segregation of duties matrix and update it to reflect relevant changes in business processes or role configurations within the application.

Recommendation 12: Include a justification for the conflicting roles that reference to compensating controls in place for the requested conflicting roles as part of requests for conflicting roles to be granted to a FAIMIS user.

Recommendation 13: Log and review any conflicting transactions performed by users with authorized conflicting roles to determine if the conflicting transactions were in fact authorized.

Recommendation 14: Validate temporary role assignments as a part of the biannual user access review to ensure they were removed on a timely basis.

Recommendation 15: Review administrator logged activity and document log activities that would require further investigation.

Recommendation 16: Implement the technical capability to disable or remove users who are inactive for greater than the organizationally defined threshold of 90 days.

Recommendation 17: Enhance the periodic recertification of access by ensuring that managers review the access privileges of their staff against the most current segregation of duties matrix to ensure the roles currently assigned conform to policy. In addition, we recommend the help desk documents the removal of roles that management has noted as unnecessary and communicates the confirmation with management that the user's roles were removed.

Recommendation 18: Enhance the process to help ensure that STAQS Access Request Forms are completed and retained.

Recommendation 19: Enhance the process to help ensure that NRC Form 270 is completed and retained for each employee that is separated from the NRC.

Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2021 (OIG-22-A-04)

17 of 18 Recommendations open since December 20, 2021

Recommendation 1: Reconcile mission priorities and cybersecurity requirements into profiles to inform the prioritization and tailoring of controls (e.g., HVA control overlays) to support the risk-based allocation of resources to protect the NRC's identified Agency level and/or National level HVAs.

Recommendation 2: Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity risk information across organizational units; and, (iii) prioritize operational risk response.

Recommendation 3: Update procedures to include assessing the impacts to the organization's ISA prior to introducing new information systems or major system changes into the Agency's environment.

Recommendation 4: Develop and implement procedures in the POA&M process to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.

Recommendation 5: Assess the NRC supply chain risk and fully define performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.

Recommendation 6: Document and implement policies and procedures for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third party providers.

Recommendation 7: Implement processes for continuous monitoring and scanning of counterfeit components to include configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

Recommendation 8: Develop and implement role-based training with those who hold supply chain risk management roles and responsibilities to detect counterfeit system components.

Recommendation 10: Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3

credential access to all NRC systems by continuing efforts to implement these capabilities using automated tools.

Recommendation 11: Update user system access control procedures to include the requirement for individuals to complete a non-disclosure and rules of behavior agreements prior to the individual being granted access to NRC systems and information.

Recommendation 12: Conduct an independent review or assessment of the NRC privacy program and use the results of these reviews to periodically update the privacy program.

Recommendation 13: Implement the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training as applicable or implement the technical capability to capture NRC employees' and contractors' initial login date so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process in place.

Recommendation 14: Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.

Recommendation 15: Implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or non-reportable incident to US CERT.

Recommendation 16: Conduct an organizational level BIA to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

Recommendation 17: Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.

Recommendation 18: Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.

Audit of the NRC's Permanent Change of Station Program (OIG-22-A-05)

4 of 4 Recommendations open since January 19, 2022

Recommendation 1: Update agency guidance to fully reflect and comply with federal guidance.

Recommendation 2: Update relocation allowance guidance to include the current practice of using moveLINQ.

Recommendation 3: Develop and implement a policy to periodically review relocation guidance to ensure the full compliance with federal guidance and alignment with current agency practices.

Recommendation 4: Update relocation guidance to include a supervisory review of reconciliation practices.

Audit of the NRC's Oversight of Counterfeit, Fraudulent, and Suspect Items at Nuclear Power Reactors (OIG-22-A-06)

8 of 8 Recommendations open since February 9, 2022

Recommendation 1: Develop processes and guidance to collect, process, and disseminate CFSI information.

Recommendation 2: Communicate those processes across the agency, or at least to the divisions affected by CFSI.

Recommendation 3: Develop a coherent agencywide approach for CFSI, identifying the agency's primary objective regarding mitigation of CFSI into agency-regulated equipment, components, systems, and structures.

Recommendation 4: Clearly define CFSI.

Recommendation 5: Include a CFSI category in the AMS.

Recommendation 6: Develop inspection guidance with examples pertaining to identifying CFSI in inspection procedures.

Recommendation 7: Develop CFSI training for inspectors.

Recommendation 8: Develop a knowledge management and succession plan for CFSI.

DNFSB

Audit of the DNFSB's Human Resources Program (DNFSB-20-A-04)

6 of 6 recommendations open since January 27, 2020

Recommendation 1: With the involvement of the Office of the Technical Director, develop and implement an Excepted Service recruitment strategy and update guidance to reflect this strategy.

Recommendation 2: Develop and implement a step-by-step hiring process metric with periodic reporting requirements.

Recommendation 3: Update and finalize policies and procedures relative to determining the technical qualifications of Office of the Technical Director (OTD) applicants. This should include examples of experience such as military, and teaching, and their applicability to OTD positions.

Recommendation 4: Develop and issue hiring-process guidance and provide training to DNFSB staff involved with the hiring process.

Recommendation 5: Conduct analyses to determine: (a) the optimal SES span-of-control that promotes agency efficiency and effectiveness; and, (b), the impact on agency activities when detailing employees to vacant SES positions.

Recommendation 6: Develop and implement an action plan to mitigate negative effects shown by the SES analyses.

Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019 (DNFSB-20-A-05)

7 of 11 recommendations open since March 31, 2020

Recommendation 3: Use the defined ISA to:
(a) implement an automated solution to help maintain an up-to-date, complete, accurate, and readily available agency-wide view of the security configurations for all its GSS components; Cybersecurity team exports metrics and vulnerability reports (Cybersecurity Team) and sends them to the CISO and CIO's office monthly, for review. Develop a centralized dashboard that the Cybersecurity Team and the CISO can populate for real-time assessments of compliance and security policies;
(b) collaborate with the DNFSB Cybersecurity Team Support to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by the Cybersecurity Team;
(c) establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program; and,
(d) implement a centralized view of risk across the organization.

Recommendation 5: Management should reinforce requirements for performing the DNFSB's change control procedures in accordance with the agency's Configuration Management Plan by defining consequences for not following these procedures, and conducting remedial training as necessary.

Recommendation 7: Complete and document a risk-based justification for not implementing an automated solution (e.g., Splunk) to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.

Recommendation 8: Continue efforts to meet milestones of the DNFSB ICAM Strategy necessary for fully transitioning to the DNFSB's "to-be" ICAM architecture.

Recommendation 9: Complete current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.

Recommendation 10: Identify and fully define requirements for the incident response technologies the DNFSB plans to utilize in the specified areas, and how these technologies respond to detected threats (e.g., cross-site scripting, phishing attempts, etc.).

Recommendation 11: Based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update the DNFSB's contingency planning policies and procedures to address ICT supply chain risk.

Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2020 (DNFSB-21-A-04)

11 of 14 recommendations open since March 25, 2021

Recommendation 3: Using the results of recommendation 2:

(a) collaborate with the DNFSB's Cybersecurity Team to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by IT Operations;
(b) utilize guidance from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – Performance Measurement Guide for Information Security to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program;
(c) implement a centralized view of risk across the organization; and,
(d) implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities.

Recommendation 5: Conduct remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.

Recommendation 6: Implement procedures and define roles for reviewing configuration change activities to the DNFSB's information system production environments, by those with privileged access, to verify that the activity was approved by the system CCB and executed appropriately.

Recommendation 7: Implement a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system.

Recommendation 8: Implement the technical capability to require PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DFNSB privileged accounts.

Recommendation 9: Implement automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

Recommendation 10: Continue efforts to develop and implement role-based privacy training.

Recommendation 11: Conduct the agency's annual breach response plan exercise for FY 2021.

Recommendation 12: Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.

Recommendation 13: Update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.

Recommendation 14: Based on the results of the DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update the DNFSB's contingency planning policies and procedures to address ICT supply chain risk.

Results of the Audit of the DNFSB's Financial Statements for FY 2020 (DNFSB-21-A-03)

2 of 2 recommendations open since December 21, 2020

Recommendation 1: Develop a plan to improve the financial reporting controls and process, including identifying and training back up staff, so that financial statements and the related notes are properly prepared and reviewed at interim and year-end on a timely basis.

Recommendation 2: Prepare and review all key financial statement reconciliations and resolve significant reconciling items on a monthly basis.

Audit of the DNFSB's Compliance Under the Digital Accountability and Transparency Act of 2014 (DATA Act) (DNFSB-22-A-02)

2 of 2 recommendations open since November 5, 2021

Recommendation 1: Enhance internal control and detective procedures surrounding DATA Act submissions. Procedures should include documenting reconciliations between DATA Files A, B, C, and D1, researching and resolving differences between files including resolving warning reports on a timely basis, and submitting DATA Act information timely to the DATA Act Broker in accordance with the reporting schedule established by the Treasury DATA Act Program Management Office. (Partial repeat of 2019 DATA Act audit report recommendation two)

Recommendation 2: Ensure Object Class Code is consistently documented on the contract.

Audit of the DNFSB's Process for Planning and Implementing Oversight Activities (DNFSB-22-A-03)

3 of 3 recommendations open since December 20, 2021

Recommendation 1: As an agency overall, and the respective Board members themselves, continue to identify, implement, and directly participate in, process improvements that will provide clearer direction and priorities from the Board during the early phases of the work planning process, such as incorporating strategic direction from the Board into the planning memo.

Recommendation 2: Develop and implement a strategy for maintaining routine awareness of future subject matter areas that may become understaffed.

Recommendation 3: Strengthen expertise in subject matter expert areas that lack depth through knowledge management and training.

Independent Evaluation of the DNFSB'S Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for FY 2021 (DNFSB-22-A-04)

23 of 24 recommendations open since December 21, 2021

Recommendation 2: Using the results of recommendations 1:
(a) Utilize guidance from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – Performance Measurement Guide for Information Security to establish performance metrics to manage and optimize all domains of the DNFSB information security program more effectively;
(b) Implement a centralized view of risk across the organization; and,
(c) Implement formal procedures for prioritizing and tracking POA&Ms to remediate vulnerabilities.

Recommendation 3: Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include:

(a) Defining a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.

Recommendation 4: Define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for:

(a) How supply chain risks are to be managed across the agency;
(b) How monitoring of external providers compliance with defined cybersecurity and supply chain requirements; and,
(c) How counterfeit components are prevented from entering the DNFSB supply chain.

Recommendation 5: Conduct remedial training to reinforce requirements for documenting security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.

Recommendation 6: Integrate the Configuration Management Plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.

Recommendation 7: Implement automated mechanisms (e.g., machine-based or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

Recommendation 8: Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.

Recommendation 9: Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.

Recommendation 10: Conduct the agency's annual breach response plan exercise for FY 2021.

Recommendation 11: Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.

Recommendation 12: Formally document requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete role-based training.

Recommendation 13: Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.

Recommendation 14: Update the DNFSB ISCM policies and procedures, clearly defining what needs to be monitored at the system and organization level.

Recommendation 15: Define standard operating procedures for the use of the agency's continuous monitoring tools or update the continuous monitoring plan to include the use of new monitoring tools.

Recommendation 16: Define the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.

Recommendation 17: Define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.

Recommendation 18: Consistently test the Incident response plan annually.

Recommendation 19: Update the agency's incident response plan to reflect the USCERT incident reporting guidelines.

Recommendation 20: Allocate and train staff with significant incident response responsibilities.

Recommendation 21: Configure all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.

Recommendation 22: Develop and track metrics related to the performance of contingency planning and recovery related activities.

Recommendation 23: Conduct a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.

Recommendation 24: Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.

Results of the Audit of the DNFSB's Financial Statements for FY 2021 (DNFSB-22-A-05)

6 of 7 recommendations open since January 31, 2022

Recommendation 1: Implement policies and procedures to perform monitoring of the NFC, including obtaining and reviewing the SOC1 report and appropriately implement CUECs, as needed. Management should maintain evidence of its review of the USDA SOC1 report and ensure all CUECs are implemented and operate effectively.

Recommendation 2: Defines and implements access and segregation of duties controls to:
(a) Provision and periodically recertify user access to Symplicity; and,
(b) Segregate the duties of users with access to the financial data in Symplicity.

Recommendation 3: Management Lacks Proper Review of Property

(a) We recommend that DNFSB management implements a process to perform a more detailed review of the General Property, Plant, and Equipment, Net balance on their financial statements, as well as further develop controls to ensure the accuracy and completeness of the asset related financial data; and,
(b) We recommend that DNFSB management implements a process to ensure that acquisition costs are reported at the time the asset is placed in service and capitalization has started, especially if there is a significant impact to the reported balance.

Recommendation 4: We recommend DNFSB management implements and documents monitoring controls to ensure all payroll related expenses from the pay files are properly and accurately recorded in the general ledger.

Recommendation 5: We recommend the DNFSB implements policies, procedures, and controls to ensure calculated imputed costs are reasonable and supportable.

Recommendation 6: We recommend DNFSB management utilizes information more directly relevant to the line item, as available, such as on the leave liability report, in order to determine the unfunded leave liability amount to be recorded as of year-end.

ABBREVIATIONS AND ACRONYMS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
C.F.R.	Code of Federal Regulations
CLA	CliftonLarsonAllen
CFSI	Counterfeit, Fraudulent, and Suspect Items
COVID-19	Coronavirus Disease 2019
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
DPO	Differing Professional Opinion
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FTR	Federal Travel Regulation
FY	Fiscal Year
GAO	Government Accountability Office
GLINDA	Global Infrastructure and Development Acquisition
GT	Grant Thornton
IAM	Issue Area Monitoring
IG	Inspector General
IT	Information Technology
MD	Management Directive
NRC	Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OEDO	Office of the Executive Director for Operations
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIP	Office of International Programs
OMB	Office of Management and Budget
ONMSS	Office of Nuclear Material Safety and Safeguards
OTD	Office of the Technical Director
PCS	Permanent Change of Station
RAC	Reasonable Accommodation Coordinator
SBG	SBG Technology Solutions, Inc.
SWP	Strategic Workforce Planning
WPA	Whistleblower Protection Act

REPORTING REQUIREMENTS

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

Citation	Reporting Requirements	Page(s)
Section 4(a)(2)	Review of legislation and regulations	13–14
Section 5(a)(1)	Significant problems, abuses, and deficiencies	15–27; 35–38
Section 5(a)(2)	Recommendations for corrective action	15–27
Section 5(a)(3)	Prior significant recommendations not yet completed	N/A
Section 5(a)(4)	Matters referred to prosecutive authorities	50, 56
Section 5(a)(5)	Listing of audit reports	51, 52, 57
Section 5(a)(6)	Listing of audit reports with questioned costs or funds put to better use	52
Section 5(a)(7)	Summary of significant reports	15–27
Section 5(a)(8)	Audit reports — questioned costs	53, 59
Section 5(a)(9)	Audit reports — funds put to better use	54, 60
Section 5(a)(10)	Audit reports issued before commencement of the reporting period (a) for which no management decision has been made, (b) which received no management comment with 60 days, and (c) with outstanding, unimplemented recommendations, including aggregate potential costs savings.	61-70
Section 5(a)(11)	Significant revised management decisions	43
Section 5(a)(12)	Significant management decisions with which the OIG disagreed	N/A
Section 5(a)(13)	FFMIA section 804(b) information	N/A
Section5(a)(14)(15)(16)	Peer review Information	75
Section 5(a)(17)	Investigations statistical tables	40-50; 55-56
Section 5(a)(18)	Description of metrics	50, 56
Section 5(a)(19)	Investigations of senior government officials where misconduct was substantiated	N/A
Section 5(a)(20)	Whistleblower retaliation	N/A
Section 5(a)(21)	Interference with IG independence	N/A
Section 5(a)(22)	Audit not made public	20
Section 5(a)22(b)	Investigations involving senior government employees where misconduct was not substantiated, and report was not made public	30-35; 36-37; 38-40

APPENDIX

Peer Review Information

Audits

The NRC OIG audit program was peer reviewed by the OIG for the Smithsonian Institution. The review was conducted in accordance with Government Auditing Standards and Council of the Inspectors General on Integrity and Efficiency (CIGIE) requirements. In a report dated September 30, 2021, the 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.* The review team issued a Letter of Comment, dated September 30, 2021, that sets forth the peer review results and includes a recommendation to strengthen the NRC OIG's policies and procedures.

Investigations

The NRC OIG investigative program was peer reviewed by the Department of Commerce OIG. The peer review final report, dated November 1, 2019, reflected that the NRC OIG is in full compliance with the quality standards established by the CIGIE and the Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the planning, execution, and reporting of investigations.

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 IT Resources
- Program Mismanagement

Ways To Contact the OIG

Call:
OIG Hotline
1-800-233-3497
TTY/TDD: 7-1-1, or
1-800-201-7165 7:00 a.m. – 4:00 p.m. (EST)
After hours, please leave a message.

Submit:
Online Form
www.nrcoig.oversight.gov
Click on OIG Hotline

Write:
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program,
MS O5 E13
11555 Rockville Pike
Rockville, MD 20852-2738

Vol. 36, No. 2 October 2022