Semiannual Report to Congress
October 1, 2022—March 31, 2023

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 U.S. Nuclear Regulatory Commission and the Defense Nuclear Facilities Safety Board, to protect people and the environment.

COVER PHOTO:

A dry cask loaded with spent fuel being lifted from a horizontal transporter to be placed vertically on a specially designed storage pad. Photo courtesy of Sandia National Laboratories.

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, 2022 to March 31, 2023. I continue to be grateful for the opportunity to lead this extraordinary group of managers, auditors, investigators, and support staff, and I am extremely proud of their exceptional work.

During this reporting period, we initiated thirteen audit reports and issued four. We also opened ten investigative cases and completed twelve, six of which were referred to the Department of Justice, and six of which were referred to NRC or DNFSB 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 financial statement evaluation; top management and performance challenges facing the NRC; DNFSB's financial statement evaluation; and, top management and performance challenges facing the DNFSB. Further, this report includes summaries of cases and/or allegations involving: the NRC's petition process; oversight of technical regulatory issues at Diablo Canyon Nuclear Power Plant; computer misuse and computer forensic support; theft of NRC government property; unauthorized telework in NRC Region II; alleged deficiencies in the fire protection program at a nuclear power plant; and, DNFSB's computer misuse and computer forensic support.

Our team members dedicate 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
Inspector General

Highlights

OFFICE of AUDITS

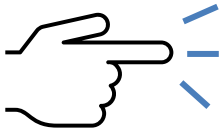
2
Reports Issued

2
Reports Issued

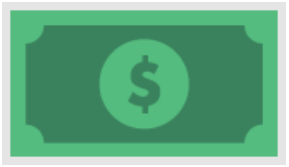
0	**Recommendations Made**	0
8	**Recommendations Closed**	20

Highlights

OFFICE of INVESTIGATIONS



1 Reprimand



1 Civil/Administrative Recovery

$ 742,500.00

10

Open Investigations

12

Closed Investigations

18

In-Progress Investigations

CONTENTS

An NRC's inspector performs a walk through inspection at a nuclear power plant.

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

U.S. Nuclear Regulatory Commission

- 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 CliftonLarsonAllen (CLA) to conduct this annual audit. CLA examined the NRC's fiscal year (FY) 2022 Agency Financial Report, which includes financial statements for FY 2022.

- The Reports Consolidation Act of 2001 requires the Office of the Inspector General (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 10 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, evaluative reports of others, including the Unites States 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 CLA to conduct this annual audit. CLA examined the DNFSB's FY 2022 Agency Financial Report, which includes financial statements for FY 2022.

- The Reports Consolidation Act of 2001 requires the OIG 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. This year, the OIG identified five areas representing challenges the DNFSB 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, evaluative reports of others, including the GAO, and input from DNFSB management.

Investigations

U.S. Nuclear Regulatory Commission

- The OIG received an allegation from a nongovernmental organization (NGO) that the NRC's policy for handling 2.206 petitions, which is Management Directive (MD) 8.11, *Review Process for 10 C.F.R. 2.206 Petitions,* does not meet the intent of the Energy Reorganization Act of 1974. Additionally, the NGO questioned if the NRC addressed the concerns identified in the OIG Event Inquiry regarding the Indian Point gas pipeline.

- The OIG initiated a special project in FY 2022 to identify any significant safety and security issues at Diablo Canyon Nuclear Power Plant. We evaluated almost two dozen technical issues from previous allegations and investigations conducted from FY 2015 to FY 2022. We combined three sets of allegations regarding emergency diesel generators, ranging from fuel leaks resulting from loose bolts, regularly occurring mechanical failures, and undue influence from a licensee on the NRC into one investigation that will be addressed in a case report scheduled in FY 2023.

- The OIG initiated a project at the beginning of FY 2021 to identify any potential cases of intrusions into the NRC Information Technology systems from both inside and outside of the agency. The project resulted in six actions, including the opening of a case in FY 2021 that is still being conducted jointly with a Federal Bureau of Investigation (FBI) field office. The OIG's Cyber Crimes Unit (CCU) monitored an incident involving a software breach and ensured the NRC Office of the Chief Information Officer (OCFO) had all current information from the FBI and the Intelligence Community. The OIG has a CCU special agent assigned to the FBI Baltimore Field Office Cyber Task Force, and OIG CCU agents participate in the daily network OCFO update meetings, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Information Technology (IT) Sub-Committee meetings, and the Department of Justice (DOJ) Computer Crime and Intellectual Property Section meetings to support governmentwide initiatives aimed at intrusions and misuse of government systems.

- The OIG completed an investigation regarding a former contract employee, who failed to return his Personal Identity Verification (PIV) card and NRC laptop after his employment was terminated. The employee acknowledged that he did not return the laptop because he felt "vindictive" about the circumstance of his removal. We executed a search warrant at the employee's premises and recovered his laptop and PIV card. The State's Attorney's Office of Howard County, Maryland charged the employee but dropped the charges three months later. The NRC's Office of the General Counsel issued a notice of debarment against the individual from all federal contracts for three years.

- The OIG received an allegation that an NRC health services contractor was not fulfilling its contract obligations because its subcontractor failed to provide records in a timely manner. Our investigation revealed that while the subcontractor's performance had declined, the records in question had, in fact, been provided.

- The OIG investigated an allegation of unauthorized telework and travel-related issues by an NRC employee, and that management was complicit in these violations. We found the employee had unauthorized telework on 11 dates during 2021, but did not find management complicit. We also found that between January 2018 and July 2021, the employee violated federal and NRC policy by traveling indirectly 17 times, claiming an improper temporary duty location with higher per diem rates on 3 occasions, and overcharging the government for multiple modes of travel once, which resulted in a loss of $1,701.24. Lastly, we found payment of per diem meals and incidental expenses for non-workdays on nine of the employee's travel vouchers between January 2018 and February 2020, totaling an overpayment of $3,867—a grand total of $5,568.24. We recommended that the agency recover the overpayment.

- The OIG received an allegation regarding deficiencies in the fire protection program at a nuclear power plant, related in part to the plant's transition to a performance-based fire protection

model under National Fire Protection Association Standard 805. The alleger asserted that the licensee provided the NRC with inaccurate and incomplete information about potential areas of code noncompliance, and that multiple fire code noncompliance issues remain at the plant. Our investigation identified potential oversight concerns involving fire safety relating to the plant's service water intake structure pump rooms and fire probabilistic risk assessment.

Defense Nuclear Facilities Safety Board

- The OIG initiated a project to identify potential cases of intrusions to the DNFSB IT system because of emails and website traffic from internal and external sources. The project resulted in the DNFSB migrating to a different website monitoring software system with greater capability to determine which restricted sites internal users accessed. OIG CCU special agents worked with the Chief Information Security Officer (CISO) to build relationships with CISO staff members and participated with the FBI Baltimore Field Office Cyber Task Force, the CIGIE IT Sub-Committee, and the DOJ Computer Crime and Intellectual Property Section to support governmentwide initiatives aimed at intrusions.

Spent nuclear fuel dry storage casks

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 at NRC offices and in communities throughout the United States; 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 amendments to the IG Act, to provide oversight of NRC operations. The Consolidated Appropriations Act of 2014 subsequently authorized the NRC IG to exercise the same authorities concerning DNFSB operations. The OIG's mission is to provide independent, objective audit and investigative oversight of the operations of these agencies, 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.

OIG PROGRAMS AND ACTIVITIES

Audit Program

The OIG Audit Program focuses on management and financial operations; the economy and 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. They 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 Chair or DNFSB Chair, 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 posing a high potential for fraud, waste, and abuse.

Because the NRC's mission is to protect public health and safety, 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. § 404(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, 2022 to March 31, 2023, the OIG's General Counsel (GC) 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 GC 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 GC 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 GC did not identify any issues that would significantly compromise our independence or conflict with our audit or investigatory functions. The OIG GC, however, did identify certain proposed staff polices that might affect, to some extent, the work of the OIG. In these cases, the OIG GC proposed edits or changes that would mitigate the impacts and requested responses from the staff. Agency staff either accepted the OIG GC's proposals or offered well-supported explanations as to why the proposed changes were not accepted. These reviews are described in further detail below.

NRC Management Directives

- MD 4.2, *Administrative Control of Funds*, which describes the policies, procedures, and standards the NRC has implemented to comply with the Antideficiency Act, the Chief Financial Officers Act, the Economy Act, the Impoundment Control Act, Office of Management and Budget (OMB) Circular A-11, and other authorities. The revisions to this MD reflected changes affected by the Nuclear Energy Innovation and Modernization Act, as well as the addition of new MD sections addressing "Forward Funding" and "Fund Sources." The OIG's comments on this MD included a recommendation to remove references to OIG report OIG-13-A-18, "Audit of the NRC's Budget Execution Process," because the NRC staff had already addressed that report in a prior revision of MD 4.2. The OIG also recommended changes to various legal citations in the MD to reflect the December 2022 recodification of the Inspector General Act at 5 U.S.C. §§ 401–424.

- MD 4.4, *Enterprise Risk Management*, which provides guidance to the NRC staff for complying with the Federal Managers' Financial Integrity Act of 1982, OMB Circular A-123, the GAO's "Standards for Internal Control in the Federal Government," and other authorities. The OIG provided extensive comments on this MD that included recommendations to clarify the responsibilities of various NRC offices or divisions, more fully explain the steps involved when the NRC takes certain actions described in the MD, cross-reference language in the MD with associated NRC documents or external documents, and update references or remove outdated references. Because some of the revisions in the MD related to recommendations the OIG made in report OIG-21-A-16, "Audit of the NRC's Implementation of the Enterprise Risk Management Process," and because the OIG has not yet closed its recommendations in that report, the OIG also advised the NRC staff that it must continue to engage with the OIG on the subject of enterprise risk management. In particular, the OIG will need to evaluate revisions to other documents that are relevant to report OIG-21-A-16 and may need to engage in further discussions with the staff regarding audit-related items.

- MD 12.8, *NRC Defensive Counterintelligence Program*, which is a new MD that provides guidance for the agency's limited-scope

defensive counterintelligence program. The OIG contributed to this MD at an early stage by providing input on both the MD and an associated "Defensive Counterintelligence Program Guide" that provides office-specific and position-specific guidance for carrying out responsibilities associated with the agency's program. The OIG also reviewed both the MD and the Program Guide, once finalized, as well as an associated delegation-of-authority memorandum, to ensure they accurately reflect applicable laws, rules, and policies, including those that relate to OIG oversight.

The OIG also reviewed the following MDs during the period covered by this Semiannual Report: MD 2.8, *Integrated Information Technology Management Governance Framework*; MD 3.7, *NUREG-Series Publications*; MD 5.4, *Official Representation Expenses*; MD 8.14, *Agency Action Review Meeting*; MD 9.8, *Organization and Functions, Office of Investigations*; MD 9.11, *Organization and Functions, Office of Public Affairs*; MD 9.21, *Organization and Functions, Office of Administration*; MD 10.1, *Recruitment, Appointments, and Merit Staffing*; MD 10.12, *Use of Advisory Committee Members* (the OIG reviewed an initial revision to this MD in the period covered by the last Semiannual Report, and the OIG reviewed a second revision during the current period); MD 10.138, *Reductions in Force and Furloughs in the Senior Executive Service*; MD 10.50, *Pension Offset Waiver*; and MD 12.2, *NRC Classified Information Security Program*. While the OIG provided editorial or formatting suggestions for some of these MDs, we had no substantive comments on these directives.

DNFSB Directive

- D-231.2, *Freedom of Information Act (FOIA) Program*, which establishes policies and assigns responsibilities for complying with the FOIA and related authorities. The OIG recommended changes to clarify the responsibilities of various DNFSB officials under the directive and better align the directive's language with the FOIA. The OIG also recommended adding a specific reference to our office in a section of the directive that mentions the DNFSB's process for referring FOIA requests to other federal agencies or consulting with other agencies on a FOIA response.

Other Activities

NRC OIG: Settlement of Fraud Allegations Involving NRC Contractor

After years of coordinated effort between the NRC OIG and four other agencies, as well as cooperation from the NRC staff, the IG is pleased to announce the settlement of fraud allegations involving an NRC contractor. Though the claims resolved by the settlement are allegations only, and there has been no determination of liability, the settlement will recover more than $700,000 to the benefit of the national treasury.

You can find more information about this case in a press release from the U.S. Attorney's Office for the Eastern District of Virginia.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in FY 2023*   ***(As identified by the Inspector General)***
Challenge 1: *Ensuring safety while transforming into a modern, risk-informed regulator.*
Challenge 2: *Overseeing the decommissioning process and the management of decommissioning trust funds.*
Challenge 3: *Strengthening the NRC's readiness to respond to future mission-affecting disruptions.*
Challenge 4: *Advancing 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: *Implementing strategic workforce planning during transformation and industry change.*
Challenge 7: *Oversight of materials, waste, and the National Materials Program.*
Challenge 8: *Managing financial and acquisitions operations to enhance transparency and fiscal prudence.*
Challenge 9: *Reinforcing the NRC's readiness to address cyber and physical security threats to critical national infrastructure sectors impacting the NRC's public health and safety mission and/or NRC licensees.*
Challenge 10: *Maintaining public outreach to continue strengthening the agency's regulatory process.*

** For more information on these challenges, see OIG-22-A-03, "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC in Fiscal Year 2023." https://nrcoig.oversight.gov/top-management-challenges*

NRC AUDITS

Audit Summaries

Audit of the NRC's Fiscal Year 2022 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 NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with CLA to conduct this annual audit. CLA examined the NRC's FY 2022 Agency Financial Report, which includes financial statements for FY 2022.

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

Audit Results:

In CLA's opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the NRC as of September 30, 2022, 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 CLA's opinion, the NRC maintained, in all material respects, effective internal control over financial reporting as of September 30, 2022, no reportable noncompliance for FY 2022 with provisions of applicable laws, regulations, contracts, and grant agreements we tested and no other matters.

(Addresses Management and Performance Challenge #8)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in Fiscal Year 2023

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 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 10 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 #1–10)

Audits in Progress

Audit of the NRC's Information Technology Services and Support

OIG Strategic Goal: Corporate Management

The NRC offers various 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 6 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 #5)

Audit of the NRC's Oversight of Irretrievable Well Logging Source Abandonments

OIG Strategic Goal: Safety

Well logging is a process used to determine whether a well drilled deep into the ground has the potential to produce oil. This process uses a byproduct or special nuclear material tracer and sealed sources in connection with the exploration for oil, gas, or minerals in wells. If a sealed source becomes lodged in a well and it becomes apparent that efforts to recover the sealed source will not be successful, the source is considered irretrievable, and licensees are permitted to abandon the well logging source.

Title 10 of the Code of Federal Regulations (C.F.R.), Part 39, prescribes the requirements for license issuance and radiation safety requirements for

well logging. Under Part 39, if a licensee has an irretrievable well logging source, the licensee must notify the NRC to obtain approval to implement abandonment procedures.

The audit's objective is to determine the adequacy of the NRC's handling and processing of irretrievable well logging source abandonments.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Processes for Deploying Reactive Inspection Teams

OIG Strategic Goal: Safety

The NRC conducts routine inspections at nuclear power plants to maintain baseline safety and security oversight of nuclear power licensees. However, the agency also conducts reactive inspections in response to events that may have compromised the safety or security at nuclear power plants. The agency may also deploy more resource-intensive augmented or integrated inspection teams depending on an incident's risk significance, complexity, and generic safety or security implications.

According to MD 8.3, "NRC Incident Investigation Program," NRC managers should use a combination of deterministic and quantitative risk criteria in deciding whether to deploy special, augmented, or incident inspection teams to power reactor sites. Deterministic criteria include major design, construction, or operational deficiencies that could have generic implications; failure of plant safety-related equipment; and, physical or information security breaches. Risk criteria are based on conditional core damage probabilities ranging on a scale from 1E-6 or lower to 1E-3; accordingly, lower risk events merit special inspection teams, while progressively higher risk events merit augmented and integrated inspection teams.

The NRC may also deploy special, augmented, and integrated inspection teams to non-power reactor sites based on deterministic criteria. For example, MD 8.3 states that integrated inspection teams should be considered in response to events that cause significant radiological releases, or occupational or public radiological exposures that exceed specific regulatory limits. The guidance also recommends integrated inspection teams for a variety of other events that have actual or potential adverse health, safety, or security consequences.

The audit objective is to assess the consistency with which the NRC follows agency guidance for deploying special, augmented, and integrated inspection teams in response to safety and security incidents at nuclear power plants.

(Addresses Management Performance Challenge #1)

Audit of the NRC's Voluntary Leave Transfer Program

OIG Strategic Goal: Corporate Management

The Voluntary Leave Transfer Program makes it possible for employees to donate annual leave, on a confidential and voluntary basis, to employees who face financial hardship because of personal or family illness. NRC employees may donate as much as one-half of the total annual leave accrued in the current leave year. Annual leave donations may be made at any time during the year.

An employee who has been affected by a medical emergency may apply to become a leave recipient. Such application must be in writing, signed by the employee and addressed to the Director, Office of the Chief Human Capital Officer (OCHCO). The Director, OCHCO, or designee, will normally approve, or disapprove with explanation, the applicant's request within 10 calendar days (excluding Saturdays, Sundays, and legal public holidays) from the receipt of an adequately documented request.

The audit objective is to determine the extent to which the NRC has established effective policies and procedures for managing its voluntary leave transfer program.

(***Addresses Management Performance Challenge #6)***

Audit of the NRC's Fiscal Year 2022 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

Enacted in 2020, the Payment Integrity Information Act of 2019 (PIIA) requires executive agencies to periodically review all programs and activities an agency administers and identify all programs and activities with outlays exceeding $10 million that may be susceptible to significant improper payments. The review should occur not less than once every 3 years for each program and activity. The PIIA requires the OIG of each executive agency to determine agency compliance annually.

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

(Addresses Management Performance Challenge #8)

Audit of the NRC's Oversight of the Agency's Federally Funded Research and Development Center Contract

OIG Strategic Goal: Corporate Management

In October 1987, the NRC entered into a 5-year contract with Southwest Research Institute (SwRI) to operate a Federally Funded Research and Development Center (FFRDC) in San Antonio, Texas. SwRI established the Center for Nuclear Waste Regulatory Analyses (the Center) to provide the agency with long-term technical assistance and research related to the NRC's High-Level Waste program under the Nuclear Waste Policy Act of 1982, as amended. The current contract, which expired on March 29, 2023, has a ceiling of $52 million, and is one of the NRC's largest active contracts. The Commission must decide whether to renew it.

The Federal Acquisition Regulation (FAR) requires that, prior to renewing a contract for an FFRDC, a sponsor must conduct a comprehensive review of the use and need for the FFRDC. The OIG previously reviewed the nature and adequacy of the NRC's renewal justification in 1992, 1997, 2002, 2007, 2012, and 2018.

The audit objectives are to determine if the NRC is properly considering all FAR requirements for an FFRDC review in preparing its renewal justification, and to determine if the NRC is adequately fulfilling its oversight responsibilities for the FFRDC.

(Addresses Management Performance Challenge #8)

Audit of the NRC's Process for Announcing Staff Vacancies

OIG Strategic Goal: Corporate Management

During the NRC's 2022 Regulatory Information Conference, Commissioner Jeff Baran said the NRC is facing a significant hiring challenge with many employees eligible for retirement, and an annual attrition rate of approximately six to eight percent. Commissioner Baran stated that the NRC must hire approximately 200 employees per year to sustain its workforce, and for 2022, the NRC must hire 300 employees.

The policy of the NRC is to operate an external recruitment program, operate a merit staffing program, and appoint or assign diverse employees who are well qualified to carry out the mission of the agency efficiently and effectively. The NRC designates vacancies as either part of a bargaining or non-bargaining unit. A union represents bargaining unit employees, who, as such, have rights and entitlements that are spelled out in a Collective Bargaining Agreement. A non-bargaining unit employee is not represented by a union.

The practices and policy for bargaining unit status employees are contained in the NRC's and the National Treasury Employee Union's Collective Bargaining Agreement. This Agreement states that a vacancy announcement must be posted for at least 10 calendar days. NRC's MD 10.1, Recruitment, Appointments, and Merit Staffing, covers the policies and practices for non-bargaining unit employees. To ensure job applicants have an equal opportunity to compete, vacancy announcements must be open for a minimum of 5 working days.

The audit objective is to determine if the NRC provides adequate time for job applicants to compete for positions, and identify opportunities for improvement in the vacancy announcement process.

(Addresses Management Performance Challenge #6)

Audit of the NRC's Security Oversight of Category 1 and Category 2 Quantities of Radioactive Material

OIG Strategic Goal: Security

Radioactive materials are used throughout the United States for medical and industrial purposes such as treating cancer, sterilizing medical instruments, and detecting flaws in metal welds. Among the materials most commonly used for these applications are americium-241/beryllium, cesium-137, cobalt-60, and iridium-192. However, these materials, if used improperly, can be harmful and dangerous.

The International Atomic Energy Agency's Code of Conduct on the Safety and Security of Radioactive Sources establishes basic principles and guidance to promote the safe and secure use of radioactive material. It defines categories of radiation source quantities:

- A Category 1 of a given radionuclide, such as americium-241, is defined as an amount 1,000 times or more than the amount necessary to cause permanent human injury;
- A Category 2 is defined as an amount at least 10 times but less than 1,000 times the amount necessary to cause permanent human injury;
- A Category 3 of a given radionuclide is defined as at least the minimum amount, but less than 10 times the amount, sufficient to cause permanent injury; and,
- Category 4 and 5 of radioactive materials are unlikely to cause permanent injury.

The regulations in 10 C.F.R. Part 37 prescribe requirements for the physical protection program for any licensee that possesses an aggregated Category 1 or Category 2 quantity of radioactive material listed in Appendix A to this part. These requirements provide reasonable assurance of the security of Category 1 or Category 2 quantities of radioactive material by protecting these materials from theft or diversion. Only Categories 1 and 2 radiation sources are subject to Part 37's requirements since Categories 3 through 5 sources are not considered to be as dangerous.

The audit objective is to determine whether the NRC provides adequate security oversight of Category 1 and Category 2 quantities of radioactive material.

(Addresses Management Performance Challenge #7)

Audit of NRC Safety Inspections at Research and Test Reactors

OIG Strategic Goal: Safety

The NRC currently licenses 30 operating research and test reactors in the United States. Most are located at universities and colleges, while others are located at federal, state, and private sector facilities. Research and test reactors contribute to research in diverse fields such as physics, medicine, archeology, and materials science. Research and test reactors use a limited amount of radioactive material in their diverse designs and are rated at power levels ranging from 5 watts thermal energy to 20 megawatts. All are designed to be inherently safe and resistant to unintentional or intentional misoperation.

The NRC categorizes operating research and test reactors into two classes for inspection purposes. Class I reactors are rated at 2 megawatts or higher and are inspected annually. Class II reactors are rated below 2 megawatts and are inspected biennially. NRC staff use different procedures to inspect these two classes of research and test reactors; however, the procedures all address safety, security, and transportation of radiological materials used in the reactors. The OIG audited NRC security inspections at research and test reactors in FY 2018 (OIG-18-A-07) and conducted investigative work pertaining to safety inspections at Class I research and test reactors during FY 2022.

The audit objective is to determine whether the NRC performs safety inspections at Class II research and test reactors in accordance with agency guidance and inspection program objectives.

(Addresses Management Performance Challenge #1)

Audit of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2023

OIG Strategic Goal: Corporate Management

The FISMA outlines information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. In addition, the FISMA includes such provisions as 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 to 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 Office of Management and Budget and Congress on the effectiveness of their security programs.

The audit objective is to assess the effectiveness of the information security policies, procedures, and practices of the NRC.

(Addresses Management Performance Challenge #5)

NRC INVESTIGATIONS

Investigative Summaries

Concerns Regarding the NRC's 10 C.F.R. 2.206 Petition Process

OIG Strategic Goal: **Safety**

Allegation:

We reviewed an allegation from an NGO that the NRC's policy for handling 2.206 petitions, which is MD 8.11, "Review Process for 10 C.F.R. 2.206 Petitions," does not meet the intent of the Energy Reorganization Act of 1974. The NGO alleged that the U.S. public "gets an unfair deal in the [10 C.F.R.] 2.206 petition process." According to the alleger, the NRC has granted "substantive relief" to only 2 of about 1,000 petitions filed from 1975 to 2012; 613 were rejected outright. In addition, the alleging NGO charged that the NRC has not addressed concerns identified by a 2020 NRC OIG Event Inquiry report regarding the Indian Point gas pipeline.

Background:

Under the process, members of the public can bring issues to the agency's attention, and the Commission, in response, may grant a request for action to modify, suspend, or revoke a license. The OIG audited the NRC's 2.206 petition process in 2017, finding that there was no periodic assessment of the process, and the petition review and rejection criteria were unclear. In September 2021, the NRC updated its desktop guide for the petition process partly in response to the OIG Audit report. In connection with the allegations, OIG investigators opened a new case to review several 2.206 petitions regarding the San Onofre Nuclear Generating Station's independent spent fuel storage installation.

Investigative Results:

The 10 C.F.R. 2.206 regulation has not substantively changed since its codification in 1974, yet MD 8.11 has been revised as recently as 2019, and the corresponding MD 8.11 desktop guide in 2021. Relevant information regarding the NRC's implementation of 2.206 petitions according to the agency's policy and regulation will be reported in the conclusion of a similar ongoing investigation, since that case relates to specific 2.206 petition concerns.

(Addresses Management and Performance Challenges #1 and #10)

Special Project: NRC Regulatory Oversight Involving Diablo Canyon

OIG Strategic Goal: Safety

Project Background:
This project was initiated on January 21, 2022, to identify investigative matters associated with the NRC's handling of technical regulatory issues involving safety and/or security significance at Diablo Canyon Nuclear Power Plant (DCNPP) that may impact the health and safety of the public.

Investigative Results:
We correlated many allegations and proactive reviews to this project, and monitored, developed, and dispositioned them accordingly. This project supported one investigation, and the OIG identified three concerns regarding emergency diesel generators that will be addressed in that case report:

(1) Allegations that NRC Region IV is covering up fuel leaks in emergency diesel generators (EDG) resulting from loose bolts on the fuel system that were identified during Problem Identification and Resolution inspections at DCNPP;

(2) Allegations that the NRC is being unduly influenced by the licensee and has not maintained an appropriate "arm's length" distance; and,

(3) Allegations that EDGs have consistently had mechanical failures, but the NRC's regular inspections of them yielded minimal findings.

We evaluated almost two dozen technical issues from previous allegations and investigations conducted from FY 2015 to FY 2022. We combined three sets of allegations regarding emergency diesel generators, ranging from fuel leaks resulting from loose bolts, regularly occurring mechanical failures, and undue influence from a licensee on the NRC into one investigation that will be addressed in a case report scheduled in FY 2023.

(Addresses Management and Performance Challenge #1)

Proactive Initiative: Computer Misuse and Computer Forensic Support

OIG Strategic Goal: Corporate Management

Project Background:

We initiated a project at the beginning of FY 2021 to identify any potential cases of intrusions into the NRC IT systems from both inside and outside of the agency, and other cyber-related incidents affecting NRC IT systems and employees.

Investigative Results:

The project resulted in numerous actions to include:

(1) The OIG's Cyber Crimes Unit (CCU) monitored an incident involving the Solarwinds software breach and ensured the NRC Office of the Chief Information Officer had all current information from the FBI and the Intelligence Community;

(2) OIG's CCU provided digital forensic support to the NRC's Office of Investigation to assist in discovering evidence of wrongdoing during a reportable event at a licensee location; and,

(3) Through its liaison with the NRC Office of the Chief Information Officer, OIG's CCU learned of several instances when sensitive internal information was spilled through internal email or because users had posted documents to the wrong SharePoint site. These spills were handled by the internal processes and monitored by the CCU to ensure proper mitigation.

In addition, the OIG has one of its CCU special agents assigned to the FBI Baltimore Field Office Cyber Task Force to monitor any targeted spear phishing or intrusion attempts, or any other cyber targeted activities, related to the mission of the NRC and DNFSB, to include their own systems. The OIG CCU-assigned special agent also assists the FBI Baltimore Field Office Cyber Task Force with its investigations as a member of the team. Additionally, the OIG CCU special agents actively participate in meetings of the Council of the Inspectors General on Integrity and Efficiency IT Sub-Committee, the Department of Justice Computer Crime and Intellectual Property Section, and the NRC Office of the Chief Information Officer to support governmentwide initiatives aimed at intrusions. This partnership enabled the OIG CCU special agents to stay abreast of current cyber threat trends and keep the agency informed of any potential threats to its systems.

(Addresses Management and Performance Challenges #5 and #9)

Potential Theft of NRC-Owned Laptop Computer and Government Property

OIG Strategic Goal: Corporate Management

Allegation:
We investigated an allegation from an NRC manager, who reported that a former NRC contractor had failed to return his NRC-issued laptop and PIV card when he was terminated from his position in November 2021. The alleger stated that a return box was sent to the contractor's home address, but that the items had not been received. The NRC stated it tracked the NRC-issued laptop, which it detected being used online, and it appeared to have been re-imaged to Windows 11.

Investigative Results:
We found that the contractor intentionally refused to return government property and converted the operating system for his own use after he was terminated from his position as a contractor for the OCIO. The employee acknowledged that he did not return the laptop because he felt "vindictive" about the circumstance of his removal. We executed a search warrant at the employee's premises and recovered the laptop and PIV card.

Impact:
The NRC property was retrieved, the contractor is no longer employed as an NRC contractor, and the contractor has been debarred from Executive Branch federal government contracts for three years.

(Addresses Management and Performance Challenge #5)

NRC Medical Service Contract Issue within the Office of Investigations

OIG Strategic Goal: Corporate Management

Allegation:
We investigated an allegation received from the NRC Office of Investigations (OI) that a contractor with the NRC had not fulfilled the requirements of its contract. The OI used the contractor to comply with requirements for agents to complete annual physical examinations. In

several instances, the contractor subcontracted the examinations. The OI reported to us that it had not received records related to the completion of the annual physical examinations that had been subcontracted out.

Investigative Results:

We did not substantiate the allegation, finding that neither the contractor nor the subcontractor violated regulations. A Senior Contracting Officer in the NRC's Office of Administration, Acquisition Management Division confirmed that the NRC Health Center had all relevant OI agents' physical examination records, to include those subcontracted out. Internal business disruption within the contractors caused the late production of the physical examination records, but the NRC was not invoiced for the examinations prior to receiving the examination records.

Upon review of the contract and testimony provided, we found the contractor met the terms of its contract with the NRC when it provided annual physical examinations to OI agents through its subcontractor, and subsequently produced appropriate records of the examinations.

(Addresses Management and Performance Challenge #5)

Allegation that Region II Management Knowingly Allowed Unauthorized Telework

OIG Strategic Goal: Corporate Management

Allegation:

We initiated this investigation after receiving an anonymous allegation claiming an NRC employee, who is ineligible for telework, could be circumventing the Telework Enhancement Act (TEA). The alleger stated that regional management may be complicit in the violation by allowing the employee to telework and approving his time and attendance.

Investigative Results:

Our investigation substantiated the employee violated the TEA and identified other travel-related misconduct as well as administrative issues; however, we did not find evidence that regional management was complicit in these violations.

Issue #1. Telework by ineligible individual

We found evidence that the employee worked remotely on various dates in 2021 while ineligible for telework under the TEA. The employee failed to notify his supervisor that he was working from home, except during

mandatory telework for the COVID-19 pandemic.

Issue #2. Region II not complicit in allowing unauthorized telework
We did not substantiate that regional management was complicit in allowing the employee unauthorized telework. Although regional management expressed a desire to allow the employee to telework and discussed the matter with the Office of the Chief Human Capital Officer, NRC, the request was denied and management directed the employee to return to in-person work at the regional office. Additionally, the employee stated that management was unaware he had worked from home and did not approve telework.

Issue #3. Travel routing and reservations violated policy
We substantiated that between January 2018 and July 2021, the employee violated federal and NRC travel policy on 18 occasions: 17 by indirect routing and 1 additional incident of routing not advantageous to the government. On 17 occasions, the employee improperly booked flights into and out of airports near his residence instead of his official duty station or temporary duty locations. The employee also overcharged the government for multiple modes of travel for personal benefit. Lastly, three of the eighteen incidents also involved claiming an improper TDY location with higher per diem rates.

Issue #4. Overpayment of travel voucher expenses
We found payment of per diem meals and incidental expenses (M&IE) for non-workdays during interrupted travel on nine of the employee's vouchers for travel between January 2018 and February 2020, totaling an overpayment of $3,867. Receipt of M&IE during interruption of travel is a violation of both federal and NRC travel policy. The employee denied intentionally requesting reimbursement for these expenses or knowledge that the funds were received. The employee stated he is willing and able to pay back the funds.

NRC's Response:
To address the findings, the NRC issued the employee a Notice of Proposed Removal for four charges of misconduct: inappropriate conduct, failure to follow travel procedures, failure to follow supervisory instructions, and lack of candor in an official investigation. This proposal notice was coordinated with the Office of the Chief Human Capital Officer and Office of the General Counsel. During the reply period, the employee chose to retire.

(Addresses Management and Performance Challenge #6)

Allegation Related to Oversight of NFPA 805 Program at Farley Nuclear Power Plant

OIG Strategic Goal: Safety

Allegation:

We received an allegation of misconduct that NRC management is unwilling "to recognize the seriousness of long-standing fire protection at Farley Nuclear Plant [FNP]." The alleger also raised concerns about multiple instances of code noncompliance relating to FNP's transition to National Fire Protection Association Standard 805, and suggested that fire protection experts from the Office of Nuclear Reactor Regulation address those concerns.

Investigative Results:

Our investigation did not substantiate the allegation of misconduct by NRC management, but we did identify potential safety concerns relating to the FNP service water intake structure (SWIS) pump rooms and fire probabilistic risk assessment (PRA). We recommended that certified fire protection engineers review these concerns and assess whether additional inspections or corrective actions are appropriate.

NRC's Response:

The staff reviewed additional information from the licensee and performed a site visit at the FNP. The staff identified issues associated with the installed fire mitigation structures in the SWIS pump room, how certain scenarios and target sets were captured in the base PRA model, and how the fire brigade response timing to the SWIS was captured in the base PRA model. The staff determined that there were no immediate safety concerns regarding these issues and has brought them to the attention of regional staff for follow-up through the Reactor Oversight Process, as appropriate.

(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 in 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. 3) 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 2023*   ***(As identified by the Inspector General)***
Challenge 1: *Leading a healthy and sustainable 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: *Continuing a systematic safety focus in the DNFSB's technical safety oversight and reviews.*
Challenge 4: *Strengthening the DNFSB's readiness to respond to future mission-affecting disruptions.*
Challenge 5: *Managing the DNFSB's efforts to elevate its visibility, credibility, and influence, and to assess and improve its relationship with the DOE and external stakeholders.*

** 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 in Fiscal Year 2023."*
https://nrcoig.oversight.gov/top- management-challenges

DNFSB AUDITS

Audit Summaries

Audit of the DNFSB's Fiscal Year 2022 Financial Statements

OIG Strategic Goal: Corporate Management

Under the Chief Financial Officers Act, the Government Management and Reform Act, and OMB Bulletin 21-04, Audit Requirements for Federal Financial Statements, the OIG is required to audit the DNFSB's financial statements.

The audit objectives were to:

- Express opinions on the agency's financial statements and internal controls;
- Review compliance with applicable laws and regulations; and,
- Review controls in the DNFSB's computer systems that are significant to the financial statements.

Audit Results:

CliftonLarsonAllen concluded that:

- The DNFSB's financial statements as of and for the FY ended September 30, 2022, are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles (GAAP);
- The DNFSB maintained, in all material respects, effective internal control over financial reporting as of September 30, 2022; and,
- No reportable noncompliance for FY 2022 with provisions of applicable laws, regulations, contracts, and grant agreements we tested and no other matters.

(Addresses Management and Performance Challenge #2)

Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB in Fiscal Year 2023

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, 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 2022 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

Enacted in 2020, the Payment Integrity Information Act of 2019 (PIIA) requires executive agencies to periodically review all programs and activities an agency administers and identify all programs and activities with outlays exceeding $10 million that may be susceptible to significant improper payments. The review should occur not less than once every 3 years for each program and activity. The PIIA requires the OIG of each executive agency to determine agency compliance annually.

The audit objectives are to assess the DNFSB's compliance with the PIIA and report any material weaknesses in internal control.

(Addresses Management and Performance Challenge #2)

Audit of the DNFSB's Freedom of Information Act Program

OIG Strategic Goal: Corporate Management

The Freedom of Information Act (FOIA), found at 5 U.S.C. § 552, grants every person the right to request access to federal agency records. Federal agencies are required to disclose records upon receiving a written request, with the exception of records that are protected from disclosure by one or more of the FOIA's nine exemptions. This right of access is enforceable in court.

The DNFSB makes many of its documents, such as agency regulations and policy statements, technical reviews, and reports to Congress, publicly available through its website. For documents that are not available through the website, people may submit FOIA requests by mail or email, or through the National FOIA Portal website.

The DNFSB is required to respond to a FOIA request within 20 business days of receiving a FOIA request, and the agency may pause the 20-day response period one time to seek information from a requester. FOIA requests are subject to variable fees, which can be waived under certain

circumstances. The DNFSB can pause the 20-day response period as long as necessary to clarify fee assessments.

During FY 2021, the DNFSB received 19 FOIA requests. The agency processed 18 requests, while 1 remained pending at the end of the fiscal year. The agency fully or partially granted 11 requests, while the remaining 7 were denied on grounds other than FOIA exemption criteria. Specifically, the DNFSB either had no records covered by the requests, or the requestors did not reasonably describe records sought. In one case, a request was withdrawn. The DNFSB allocated 0.5 FTE and approximately $50,000 to processing FOIA requests during FY 2021.

The audit objective is to assess the consistency and timeliness of the DNFSB's FOIA request decisions, and to assess the agency's effectiveness in communicating FOIA policies to FOIA requestors.

(Addresses Management and Performance Challenge #3)

Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023

OIG Strategic Goal: Corporate Management

The Federal Information Security Modernization Act (FISMA) was enacted in 2014. The FISMA outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. In addition, the FISMA includes provisions, such as those requiring the development of minimum standards for agency systems, that 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 to 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 audit objective is to assess the effectiveness of the information security policies, procedures, and practices of the DNFSB.

(Addresses Management and Performance Challenge #2)

DNFSB INVESTIGATIONS

Investigative Case Summary

Proactive Initiative: Computer Misuse and Computer Forensic Support

OIG Strategic Goal: Corporate Management

Project Background:
We initiated this project in October 2020 to identify potential cases involving network intrusions from unknown traffic and emails by internal and external sources and other cyber-related incidents affecting DNFSB IT systems and employees.

Investigative Results:
Selective actions under this project include the following:

(1) The DNFSB's migration to a website monitoring software system with greater capability to determine the specific websites users are attempting to access with DNFSB-furnished equipment even when not connected to the network.

OIG CCU special agents assigned to the Cyber Crimes Unit (CCU) reviewed the network traffic logs for DNFSB to determine if any users accessed unauthorized Internet websites via their government-issued devices. The DNFSB tracks all website access through a monitoring software system. The OIG found that although the monitoring system categorizes site users attempts to access, and blocks users from restricted sites, it does not record the name of each specific site.

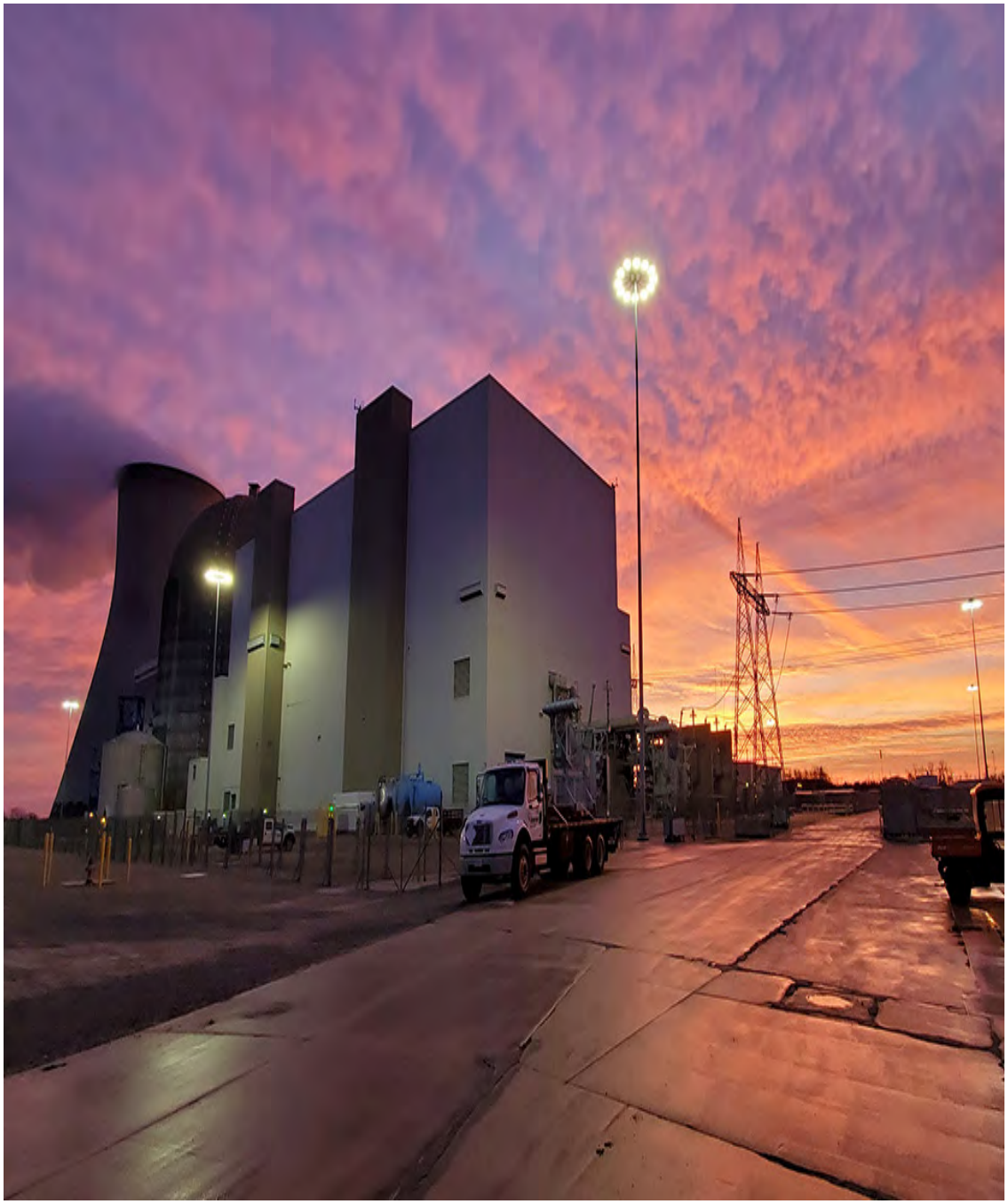
The DNFSB's CISO informed the CCU that the DNFSB was migrating to a different monitoring platform that would allow for better insight into what Internet sites users were attempting to access. The CISO notified the CCU that the new monitoring software had been deployed to all the users' workstations and would be able to monitor users' Internet activity even when not connected to the DNFSB network.

(2) The CCU has continued to build relationships with the Office of the General Manager and CISO staff members.

(3) This project provided information to support another project—Proactive Initiative to Identify Fraud within DNFSB Programs and Operations.

In addition, CCU special agents participated with the Federal Bureau of Investigations Baltimore Field Office Cyber Task Force, the Council of the Inspectors General on Integrity and Efficiency IT Sub-Committee, and the Department of Justice Computer Crime and Intellectual Property Section to support governmentwide initiatives aimed at intrusions.

(Addresses Management and Performance Challenge #2)



Callaway Nuclear Power Plant in Fulton, Missouri, at sunrise

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

October 1, 2022 – March 31, 2023

Complaints Received: 84 (49 received from the NRC OIG Hotline)

Investigative Statistics

Source of Complaints

NRC Employee	36
NRC Management	9
General Public	18
Other Government Agency	1
Anonymous	18
Contractor	1
Regulated Industry (Licensee/Utility)	0
OIG Proactive Initiation	1

Disposition of Complaints

Reviewed Complaint and Closed (no additional action needed)	30
Correlated to Existing OIG Investigation	7
Referred to New OIG Investigation	5
Referred to Audits	4
Referred to NRC Management for Action	23
Reviewing Complaint	15
Total:	**84**

Status of Investigations

Federal

DOJ Referrals	6
DOJ Declinations	5
DOJ Accepted	1
DOJ Pending	1
Criminal Convictions/Arrests	0
Criminal Information/Indictments	0
Civil/Administrative Recovery	1

Civil Recovery Amount - $ 742,500.00

State and Local

State and Local Referrals	0

NRC Administrative Actions

Review and/or Change of Agency Process	2
Letter of Reprimand	1
Pending Agency Action	1
Termination or Retired in lieu of Proposed Termination	2

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	2	2	1	1	2
Event Inquiry	2	0	2	0	0
Internal Fraud	1	0	0	0	1
Management Misconduct	6	4	2	0	6
Miscellaneous	1	0	1	0	0
Nuclear Regulatory Actions	4	2	2	0	4
Theft	1	0	1	0	0
Whistleblower Reprisal	2	0	1	0	1
External Fraud	3	1	1	0	3
False Statements	1	1	1	0	1
TOTAL:	**23**	**10**	**12**	**1**	**18**

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

NRC Audits Completed

Date	Title	Audit Number
11/10/2022	Audit of the NRC's Financial Statements for Fiscal Year 2022	OIG-23-A-02
10/28/2022	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC in Fiscal Year 2023	OIG-23-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	5	$2,295,007	0
B. Which were issued during the reporting period	0	$0	0
Subtotal (A + B) ‡	5	$2,295,007	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	5	$2,295,007	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.*

‡ 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, 2022 – March 31, 2023

Complaints Received from the DNFSB OIG Hotline: 2

Investigative Statistics

Source of Complaints

DNFSB Employee	1
DNFSB Management	n/a
General Public	n/a
Anonymous	1
Contractor	n/a
TOTAL:	**2**

Disposition of Complaints

Correlated to Existing Case	1
Referred to OIG Investigations	n/a
Referred to OIG Audit	n/a
Referred to DNFSB Management	n/a
Reviewing Complaint	1
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

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
Review of Agency Process	1

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	1	0	1	0	0
Management Misconduct	2	0	0	0	2
Proactive Initiatives	1	0	1	0	0
TOTAL:	**4**	**0**	**2**	**0**	**2**

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

DNFSB Audits Completed

Date	Title	Audit Number
11/30/2022	Results of the Audit of the DNFSB's Financial Statements for Fiscal Year 2022	DNFSB-23-A-02
10/28/2022	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB in Fiscal Year 2023	DNFSB-23-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 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.

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 the 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)

2 of 13 recommendations open since June 2, 2020

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 Property Management Program (OIG-20-17)

5 of 7 recommendations open since September 30, 2020

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 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.

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)

10 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, 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 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 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)

1 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.

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.

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)

14 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 (a) aggregate security risks, (b) normalize cybersecurity risk information across organizational units; and, (c) 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 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 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 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)

1 of 4 Recommendations open since January 19, 2022

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

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

5 of 8 Recommendations open since February 9, 2022

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

Recommendation 4: Clearly define CFSI.

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.

Audit of the NRC's Drop-In Meeting Policies and Procedures (OIG-22-A-12)

4 of 4 Recommendations open since August 12, 2022

Recommendation 1: Develop and publish a public description of the purposes and benefits of, and the controls on, the drop-in meeting process.

Recommendation 2: Develop guidance to systematize practices across the agency for consistently informing technical staff about drop-in meetings, both before and after the meetings.

Recommendation 3: Develop guidance to systematize practices across the agency for consistently including staff observers as part of staff development and training efforts.

Recommendation 4: Once the new guidance is developed, train all managers on the new guidance and controls for drop-in meetings and related interactions with external stakeholders.

Audit of the NRC's Strategic Workforce Planning Process (OIG-22-A-13)

3 of 3 Recommendations open since September 26, 2022

Recommendation 1: Update the *Enhanced Strategic Workforce Planning: Office Director and Regional Administrator* Guidance to provide specific methodologies, detailed instructions, measurement criteria, and scales that can be used to estimate the anticipated level of workload change, ranking of position risk factors, and prioritization of workforce gaps or surpluses.

Recommendation 2: Update the *Enhanced Strategic Workforce Planning: Office Director and Regional Administrator Guidance* to incorporate attrition rates so that the agency quantifies and considers non-retirement separations in workforce planning.

Recommendation 3: Update agency policy and procedures to include Human Capital Operating Plan information—specifically, information regarding the periodicity of the plan's review, approval, and updating—in accordance with the Office of Personnel Management's *Human Capital Operating Plan Guidance: Fiscal Years 2022-2026*.

Audit of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2022 (OIG-22-A-14)

7 of 7 Recommendations open since September 29, 2022

Recommendation 1: Review and update the ITI Core Services SSP System Interconnections tab and related security control implementation to ensure system interconnection details reflect the current system environment.

Recommendation 2: Implement a process to verify that remaining external interconnections noted in the ITI Core Services SSP have documented, up-to-date ISA/MOUs or SLAs in place as applicable.

Recommendation 3: Update the ITI inventory to correct any discrepancies and incorrect information listed for ITI devices tracked in the Common Computing Services, Peripherals, Unified Communications and Voice over Internet Protocol subsystem inventories.

Recommendation 4: Document and implement a periodic review of subsystem inventories to verify information maintained for each ITI subsystem is current, complete and accurate.

Recommendation 5: Implement a process to document the supply chain risk management requirements within the NRC information systems' system security plans.

Recommendation 6: Implement a process to validate that all personnel with privileged level responsibilities complete annual security awareness and role-based training.

Recommendation 7: Implement a process to validate that all new contractors complete their initial security training requirements and acknowledgement of rules of behavior prior to accessing the NRC environment and to subsequently ensure completion of annual security awareness training and renewal of rules of behavior is tracked.

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)

14 of 14 recommendations open since March 25, 2021

Recommendation 1: Define an ISA in accordance with the Federal Enterprise Architecture Framework.

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; and,
(d) Conduct a supply chain risk assessment.

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 4: Finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. Continue ongoing efforts to apply the Track-It!, ForeScout and KACE solutions.

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.

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)

24 of 24 recommendations open since December 21, 2021

Recommendation 1: Update the ISA and use the updated ISA to:
(a) Assess enterprise, business process, and information system level risks; and,
(b) Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.

Recommendation 2: Using the results of Recommendation 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 [comply] (sic) 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, [so that they] (sic) 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.

Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2022 (DNFSB-22-A-07)

8 of 11 Recommendations open since September 29, 2022

Recommendation 1: Implement a process to ensure a security control assessment for the DNFSB GSS is completed and documented on an annual basis.

Recommendation 2: Implement a process to validate the DNFSB GSS security authorization is maintained in accordance with DNFSB policy.

Recommendation 3: Enforce existing DNFSB policy requirements to document security impact analyses, test plans, test results and backout plan requirements for each change.

Recommendation 4: Complete the implementation and consistent performance of monthly reviews to ensure security impact analyses, test plans, test results and backout plans are documented as required for each change.

Recommendation 5: Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.

Recommendation 6: Update the current change process, the Track-It! Tool, or both, to enforce segregation of duties controls for a requester and an approver of a change (e.g., requiring a second approver signature for all non-emergency changes, when the requester is eligible to be an approver).

Recommendation 7: Create procedures for vulnerability and compliance management based on risk and level of effort involved to mitigate confirmed vulnerabilities case-by-case such as:

(a) Prioritizing mitigation in accordance with all requirements specified by CISA BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities and Emergency Directives, as applicable;
(b) Opening plans of action and milestones to track critical and high vulnerabilities that cannot be addressed within 30 days; and,
(c) Preparing risk-based decisions in unusual circumstances when there is a technical or cost limitation making mitigation of a critical or high vulnerability infeasible with documented, effective compensating controls coupled with a clear timeframe for planned remediation.

Recommendation 10: Document and implement system and information integrity and systems and communications protection policies and procedures in accordance with DNFSB policy.

ABBREVIATIONS AND ACRONYMS

CCU	Cyber Crimes Unit
C.F.R.	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CLA	CliftonLarsonAllen
DCNPP	Diablo Canyon Nuclear Power Plant
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
EDG	Emergency Diesel Generator
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GAO	Government Accountability Office
GLINDA	Global Infrastructure and Development Acquisition
COVID-19	Coronavirus Disease of 2019
IAM	Issue Area Monitoring
IG	Inspector General
IT	Information Technology
MD	Management Directive
NGO	Non-Governmental Organization
NRC	Nuclear Regulatory Commission
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OEDO	Office of the Executive Director for Operations
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act of 2019
PIV	Personal Identity Verification
SwRI	Southwest Research Institute
TEA	Telework Enhancement 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 O12- A12
11555 Rockville Pike
Rockville, MD 20852-2738