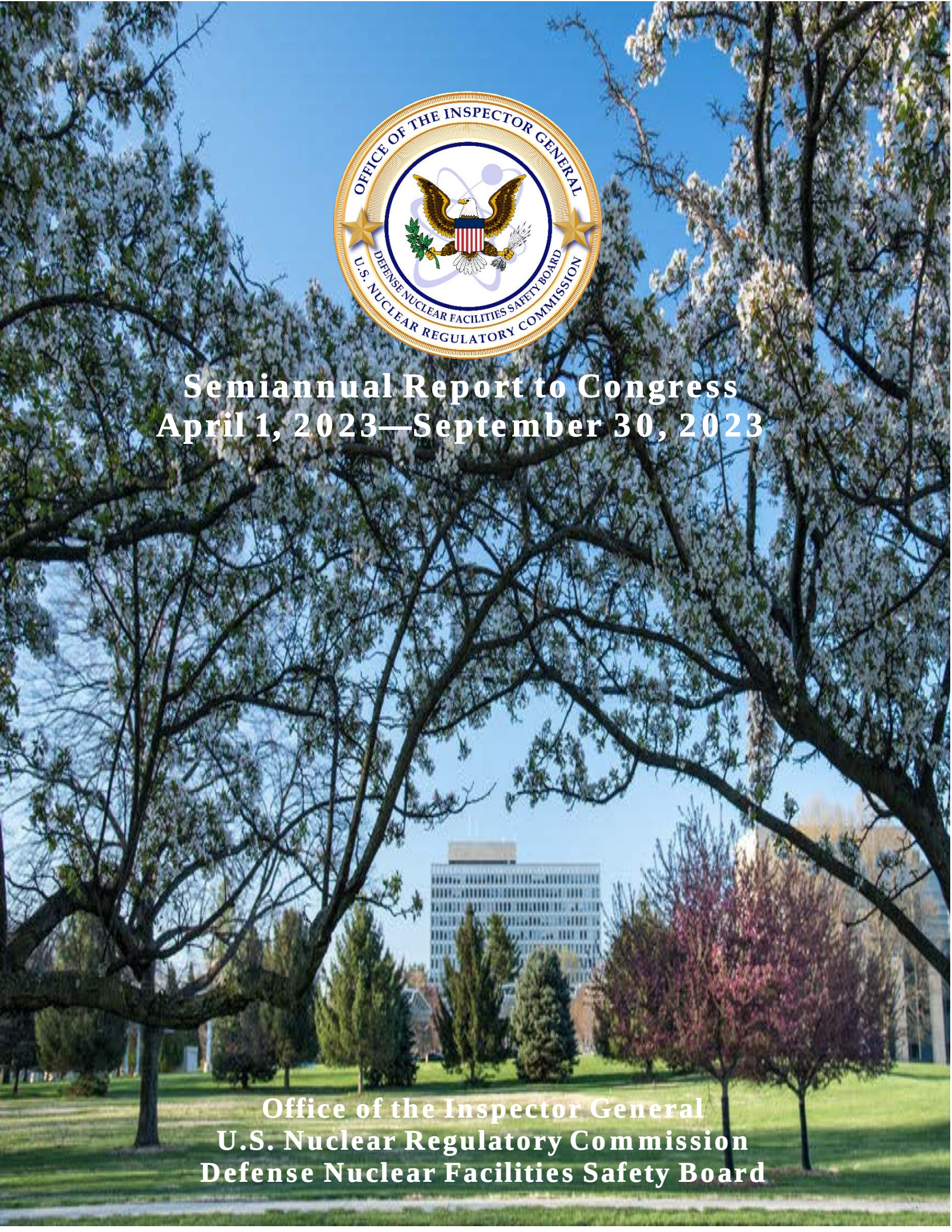


Semiannual Report to Congress
April 1, 2023—September 30, 2023

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:

National Institute of Standards and Technology
Gaithersburg, Maryland

A MESSAGE FROM THE INSPECTOR GENERAL

On behalf of the Office of the Inspector General, U.S. Nuclear Regulatory Commission (NRC) and Defense Nuclear Facilities Safety Board (DNFSB), it is my pleasure to present this Semiannual Report to Congress, covering the period from April 1, 2023, to September 30, 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 issued eleven audit and evaluation reports, and recommended several ways to improve NRC and DNFSB safety, security, and corporate management programs. We also opened twenty-nine investigative cases and completed twenty, one of which was referred to the Department of Justice, and six of which were referred to NRC and 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 compliance with the Payment Integrity Information Act, voluntary leave transfer program policies and procedures, Federally Funded Research and Development Center contract requirements, irretrievable well logging source abandonment procedures, reactive inspection teams deployment processes, and vacancy announcements processes; as well as the DNFSB's compliance with the Payment Integrity Information Act. Further, this report includes summaries of cases involving the NRC's oversight of research and test reactors, diesel generators at Diablo Canyon Nuclear Power Plant, inspection concerns at spent fuel storage installations, concerns of discrimination against Army veterans, and a potential violation of the agency's prohibited securities rule, as well an alleged contract violation involving DNFSB leadership and separate allegations that DNFSB leadership took actions inconsistent with the delegation of functions required by the Atomic Energy Act.

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

Robert J. Feitel

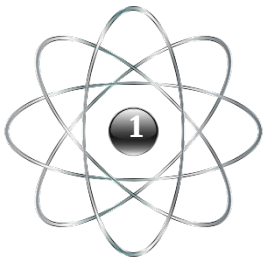
Robert J. Feitel
Inspector General

Highlights

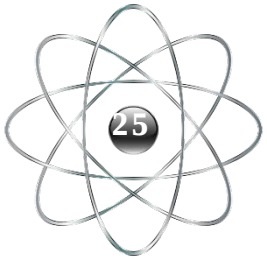
OFFICE of AUDITS

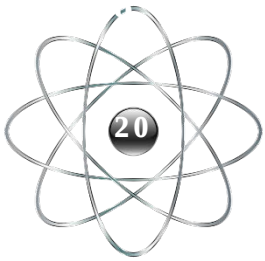
2
Reports Issued

9
Reports Issued

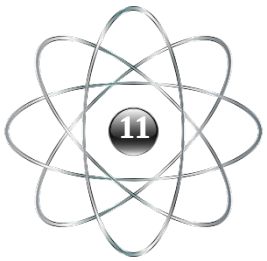


Recommendations Made





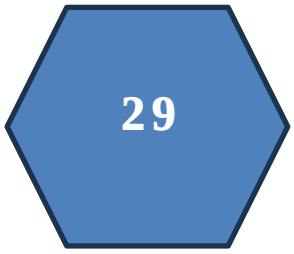
Recommendations Closed



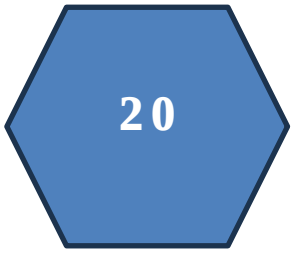
Highlights

OFFICE of INVESTIGATIONS

Open Investigations



Closed Investigations



CONTENTS

Radiation workers at a research reactor

Audit/Investigation Synopsis

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 U.S. Nuclear Regulatory Commission (NRC) Voluntary Leave Transfer Program (VLTP) helps ease the financial burden of employees during periods of personal or family medical emergencies. NRC employees may donate annual leave, on a confidential and voluntary basis, to employees who face financial hardship because of personal or family illness. An employee who has been affected by a medical emergency may apply to become a leave recipient. Given the potential for error or abuse, effective controls are essential to the leave transfer program to ensure integrity and accountability. The Office of the Inspector General (OIG) assessed the extent to which the NRC has established effective policies, procedures, and controls for managing its VLTP.

- Since 1987, the NRC has contracted to operate a Federally Funded Research and Development Center (FFRDC), with the principal focus to provide support for the NRC's activities in licensing a deep geologic repository for high-level waste and spent nuclear fuel. The NRC recently renewed the FFRDC contract for the seventh time. The OIG reviewed the contract renewal to determine if the NRC properly considered all Federal Acquisition Regulation (FAR) requirements for an FFRDC review in preparing its renewal justification, and adequately fulfills its contract oversight responsibilities for the FFRDC.

- The NRC conducts reactive inspections in response to events that may have compromised the safety or security at nuclear power plants. Inspection of significant events is a formal process conducted for the purpose of accident prevention. The process includes gathering and analyzing information; determining findings and conclusions, including the cause(s) of a significant

event; and, disseminating the investigation results for the NRC, industry, and public review. Incidents must be examined against deterministic criteria and risk assessment criteria when deciding on the appropriate level of reactive inspection response. The OIG assessed the consistency with which the NRC follows agency guidance for deploying special, augmented, and incident inspection teams in response to safety and security incidents at nuclear power plants.

- 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 three years for each program activity. The PIIA also requires the OIG of each executive agency to annually determine agency compliance. The OIG assessed the NRC's compliance with the PIIA.

- 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. If a licensee has an irretrievable well logging source, the licensee must notify the NRC to obtain approval to implement abandonment procedures. The OIG reviewed the adequacy of the NRC's handling and processing of irretrievable well logging source abandonments.

- The NRC posts vacancies through vacancy announcements and public notices. The NRC fills vacant positions by recruiting eligible candidates from within the agency or by recruiting from outside the agency through the appropriate sources. Vacancy announcements and public notices include an open period to provide applicants with a reasonable time to apply, and for the NRC to collect enough applications. The open period may differ based on the type of vacancy. The OIG assessed whether the NRC

provides adequate time for job applicants to compete for positions, to identify opportunities for improvement in the vacancy announcement process.

- The Federal Information Security Modernization Act (FISMA) of 2014 established information security management requirements for agencies, including the requirement for an annual independent assessment by each agency's IG. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security. The OIG contracted with CliftonLarsonAllen (CLA) to conduct an independent audit of the NRC's overall information security program and practices in response to the FY 2023 IG FISMA Reporting Metrics.

Defense Nuclear Facilities Safety Board

- The PIIA requires each executive agency to periodically review all programs and activities the 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 three years for each program activity. The PIIA also requires the OIG of each executive agency to annually determine whether the agency is in compliance with the act's requirements. The OIG assessed the DNFSB's compliance with the PIIA.

- The FISMA of 2014 established information security management requirements for agencies, including the requirement for an annual independent assessment by each agency's IG. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security. The OIG contracted with CLA to conduct an independent audit of the DNFSB's overall information security program and practices in response to the FY 2023 IG FISMA Reporting Metrics.

Investigations

U.S. Nuclear Regulatory Commission

- The OIG initiated a special inquiry following a radioactive release to the environment from a National Institute of Standards and Technology (NIST) test reactor on February 3, 2021. The special inquiry's focus broadened from the NIST event to include consideration of the NRC's oversight of other research and test reactor (RTR) facilities to assess potential systemic issues. The OIG found that inadequate RTR oversight led to a failure to identify and correct problems not only with the NIST test reactor but also with other RTRs.

- The OIG received concerns from an NRC employee, Congressional staff, and other stakeholders about inspections of independent spent fuel storage installations (ISFSIs). The OIG conducted a special inquiry and found that Region II's past inspection practices resulted in missed opportunities to identify violations of plant processes for loading spent fuel into dry cask storage. While the OIG did not identify an immediate safety concern related to ISFSIs, the OIG found that a significant number of loaded casks still had not received adequate NRC inspections to ensure licensees met regulatory requirements for long-term storage and retrievability. The NRC responded to the report by agreeing that there was no immediate safety concern and further stating that the agency has reasonable assurance of long-term safety of ISFSIs. The NRC response focused on the new inspection program implemented in January 2021, however, which was not the OIG's concern. The agency also failed to provide a complete explanation for why Region II inspections of ISFSI repeat-loading campaigns took, on average, significantly less time—only approximately 20% of the hours—than those projected in the agency's own inspection guidance.

- The OIG initiated an investigation based on three sets of allegations regarding all six emergency diesel generators at Diablo Canyon Nuclear Power Plant. The OIG did not substantiate alleged misconduct by NRC staff nor did it find that NRC inspectors and licensee staff tried to conceal problems with the

generators. Following the OIG's initiation of the investigation, NRC inspectors issued findings regarding leaking generators at Diablo Canyon.

- The OIG received an allegation that the NRC Office of Investigations (OI) was discriminating against individuals who were Army veterans and criminal investigators in the Army, due to the training they received allegedly not meeting minimum requirements for a criminal investigator position at the NRC.

- The OIG initiated an investigation based on an allegation that an employee had violated 5 Code of Federal Regulations (C.F.R.) 5801.102, which prohibits "covered" NRC employees—that is, employees with substantive regulatory responsibilities—from owning stocks, bonds, and other security interests issued by major entities in the commercial nuclear field. The spouses and minor children of covered employees are also prohibited from owning these stocks.

- The OIG opened a proactive investigation to determine whether counterfeit, fraudulent, or suspect breakers may have entered the supply chain at commercial nuclear power plants based on concerns from a manufacturer of breakers used in nuclear power plants. The OIG coordinated with other federal law enforcement entities in reviewing various threshold investigative issues.

Defense Nuclear Facilities Safety Board

- The OIG initiated an investigation based on an allegation that the Defense Nuclear Facilities Safety Board (DNFSB) Chair failed to appropriately delegate administrative functions to the Office of the Executive Director (EDO) as required by the Atomic Energy Act.

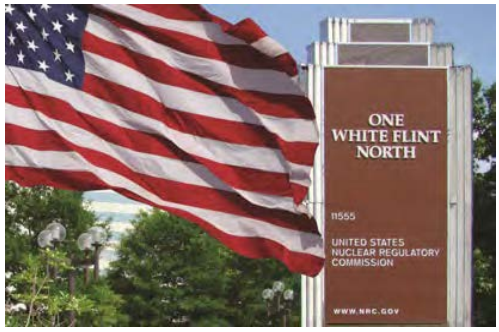
- The OIG initiated an investigation based on an allegation that the DNFSB Chair had ordered a contractor to do work outside of a contract's scope of work and without appropriate supervision. During the investigation, the OIG considered an additional concern that the Chair had allegedly violated the FAR by inappropriately providing an evaluation of the contract employee to the contractor's program manager.

The Inspector General and Assistant Inspectors General convened in Vienna, Austria, for the International Conference on Nuclear Decommissioning, hosted by the International Atomic Energy Agency.

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; 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 the media 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 OIG for the NRC was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendment to the IG Act. The Consolidated Appropriations Act of 2014 (Public Law 113–76) later authorized the OIG to also oversee the DNFSB. The OIG's mission is to provide independent, objective audit and investigative oversight of the operations of the NRC and the DNFSB, in order to protect people and the environment.

The OIG is committed to ensuring the integrity of both NRC and DNFSB 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 Strategic Plans that include the major challenges and critical risk areas facing the NRC and the DNFSB. The plans identify the OIG's priorities and establish 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.

The National Institute of Standards and Technology administrative building in Gaithersburg, Maryland

OIG PROGRAMS AND ACTIVITIES

Audit Program

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

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

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

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

- **Resolution** – Positive change results from the resolution process in which management takes action to improve operations based on the recommendations in the published audit report. Management actions are monitored until final action is taken on all recommendations. When management and the OIG cannot agree on the actions needed to correct a problem identified in an audit report, the issue can be taken to the NRC 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 alleged misconduct by employees and contractors, interfacing with the U.S. Department of Justice on OIG-related criminal and civil matters, and coordinating investigations and other OIG initiatives with federal, state, and local investigative agencies, and other OIGs.

Investigations may be initiated as a result of allegations or referrals from private citizens; licensee employees; government employees; Congress; other federal, state, and local law enforcement agencies; OIG audits; the OIG Hotline; and, OIG initiatives directed at areas bearing a high potential for fraud, waste, and abuse.

Because both the NRC's and the DNFSB's missions involve protecting the health and safety of the public, the OIG's Investigative Program directs much of its resources and attention to investigating allegations of NRC or DNFSB staff conduct that could adversely impact matters related to health and safety. These investigations may address allegations of:

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

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

- Failure by the agency 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 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 agencies' 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's 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 April 1, 2023 to September 30, 2023, the OIG reviewed a variety of regulatory documents. In its reviews, the OIG remained cognizant of how the proposed rules or policies could affect the OIG's functioning or independence. The OIG also considered whether the rules or policies could significantly affect NRC or DNFSB operations or be of high interest to NRC or DNFSB staff and stakeholders. In conducting its reviews, the OIG applied its knowledge and awareness of underlying trends and overarching developments at the agencies and in the areas they regulate.

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

NRC Management Directives

- MD 3.11, *Conferences*, which sets forth policies applying to the NRC's participation in or sponsorship of various types of conferences. The OIG reviewed proposed changes to the MD that were intended to capture recent Office of Management and Budget (OMB) policy statements, as well as changes recognizing that conferences may now include virtual and hybrid gatherings. The OIG found that the proposed changes to the MD were adequately supported, although we also recommended that the NRC clarify that the agency procedures in the MD do not apply to the OIG, which has independent budget authority and separate approval processes that apply to conference participation.

- MD 7.9, *Ethics Approvals and Waivers*, which establishes policies NRC employees must follow before engaging in certain activities, or accepting certain gifts or awards, that are covered by federal ethics rules or the NRC's supplemental ethics rules. The NRC's proposed revisions to this MD were intended to clarify the agency designee for considering various waivers and authorizations, as well as provide additional guidance on the approval standards and the factors that may be considered for these waivers and authorizations. The OIG's comments on this MD included recommendations to clarify certain terms and better align them with regulatory language. The OIG also recommended adding a citation to the Ethics in Government Act that reflected the act's recodification at 5 U.S.C. §§ 13,101–13,146.

- MD 7.12, *Enforcement of Post-Employment Restrictions*, which is designed to ensure that NRC employees are aware of the ethics restrictions in 5 C.F.R. Part 2641 before leaving government service, understand what types of actions may be taken to enforce those restrictions, and know how to report suspected violations to the appropriate authorities. The NRC's proposed revisions to this MD were intended to clarify the types of actions the agency may take in response to a suspected violation of the post-employment rules. The OIG discussed this matter with NRC attorneys and agreed that, consistent with the policies of the Office of Government Ethics (OGE) and the NRCs practical experience in this area, certain provisions referring to agency administrative hearings could be removed. The OIG also provided recommendations for clarifying text in the MD that refers to OIG investigatory reports and certain ethics standards.

- MD 13.1, *Property Management*, which establishes the NRC's policies for managing property in its possession or its contractors' possession. The NRC's proposed revisions to this MD were intended to clarify the requirement for offices to maintain internal control procedures for property items valued under $2,500, the role of the agency's Office of the Chief Information Officer in maintaining NRC-owned IT assets, and the guidance applicable to employees when managing and reporting on newly acquired property. In addition, the proposed revisions addressed the recommendations for improvement the OIG had made in reports OIG-17-A-27, *Evaluation of NRC's Management of Government Cell Phones*, and OIG-20-A-17, *Audit of the NRC's Property Management Program*. The OIG closely reviewed all revisions to the MD, and in particular the revisions addressing the OIG's audit recommendations. The OIG concluded that the revisions to the MD generally aligned with our recommendations in both audit reports, and we did not identify any conflicts with those recommendations.

- The OIG also reviewed the following MDs or other guidance documents during the period covered by this Semiannual Report: MD 4.5, *Contingency Plan for Periods of Lapsed Appropriations*; MD 7.1, *Tort Claims Against the United States*; MD 7.2, *Claims for Personal Property Loss*; MD 8.8, *Management of Allegations*; MD 9.3, *Organization and Functions, Advisory Committee on Reactor Safeguards*; MD 9.7, *Organization and Functions, Office of the General Counsel*; MD 9.14, *Organization and Functions, Office of International Programs*; MD 9.19, *Organization and Functions, Office of Enforcement*; MD 10.77, *Employee Development and Training*; MD 10.138, *Reduction in Force in the Senior Executive Service*; MD 12.2 *NRC Classified Information Security Program*; and Draft Classification Guide NRC-PS-1, *Classification and Designation Guide for NRC Protection and Security Information*. While the OIG provided editorial or formatting suggestions for some of these directives or guidance documents, we had no substantive comments on these documents.

DNFSB Directives

None for this period

Experiment facility at the NIST-Gaithersburg, Maryland

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 effective acquisition, management, and protection of information technology and data.*
Challenge 6: *Implementing strategic workforce planning during transformation and industry change.*
Challenge 7: *Overseeing 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-23-A-01, "The Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in Fiscal Year 2023." https://nrcoig.oversight.gov/top-management-challenges*

NRC AUDITS

Audit Summaries

Audit of the NRC's Voluntary Leave Transfer Program

OIG Strategic Goal: Corporate Management

The NRC's Voluntary Leave Transfer Program (VLTP) helps ease the financial burden of employees during periods of personal or family medical emergencies. NRC employees may donate annual leave, on a confidential and voluntary basis, to employees who face financial hardship because of personal or family illness. An employee who has been affected by a medical emergency may apply in writing to become a leave recipient. Given the potential for error or abuse, effective controls are essential to the leave transfer program to ensure integrity and accountability.

The audit objective was to determine the extent to which the NRC has established effective policies, procedures, and controls for managing its VLTP.

Audit Results:

The OIG found that the VLTP supports employees who need additional leave for medical emergencies. However, the NRC does not comply with federal regulations governing supporting documentation for VLTP applications. Specifically, required documentation supporting some leave recipients' eligibility is missing or unsigned because policies and procedures for managing the VLTP are decentralized, outdated, and implemented inconsistently. This increases the risk of leave resource mismanagement and inequitable treatment of VLTP participants. VLTP participants' enrollment and termination data show discrepancies across different agency data sources because agency staff does not perform quality assurance checks to validate the data. The resultant data reliability risks can impair program management and stewardship of leave resources.

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Corporate Management

Since October 1987, the NRC has contracted to operate an FFRDC, with the principal focus to provide support for the NRC's activities in licensing a deep geologic repository for high level waste and spent nuclear fuel. The current contract is the NRC's seventh renewal of the FFRDC contract. FAR Section 35.017-4 requires, prior to extending a contract for an FFRDC, a sponsoring agency must conduct a comprehensive review of the use and need for the facility.

The audit objectives were to determine if the NRC is (1) properly considering all FAR requirements for an FFRDC review in preparing its renewal justification; and, (2) adequately fulfilling its oversight responsibilities for the FFRDC.

Audit Results:

The OIG found that, although all FFRDC renewal FAR requirements were satisfied, the NRC's administration of the FFRDC contract relating to the final invoice billing is inadequate. The NRC requested that the contractor delay sending final invoices until requested to do so by the Contracting Specialist, because the NRC lacks resources related to closeout of cost-reimbursement contracts. The contractor now claims that the NRC owes $599,414 on tasks completed between fiscal years 2011 and 2021. The NRC on its own initiative issued an extension of the 120-day period for submitting invoices covering that period, even though the relevant FAR section, 52.216-7(d)(5), does not provide clear authority for the agency to take such action without a request from the contractor. This increases the risk of claims that funds are subject to the Prompt Payment Act, potential billing discrepancies not being identified or corrected in a timely manner, and old contract funds being unavailable for payment. The report made recommendations to improve the final invoice billing and closeout process.

(Addresses Management and Performance Challenge #8)

The Defense Contract Audit Agency's (DCAA) Audit Report Numbers 1431-2019L10100001 & 1431-2020L10100001

OIG Strategic Goal: Corporate Management

The OIG and the Defense Contract Audit Agency (DCAA) have an interagency agreement whereby the DCAA provides contract audit services for the OIG. The DCAA is responsible for the audit methodologies used to reach an audit's conclusions, monitoring its staff's qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute a completed audit report to NRC management and follow up on agency actions initiated as a result of the audit.

The audit objective was to determine if the NRC contract costs are reasonable, allowable, and allocable.

Audit Results:

At the request of the NRC, the DCAA audited Numark Associates, Inc., and provided the OIG with an audit report. The DCAA audit report, dated May 5, 2023, identified questioned costs to be addressed by NRC management.

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Safety

The NRC conducts reactive inspections in response to events that may have compromised the safety or security at nuclear power plants. Inspection of significant events is a formal process conducted for the purpose of accident prevention. The process includes gathering and analyzing information; determining findings and conclusions, including the cause(s) of a significant event; and, disseminating the investigation results for the NRC, industry, and public review. Incidents must be examined against deterministic criteria and risk assessment criteria when deciding on the appropriate level of reactive inspection response.

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 in response to a significant event. 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 incident inspection teams.

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

Audit Results:
The OIG found inconsistent completion and profiling of reactive inspection screening evaluation forms, and that reactive decision-making information is not shared with the public. Moreover, the OIG found that the NRC does not have clear and consistent reactive inspection screening guidance and has not assessed the effectiveness of its guidance in this area.

(Addresses Management and Performance Challenge #1)

Audit of the NRC's Compliance with the Requirements of the Payment Integrity Information Act of 2019 in Fiscal Year 2022

OIG Strategic Goal: Corporate Management
The Payment Integrity Information Act (PIIA) requires each agency to annually estimate its improper payments. The PIIA also requires federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. In addition, the PIIA requires the OIG of each agency to determine whether the agency complies with the PIIA and submit a report on that determination. The OIG, therefore, engaged with CLA to perform the assessment of the NRC's compliance with the PIIA.

The objectives of this audit were to assess the NRC's compliance with the PIIA and report any material weaknesses in internal control.

Audit Results:
CLA concluded that the NRC complied with the PIIA in accordance with OMB Memorandum 21-19, which establishes standards for payment integrity improvement.

(Addresses Management and Performance Challenge #8)

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. Part 39 in Title 10 of the C.F.R. prescribes the requirements for license issuance and radiation safety requirements for well logging. Under the Part 39 regulations, if a licensee has an irretrievable well logging source, the licensee must notify the NRC to obtain approval to implement abandonment procedures.

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

Audit Results:

The NRC's handling and processing of irretrievable well logging source abandonments are generally aligned with the agency's regulations; however, the NRC has not developed standard guidance for handling irretrievable well logging source abandonment notifications, and there is inconsistent documentation of irretrievable well logging source abandonment notifications and licensee reports. This has resulted in inconsistencies and inefficiencies in the abandonment notification process, and the possibility of ineffective oversight of these abandonments.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Vacancy Announcement Process

OIG Strategic Goal: Corporate Management

The NRC faces a significant hiring challenge. The NRC fills vacant positions by recruiting eligible candidates from within the agency or by recruiting from outside the agency through appropriate sources. The NRC posts vacancies through vacancy announcements and public notices. Vacancy announcements and public notices include an open period to provide applicants with a reasonable time to apply, and for the NRC to collect enough applications. The open period may differ based on the type of vacancy.

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

Audit Results:

The OIG found that the NRC provides adequate time for job applicants to compete for open positions; however, vacancy announcement data maintained by the Office of the Chief Human Capital Officer is incomplete and not easily retrievable. NRC staff do not consistently enter data into the Workforce Transformation Tracking System, and, as a result, the NRC's hiring process may be weakened. Further, the NRC's hiring managers do not have a consistent understanding of Direct Hire Authority (DHA) requirements, because DHA requirements are not included in NRC policy. Consequently, the NRC may not be effectively using DHA to address hiring challenges.

(Addresses Management and Performance Challenge #6)

U.S. Nuclear Regulatory Commission's Vulnerability Assessment and External Penetration Test

OIG Strategic Goal: Security

The FISMA outlines the information security management requirements for federal agencies, which includes an annual independent evaluation of the agency's information security program and practices to determine their effectiveness. The FISMA requires the annual evaluation to be performed by the agency's OIG or by an independent auditor. The NRC OIG retained CLA, to perform the fiscal year 2023 FISMA audit, including conducting an external vulnerability assessment and penetration test of the NRC's information system environment in support of the NRC's FY 2023 FISMA audit.

The audit objective was to assess the NRC's technical configuration and security controls by performing coordinated network and host-based security tests supporting the NRC's FY 2023 FISMA audit.

Audit Results:

During the vulnerability assessment and external penetration test, CLA identified weaknesses that if remediated would help strengthen the NRC's security posture. The OIG made two recommendations to assist the NRC in continuing to strengthen the vulnerability management program.

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

Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2023

OIG Strategic Goal: Corporate Management

The FISMA of 2014 established information security management requirements for agencies, including the requirement for an annual independent assessment by each agency's IG. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security. The OIG contracted with CLA to conduct an independent audit of the NRC's overall information security program and practices in response to the FY 2023 IG FISMA Reporting Metrics.

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

Audit Results:

CLA concluded that the NRC implemented effective information security policies, procedures, and practices. However, CLA noted new and repeat weaknesses in its security program related to the risk management, supply chain risk management, configuration management, identity and access management, security training, incident response, and contingency planning domains of the FY 2023 IG FISMA Reporting Metrics. CLA made recommendations to assist the NRC in strengthening its information security program.

(Addresses Management and Performance Challenge #5)

Audits in Progress

Audit of the NRC's Contract Management of Information Technology

OIG Strategic Goal: Corporate Management

The NRC offers various information technology (IT) services and support to employees. These services are acquired under the Global Infrastructure and Development Acquisition (GLINDA) initiative/contract. Commencing in June 2017, GLINDA is a blanket purchase agreement (BPA) with 6 awardees with a total of 11 BPA calls issued against them for various 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 is efficiently and effectively managing IT related contracts for the agency's information technology services and support.

(Addresses Management and Performance Challenge #5)

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 U.S. 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 quantity 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 quantity 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 quantity 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 quantities 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 quantities are subject to Part 37's requirements since Category 3 through 5 quantities are not considered to be as dangerous.

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

(Addresses Management and Performance Challenge #7)

Audit of the NRC's 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 and Performance Challenge #1)

Audit of the NRC's Uranium Recovery Licensing Process

OIG Strategic Goal: Safety

The production of fuel for nuclear power plants involves extracting and processing uranium ore through a series of steps. The first step of this process, known as "uranium recovery," focuses on concentrating (or milling) natural uranium ore extracted from the earth. These recovery operations produce a product, called "yellowcake," which is then transported to a succession of fuel cycle facilities where the yellowcake is eventually transformed into fuel for nuclear power reactors. The NRC does not regulate uranium mining or mining exploration, but does have authority over "in situ recovery," where the uranium ore is chemically altered underground before being pumped to the surface for further processing.

As part of its regulatory authority, the NRC oversees the licensing of uranium recovery facilities. By issuing or amending a current license, the NRC authorizes the licensee to construct and operate a uranium recovery facility, expand an existing facility, or restart an existing facility at a specific site, in accordance with established laws and regulations.

Currently, the NRC regulates active uranium recovery operations in New Mexico and Nebraska. The NRC expects to receive applications for new facilities, expansions, and restarts in a variety of projected locations throughout the United States. Section 201 of the Nuclear Energy Innovation and Modernization Act, enacted in 2019, required the NRC to identify ways to improve the efficiency and transparency of uranium recovery license issuance and amendment reviews.

The audit objective is to determine if the NRC has effectively implemented actions to improve uranium recovery licensing efficiency.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Fiscal Year 2023 Financial Statements

OIG Strategic Goal: Corporate Management

Under the Chief Financial Officers Act, the Government Management and Reform Act, and OMB Bulletin 22-01, Audit Requirements for Federal Financial Statements, the OIG is required to audit the NRC's financial statements. The report on the audit of the agency's financial statements is due on November 15, 2023.

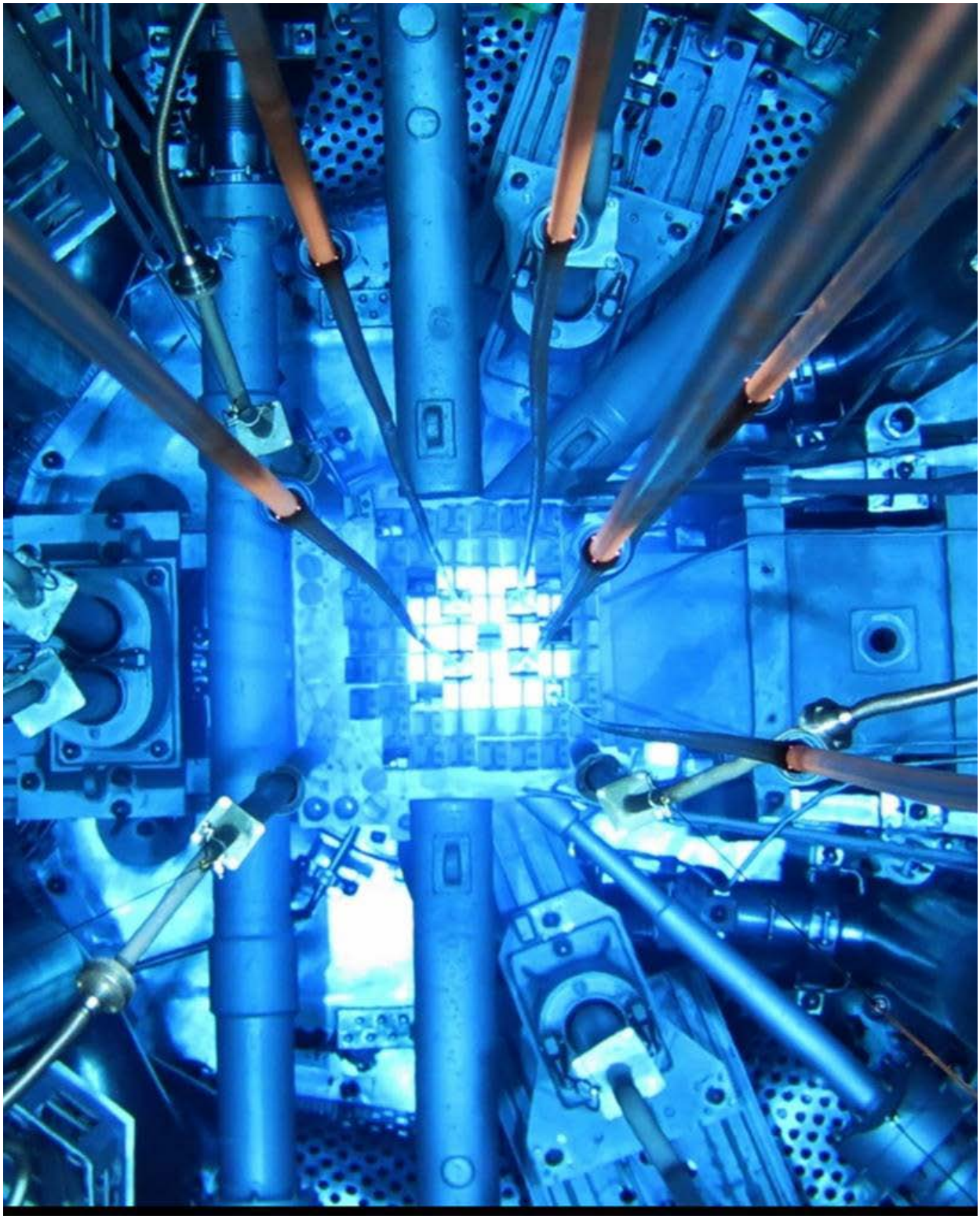
The audit objectives are to:

(1) Express opinions on the agency's financial statements and internal controls;

(2) Review compliance with applicable laws and regulations; and,

(3) Review controls in the NRC's computer systems that are significant to the financial statements.

(Addresses Management and Performance Challenge #8)



Research reactor core

NRC INVESTIGATIONS

Investigative Summaries

Special Inquiry into the NRC's Oversight of Research and Test Reactors

OIG Strategic Goal: Safety

Allegation:
The OIG initiated this Special Inquiry following a radioactive release to the environment from the NIST test reactor in Gaithersburg, Maryland on February 3, 2021. After the release, the NIST test reactor was shut down for more than two years before receiving authorization to restart from the NRC. This NIST event was one of eight unscheduled incidents or events in fiscal year 2021 that the NRC determined to be significant to public health or safety.

This Special Inquiry's focus broadened from the 2021 NIST event to include consideration of the NRC's oversight of other Research and Test Reactor (RTR) facilities to assess potential systemic issues. However, this report primarily discusses the NRC's oversight of the NIST test reactor prior to the February 2021 event because the event highlights areas in which the agency's oversight could be improved as it relates to other smaller nuclear facilities.

Investigative Results:
The OIG found that the agency's RTR program failed to identify and address problems with the NIST test reactor and other RTRs, specifically: (A) the NRC failed to identify problems with fuel movement, including precursors to later events; (B) the NRC's inspection practices often lacked direct observation of activities important to safety; (C) RTRs other than the NIST reactor experienced significant fuel oversight issues; and, (D) the agency's RTR program has not been substantively updated for at least two decades, and does not reflect the agency's risk-informed and safety culture positions.

The OIG's findings highlight future challenges for the agency's oversight programs for RTRs and advanced reactors.

NRC Response:
The NRC's response is due on January 29, 2024

(Addresses Management and Performance Challenges #1 and #4)

Concerns Regarding Inspections of Independent Spent Fuel Storage Installations

OIG Strategic Goal: Safety

Allegation:
OIG Investigations Division initiated this Special Inquiry in response to concerns that Region II acted inappropriately and without authority with respect to ISFSI inspections, that Region II failed to adhere to NRC policy by allowing resident inspectors who were not qualified under the agency's ISFSI inspection program to inspect ISFSIs, and that Region II deviated from the requirements in agency procedures for inspecting campaigns during which NRC licensees loaded spent fuel to dry cask storage.

Currently, most spent nuclear fuel is stored in specially designed pools at individual reactor sites around the country. Spent fuel rods are stored under at least 20 feet of water, which provides adequate shielding from the radiation for anyone near the pool. These spent fuel pools, however, are reaching design storage capacity. Because there are no permanent disposal facilities in the United States for high-level nuclear waste, licensees have built dry cask storage facilities, called ISFSIs, that are designed and constructed for the interim storage of spent nuclear fuel onsite. An ISFSI comprises a storage pad, storage containers, transfer equipment, and storage casks. Structures, systems, and components involved in ISFSIs are not safety-related but are classified as important to safety.

Investigative Results:
The OIG found that Region II improperly deviated from NRC policies when it authorized resident inspectors who were not qualified to inspect ISFSIs to inspect repeat spent fuel loading campaigns to dry cask storage. Furthermore, data from 2018 and 2019 show that collectively Region II's resident inspectors spent only about 20 percent of the number of hours anticipated for ISFSI inspections stated in the applicable inspection procedure. The limited inspection hours charged appear to show that Region II did not accomplish all inspection requirements identified in the procedure.

Region II's actions potentially resulted in missed opportunities to adequately evaluate whether licensees met the NRC's regulatory requirements. For example, from January 2021 to December 2022, after Region II began using properly qualified inspectors and following all the requirements in the applicable inspection procedure, those qualified inspectors identified numerous violations and other non-compliances during ISFSI inspections that could have been identified earlier. The OIG did not identify an immediate safety concern related to ISFSIs. The OIG did find, however, that Region II's deviation from

NRC policies resulted in licensees loading significant numbers of casks during repeat loading campaigns, from 2012 through 2020, that did not receive—and still have not received—adequate NRC inspections to ensure the licensees met regulatory requirements for long-term storage and retrievability.

Agency Response:

After considering the OIG's report's findings, the NRC staff concluded that no immediate safety concern exists, and the NRC has reasonable assurance of the long-term safety of ISFSIs. The NRC implemented an enhanced ISFSI inspection program in January 2021, and this program has provided a "more risk-informed, comprehensive, and consistent" approach to ISFSI oversight. In addition, the NRC reviewed the violations that the OIG stated might have been detected earlier and found that all violations were of very low safety significance.

Specifically, the NRC reported that as of January 2021, all ISFSI inspections in Region II were being performed by inspectors qualified under the ISFSI qualification process. While Region II's methodology of using reactor operations and health physics inspectors from 2012 until 2020 was not consistent with ISFSI inspector qualifications, these inspectors were qualified in areas that would provide an adequate level of understanding to identify issues to elevate to a qualified ISFSI inspector.

NRC staff reviewed the 6 violations of more than minor safety significance identified since January 2021 at the 16 ISFSI sites inspected. The staff found that three of the violations were recent design changes that would have not been in place during the previous inspections, and the remaining three violations were legacy violations. The legacy violations were of very low safety significance and did not result in safety consequences to ISFSI operations. The low number of violations did not yield any adverse programmatic deficiencies or trends.

Additionally, the staff reviewed operating experience across the ISFSI program, specifically evaluating violations across all regions over the previous 2 years and did not identify any operating experience that affected the safety of ISFSI sites. Therefore, the NRC staff concludes that no additional corrective action is needed to address the OIG's finding that qualified ISFSI inspector violations might have been detected earlier. The NRC added that the NRC has reasonable assurance of the long-term safety of ISFSIs. The NRC reviewed a sample of results of inspections performed at Region II ISFSI sites. These included inspections of preoperational and initial cask loading during the period subject to the OIGs findings and inspection of these ISFSIs under the revised inspection program.

The OIG's Review of the Agency's Response:
The NRC's response focused mostly on its enhanced ISFSI inspection program implemented after January 2021. The focus of the OIG's Special Inquiry, however, was not on the current inspection program, but on concerns related to the hundreds of spent fuel casks loaded between 2012 and 2020 at Region II operating reactors. In addition, in its response the NRC did not provide a complete explanation for why it was acceptable for Region II inspectors to spend only approximately 20% as many hours on inspections as those projected in agency guidance.

(Addresses Management and Performance Challenge #7)

The NRC's Oversight Regarding Generators at Diablo Canyon

OIG Strategic goal: Safety

Allegation:
The OIG initiated an investigation based on an anonymous allegation that the NRC, Pacific Gas and Electric, and Diablo Canyon Nuclear Power Plant managers conspired to cover up long-standing issues, such as fuel leaks from loose bolts, affecting all six emergency diesel generators at Diablo Canyon.

Emergency diesel generators (EDG) perform an important safety function when offsite power is unavailable. They supply onsite emergency electrical power for core cooling systems and other equipment necessary for mitigating an accident and maintaining the reactor in safe shutdown. For the EDG to be capable of performing this safety function, all its support systems and components must meet their functional requirements.

The Diablo Canyon Nuclear Power Plant has six air-cooled EDGs—three for each reactor designed with redundant configuration so that each reactor can withstand the loss of one vital 4KV electrical bus and still maintain the reactor's safety system functions. There are two underground diesel fuel storage tanks with a seven-day supply of fuel for each diesel generator.

Investigative Results:
The OIG did not substantiate alleged misconduct by NRC staff, nor did it find that NRC inspectors and licensee staff tried to conceal problems with the emergency diesel generators. At the same time, although the NRC staff consistently inspects EDGs, the OIG found that the NRC did not issue any violations for Diablo Canyon's EDG fuel oil system issues between 2017 through April 2022, even though the licensee has had long-standing problems with this system.

As shown in the NRC's inspection reports from April 2017 through April 2022, NRC inspectors often chose the EDGs as inspection samples for the Reactor Oversight Process, and they sampled the EDG fuel oil system more than 10 times. During this timeframe, however, the NRC did not issue any type of violation and reported "no findings" in these inspection reports.

On the other hand, the OIG found that NRC inspectors issued findings about leaking emergency diesel generators after the initiation of the OIG investigation into the concerns at Diablo Canyon. For example, a finding about emergency diesel generators was not issued following a June 2021 emergency shutdown due to excessive fuel oil leakage following a post maintenance test run. It was not until more than a year later—in August 2022, after the OIG investigation—that the NRC issued a green Non-Cited Violation for fuel oil system performance deficiencies with emergency diesel generators. Specifically, the NRC issued: (1) a green finding and associated non-cited violation in August 2022 for an event that took place just over a year earlier in June 2021; and, (2) another green finding in January 2023 related to the same June 2021 incident.

The OIG closed the investigation after it determined that the NRC took appropriate regulatory actions regarding Diablo Canyon's EDG fuel oil system performance deficiencies and presented a "Lessons Learned" briefing to Region IV staff at a June 2023 resident inspectors counterpart meeting.

(Addresses Management and Performance Challenge #1)

Alleged Hiring Discrimination Against Army Veterans for the NRC Office of Investigations Criminal Investigator Positions

OIG Strategic Goal: Corporate Management

Allegation:

The OIG received an allegation that the NRC Office of Investigations (OI) was discriminating against Army veterans who received criminal investigations training from the Army. According to the alleger, multiple OI job postings explicitly stated that criminal investigations training received at a specific Army facility would not satisfy the posting's qualification requirements.

Investigative Results and Agency Response:

After conducting an investigation to determine whether OI was discriminating

against Army veterans, the OIG did not identify any applicant who was marked disqualified or ineligible for an OI criminal investigator job posting because of training received at a specific Army facility.

However, the agency acknowledged that inclusion of language in OI job announcements about specific Army criminal investigator training not meeting minimum requirement was inaccurate, and the agency also stated that the language included in OI vacancy announcements going forward would be corrected. The Office of the Chief Human Capital Officer will take steps to remind agency human resources specialists and OI that excluding training programs that are accredited is unacceptable.

(Addresses Management and Performance Challenge #3)

Alleged Violation of the Prohibited Securities Rule

OIG Strategic Goal: Corporate Management

Allegation:
The OIG initiated an investigation based on an allegation that an employee had violated 5 CFR 5801.102, which prohibits "covered" NRC employees—that is, employees with substantive regulatory responsibilities—from owning stocks, bonds, and other security interests issued by entities in the commercial nuclear field. The spouses and minor children of covered employees are also prohibited from holding these security interests. According to the alleger, an employee's spouse was participating in a voluntary profit interest plan that gave her an interest in the profits of a company that was on the NRC's list of prohibited securities.

Investigative Results:
The OIG substantiated the allegation, finding that after becoming a "covered" employee, the NRC employee did not immediately disclose his spouse's profit plan participation. In addition, as part of his NRC duties the employee responded to a public comment from his spouse's employer, an action that potentially violated additional ethics rules. After his request for a waiver from the Prohibited Securities Rule was denied, the employee resigned from the NRC.

(Addresses Management and Performance Challenge #1)

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created the 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 as of 2014 to exercise the same authorities with respect to the DNFSB as the Inspector General exercises 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 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-23-A-01, "The Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in Fiscal Year 2023"* https://nrcoig.oversight.gov/top-management-challenges

DNFSB AUDITS

Audit Summaries

Audit of the DNFSB's Compliance with the Requirements of the Payment Integrity Information Act of 2019 for Fiscal Year 2022

OIG Strategic Goal: Corporate Management

The Payment Integrity Information Act (PIIA) requires each agency to annually estimate its improper payments. The PIIA requires federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. The PIIA also requires the OIG of each agency to determine whether the agency complies with the PIIA and submit a report on that determination. The OIG engaged CLA to perform the assessment of the DNFSB's compliance with the PIIA.

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

Audit Results:

CLA concluded that the DNFSB complied with the PIIA and the requirements in OMB Memorandum 21-19.

(Addresses Management and Performance Challenge #2)

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

OIG Strategic Goal: Corporate Management

The FISMA of 2014 established information security management requirements for agencies, including the requirement for an annual independent assessment by the agency's IG. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and to develop strategies and best practices to improve information security. The OIG contracted with CLA to conduct an independent audit of the DNFSB's overall information security program and practices in response to the FY 2022 IG FISMA Reporting Metrics.

The objective of this performance audit was to assess the effectiveness of the information security policies, procedures, and practices of the DNFSB.

Audit Results:
CLA concluded that the DNFSB did not implement effective information security policies, procedures, and practices. CLA noted new and repeat weaknesses in seven of the eight domains of the FY 2023 IG FISMA Reporting Metrics, and made one new recommendation to assist the DNFSB in strengthening its information security program.

(Addresses Management and Performance Challenge #2)

Audits in Progress

Audit of the DNFSB's Fiscal Year 2023 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 report on the audit of the agency's financial statements is due on November 14, 2023.

The audit objectives are 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.

(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, unless the records, or portions of the records, 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 within 20 business days of receiving a perfected 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 FY. 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 the FY.

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)

DNFSB INVESTIGATIONS

Investigative Case Summaries

Actions Inconsistent with the Delegation of Functions Required by the Atomic Energy Act

OIG Strategic Goal: Corporate Management

Allegation:
The OIG initiated an investigation based on an allegation that the DNFSB Chair failed to appropriately delegate administrative functions to the Executive Director of Operations (EDO) as required by the Atomic Energy Act.

Background:
At the recommendation of the Senate Committee on Armed Services, the FY 2019 National Defense Authorization Act included provisions amending the Atomic Energy Act of 1954 to establish an EDO position at the DNFSB. In particular, as amended, the Act establishes an EDO position at the DNFSB, describes the EDO's responsibilities, and requires the DNFSB's Chair to delegate certain Board functions to the EDO. The creation of the EDO position was first suggested in a 2018 report of the National Academy of Public Administration, which noted there was "a critical need to follow a more traditional management model that empowers the staff to deal with issues at an appropriate level and brings to the top only the critical, strategic matters worthy of a Presidentially Appointed Senate-confirmed Official's precious time."

Investigative Findings:
The OIG found that the Chair failed to delegate functions to the EDO as required by Atomic Energy Act sections 311 and 313. In addition, the Chair and the Board retained control over many DNFSB administrative functions, frequently bypassing the EDO when interacting with employees under the EDO's supervision. For example, even after the first EDO's appointment, the Board continued to hold meetings on topics that were primarily administrative in nature, such as conference room HVAC repair, procurement updates, and routine personnel actions. Senior managers stated that board members needed to act at a level appropriate for Presidential appointees and make nuclear safety their primary focus.

DNFSB Response: *The agency has indicated it is considering issuing a response by the end of October 2023.*

(Addresses Management and Performance Challenge #1)

Management of Contractors Questioned

OIG Strategic Goal: Corporate Management

Allegation:
The OIG initiated an investigation based on an allegation that the DNFSB Chair had ordered a contractor to do work outside of a contract's scope of work and without appropriate supervision. During the investigation, the OIG considered an additional concern that the Chair had allegedly violated the Federal Acquisition Regulation by inappropriately providing an evaluation of the contract employee to the contractor's program manager.

Investigative Results:
The OIG did not substantiate the allegation that work the contract employee performed was outside the scope of the contract or that a contractor employee was allowed to work without appropriate supervision. At the same time, the OIG determined that the Chair provided an evaluation of the contract employee that violated the Federal Acquisition Regulation by not including various required minimum aspects of an evaluation. The DNFSB's Office of the General Counsel thereafter provided training for Board and agency career staff to ensure they understand their responsibilities during interactions with contractors, and the OIG closed the investigation.

(Addresses Management and Performance Challenge #1)

Building 1 on NIST's Boulder, Colorado campus ***Photo courtesy of NIST.gov.***

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

April 1, 2023 – September 30, 2023

Complaints Received: 90 (51 received from the NRC OIG Hotline)

Investigative Statistics

Source of Complaints

NRC Employee	33
NRC Management	11
OIG Proactive Initiation	8
General Public	18
Other Government Agency	1
Anonymous	19

Disposition of Complaints

Reviewed Complaint and Closed (no additional action needed)	41
Correlated to Existing OIG Investigation	5
Referred to OIG Audit	3
Referred to New OIG Investigation	14
Referred to NRC Management	19
Reviewing Complaint	8
TOTAL:	**90**

Status of Investigations

Federal	
DOJ Referrals	0
DOJ Accepted	0
DOJ Declinations	1
DOJ Pending	3
Criminal Information/Indictments	0
Arrests	0
Criminal Convictions and/or Civil Settlement	0
Civil Recovery Amount	**$0**

State and Local	
State and Local Referrals	0
Criminal Convictions	0
Criminal Information/Indictments	0

NRC Administrative Actions	
Review of Agency Process	3
Termination or Resignation	1
Pending Agency Action	1

Summary of Investigations

Classification of Investigations	Carryover	Opened	Closed	Reports Issued*	Cases in Progress
Critical Risk – High	2	1	1	0	2
Employee Misconduct	1	1	2	0	1
External Fraud	2	0	1	0	2
False Statements	0	0	1	0	0
Internal Fraud	1	0	0	0	1
Management Misconduct	2	2	7	1	0
Miscellaneous	0	1	1	0	0
Project	0	1	1	0	0
Nuclear Regulatory Actions	2	1	1	0	3
Whistleblower Reprisal	1	1	2	0	1
TOTAL:	**11**	**8**	**17**	**1**	**10**

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

NRC Audits Completed

Date	Title	Audit Number
09/29/2023	The NRC Vulnerability Assessment and External Penetration Test Results	OIG-23-A-11
09/29/2023	Audit of the NRC's Implementation of the FISMA of 2014 for Fiscal Year 2023	OIG-23-A-10
08/21/2023	Audit of the NRC's Voluntary Leave Transfer Program	OIG-23-A-09
08/07/2023	Audit of the NRC's Oversight of the Federally Funded Research and Development Center Contract	OIG-23-A-08
08/07/2023	The Defense Contract Audit Agency Audit Report Number 1431-2019L10100001 & 1431-2020L10100001	OIG-23-A-07
05/10/2023	Audit of the NRC's Processes for Deploying Reactive Inspection Teams	OIG-23-A-06
05/09/2023	Audit of the NRC's Compliance with the Requirements of the Payment Integrity Information Act of 2019 in Fiscal Year 2022	OIG-23-A-05
05/04/2023	Audit of the NRC's Oversight of Irretrievable Well Logging Source Abandonments	OIG-23-A-04
04/17/2023	Audit of the NRC's Vacancy Announcement Process	OIG-23-A-03

NRC Contract Audit Reports

OIG Issue Date	Contractor/Title/ Contractor No.	Questioned Costs	Unsupported Costs
June 20, 2023	**Numark Associates, Inc**. Independent Audit Report on Numark Associates, Inc.'s Proposed Amounts on Unsettled Flexibly Priced Contracts for FYs 2019 and 2020 NRC-HQ-25-14-E0004, 31310020D0005	$133,947	$0

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	1	$133,947	0
Subtotal (A + B) ‡	6	$2,428,981	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	6	$2,428,981	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 $1,588,562 of the questioned costs for QiTech 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

April 1, 2023 – September 30, 2023

Complaints Received: 15 (14 received from the DNFSB OIG Hotline)

Investigative Statistics

Source of Allegations

DNFSB Employee	1
DNFSB Management	6
Anonymous	8
TOTAL:	**15**

Disposition of Complaints

Reviewed and Closed Complaint	7
Referred to OIG Investigations	3
Referred to DNFSB Management	1
Correlated to Existing OIG Investigation	4

Status of Investigations Federal

DOJ Referrals	1
DOJ Declinations	1
DOJ Pending	0
Criminal Information/Indictments	0
Criminal Convictions	0
Civil Recovery	0

State and Local	
State and Local Referrals	0
State Accepted	0
Criminal Information/Indictments	0
Criminal Convictions	0
Criminal Penalty Fines	0
Civil Recovery	0
DNFSB Administrative Actions	
Counseling and Letter of Reprimand	0
Terminations and Resignation	0
Pending Agency Action	1
Suspensions and Demotions	0

Summary of Investigations

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

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

DNFSB Audits Completed

Date	Title	Audit Number
09/29/2023	Audit of the DNFSB's Implementation of the FISMA of 2014 for Fiscal Year 2023	DNFSB-23-A-04
05/11/2023	The DNFSB Complied with the Requirements of the Payment Integrity Information Act of 2019 in Fiscal Year 2022	DNFSB-23-A-03

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.

Status: Open: Resolved.
The staff plans to add additional criteria to Regulatory Guide (RG) 1.184 (Draft Regulatory Guide (DG)-1347) and to specifically indicate that exemptions are needed for any spending of the decommissioning trust fund other than for radiological decommissioning activities. Estimated Final Rule Publication Date: November 2024.

Recommendation 2: Develop and issue clarifying guidance to NRC staff and licensees specifying instances when an exemption is not needed.

Status: Open: Resolved.
The staff plans to add additional criteria to RG 1.184 (DG-1347) and to specifically indicate that exemptions are needed for any spending of the decommissioning trust fund other than for radiological decommissioning activities. Estimated Final Rule Publication Date: November 2024.

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.

Status: Open: Resolved.
a. The NRC will perform an assessment of role-based privacy training gaps. This assessment will identify NRC employees and contract personnel who have roles that require specific privacy training. Because of resource priorities, the NRC is requesting a new target completion date of FY 2024, second quarter (Q2). The NRC recommends closure.
c. The NRC has transitioned 11 of its 15 information systems to National Institute of Standards and Technology SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, issued September 2020. The transition of the remaining 4 systems to Revision 5 is expected to be completed in the fourth quarter (Q4) of fiscal year (FY) 2024. Therefore, the NRC requests a new target completion date of FY 2024, Q4.
d. The NRC used its fully defined ISA to conduct an organization wide security risk assessment, as well as an assessment of privacy risks. Due to resource constraints, the organization wide security risk assessment covers one-third of the ISA every year. The remaining two-thirds of the organization wide security risk assessment will be completed in the fourth quarter (Q4) of FY 2024.
e. The NRC is in the process of using its fully defined ISA to conduct a supply chain risk assessment. The NRC requests a new target completion date of FY 2024, third quarter (Q3).
f. Based on the fully defined ISA, the NRC evaluated its cybersecurity policy and risk management strategy and determined that no updates were required. Because of competing priorities, the NRC requests a new target completion date of FY 2024, first quarter (Q1), to complete its update of agency cybersecurity processes.

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

Status: Open: Resolved.
The NRC will perform an assessment of role-based privacy training gaps. This assessment will identify NRC employees and contract personnel who have roles that require specific privacy training. Because of resource priorities, the NRC is requesting a new target completion date of FY 2024, second quarter (Q2).

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

Status: Open: Resolved.
The NRC estimates that the agency will need 6 months to complete this task. Because this task is dependent on the completion of recommendation 2e, the NRC's new target date for completion is FY2025, Q1.

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

Status: Open: Resolved.
The NRC estimates that the agency will need 6 months to complete this task. Because this task is dependent on the completion of recommendation 2e, the NRC's new target date for completion is FY2025, Q1.

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.

Status: Open: Resolved.
The NRC will evaluate the finalized ISA and the agency's contingency planning requirements to determine the impact and related necessary updates to policies and procedures. Due to limited resources and other priority operational and cybersecurity work, the NRC is now targeting completion for FY 2024, Q4.

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.

Status: Open: Resolved.
As part of its Operation Security (OpsSec) program, which is owned by the Office of Administration, the NRC will perform monthly checks to ensure NRC personnel are not writing passwords onto note cards, sticky notes, or other open, visible surfaces. These checks will be conducted at the NRC's Headquarters, Regions I, II, III, IV and TTC locations. Target Completion Date: FY 2023, Q2.

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.

Status: Open: Resolved.
As part of its Operation Security (OpsSec) program, which is owned by the Office of Administration, the NRC will perform monthly spot checks to ensure that NRC personnel have locked their workstation screens while unattended to prevent unauthorized viewing and network access. These checks will be conducted at the NRC's Headquarters, Regions I, II, III, IV, and TTC locations. Target Completion Date: FY 2023, Q2.

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

2 of 7 recommendations open since September 30, 2020

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

Status: Open: Resolved.
ADM revised Enclosure 5 from the OIG Office of Administration Director Memorandum, dated June 2022, to state the various methods for reporting lost/stolen property, the proper NRC Forms, and the appropriate routing path to the appropriate parties. The enclosure will be incorporated into the official agency policy in the finalized MD 13.1 scheduled for December 31, 2023.

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.

Status: Open: Resolved.
Through collaboration between ADM and OCIO, a Yellow Announcement (YA-22-0098) was issued on December 15, 2022, to inform all NRC employees of the decision to remove cell phones, laptops, and tablets from the sensitive items list and that these items are no longer being tracked in the NRCs Property Management System (SPMS) but are now being tracked and managed by OCIOs IT Service Management System (Remedy). Additionally, OCIO has updated the Hardware Asset Management playbook to include guidance on the process for reporting lost, missing, or stolen hardware assets covered under MD 12.5, *NRC Cybersecurity Program*. Supporting documentation is scheduled to be provided by December 21, 2023.

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)

8 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.

Status: Standards and Technology SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, issued September 2020, except for Office of Nuclear Security and Incident Response FISMA systems. The transition of these systems to Revision 5 is expected to be funded in the third quarter (Q3) of fiscal year (FY) 2023. Therefore, the NRC is requesting a new Target Completion date of FY2024, Q1.
d. The NRC recently implemented a 3-year cycle for the risk assessment of its information security architecture, which includes both security and privacy. Year 1 of the assessment cycle focuses on the Identify Function. Year 2 focuses on the Protect and Detect Functions. Year 3 focuses on the Respond and Recover Functions. The NRC is currently in year 2 of the cycle and expects to complete year 3 by the fourth quarter (Q4) of FY 2024. Throughout the 3-year risk assessment cycle, the NRC will follow its process to capture lessons learned and, where needed, update its risk management policies, procedures, and strategies. Target Completion Date: FY 2024, Q4
e. The NRC consistently assesses the criticality of Plans of Action and Milestones (POA&Ms) by ensuring that information systems security officers and assessors adhere to CSO-PROS-2030, *NRC Risk Management Framework (RMF) Process*, specifically step 5. CSO-PROS-2030 further prescribes that assessors follow CSO-PROS-2102, *System Cybersecurity Assessment Process*, when performing security assessments. Additionally, CSO-STD-0020, *System Security and Privacy Controls Standard*, prescribes the organizationally defined frequency by which all such testing is performed. Finally, the Risk and Continuous Authorization Tracking System (RCATS) employs a POA&M management component that requires all POA&Ms to be assigned a criticality (severity) at the time of creation. To date, 13 out of 15 FISMA systems have been migrated to RCATS. The NRC expects to migrate the remaining two systems to RCATS by FY 2023, Q3.

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.

Status: Open: Resolved.
The NRC will update its onboarding procedures to require individuals to complete a nondisclosure agreement before they are granted access to the NRC's systems and information. The clearance waiver process is wholly contained within the NRC's onboarding process and will inherit the updated procedures. The updated procedures will apply to all individuals who will be granted NRC network access after receiving an

IT-1, IT-2, L, or Q clearance. Individuals granted building access clearances will not be included because they are not granted access to the NRC network. The nondisclosure agreement will be an updated version of the NRC's Form 176A, *Security Acknowledgment*. Because of the estimated time needed to obtain an OMB clearance for these changes to Form 176A, the NRC is recommending a new target completion date of FY 2024, Q3.

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.

Status: Open: Resolved.
The NRC will conduct an in-depth, independent assessment of the Privacy Program, which will cover roles and training gaps. Using the results of the assessment, the NRC will update and develop annual role-based privacy training to address the identified gaps. The NRC will begin the assessment in Q3 of FY 2023, with completion planned by the first quarter (Q1) of FY 2024. The agency plans to complete the associated training development and implementation by FY 2025, Q1.

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.

Status: Open: Resolved.
The Office of the Chief Information Officer (OCIO) will analyze the agency's security awareness and role-based training records to better inform its response to this recommendation. OCIO staff will also consult with stakeholders such as the Office of the Chief Human Capital Officer and the National Treasury Employees Union to develop a specific, risk-based solution to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training. To perform this analysis and develop a solution the NRC requests a new Target Completion Date of Q2, FY2024.

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

Status: Open: Resolved.
The NRC will 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. Target Completion Date: FY 2023, Q4.

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.

Status: Open: Resolved.
For low-availability categorized systems, the NRC will complete an initial BIA and update the BIA whenever a major change occurs in the system or mission that it supports. The NRC will also address any necessary updates to the system contingency plan based on the completion of or updates to the system-level BIA. The NRC will also update its associated processes to incorporate these actions into its cybersecurity program. Target Completion Date: FY 2023, Q4.

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.

Status: Open: Resolved.
The NRC and OIG are working to come to an agreement on a sufficient way to complete this recommendation. The OIG will close the recommendation after the NRC integrates metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans to deliver persistent situational awareness across the organization. Target Completion Date: To be determined.

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.

Status: Open: Resolved.
The NRC and OIG are working to come to an agreement on a sufficient way to complete this recommendation. The OIG will close the recommendation when the agency provides documentation of the cost-benefit analysis and detailed information on the decision as to why or why not the agency will 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. Target Completion Date: To be determined.

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

1 of 4 recommendations open since August 19, 2021

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.

Status: Open: Resolved.
The staff held meetings with staff and attorneys of the Federal Energy Regulatory Commission (FERC) and the U.S. Federal Reserve Board (USFRB), to learn about these regulators' oversight authority over trusts and investments in decommissioning trust funds (DTFs). FERC attorneys and staff indicated that the agency will be unable to assist in the periodic assessment of trustee compliance with the master trust fund agreements in accordance with NRC investment restrictions, since FERC maintains oversight of utilities and potentially their trust fund investments but does not maintain similar oversight of merchant plants; the regulation at issue indicates "licensees that are not electric utilities," i.e., merchant plants. (See 10 C.F.R 50.75(h)(1)).

Accordingly, collaboration with FERC on this effort will not be viable. USFRB attorneys indicated that they do not perform financial audits or analyses that address the investment restrictions identified in NRC regulations. Furthermore, USFRB attorneys indicated that they were unable to put in place a general Memorandum of Understanding with the agency or other such vehicle committing to help the NRC address this task, nor were they willing to provide correspondence about a particular trustee following oversight reviews or audits performed by the USFRB in the future. Finally, staff is continuing to pursue additional outreach with trustees themselves, to learn what information that they may be able to provide regarding this matter. While not NRC licensees, the trustees may be able to provide some assurance that NRC investment restrictions in 10 C.F.R 50.75(h) are adhered to in merchant plant decommissioning trust fund portfolios. Upon completion of its outreach to trustees, staff will have performed its due diligence in responding and will terminate further assessment activities. Staff will document its research and response to Recommendation 4 by July 31, 2023.

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.

Status: Open: Resolved.
The Office of the Executive Director for Operations (OEDO) staff is working to develop the agency's risk appetite statement. Upon completion, the staff will implement a process to periodically communicate a consistently understood agency risk appetite. The agency's risk appetite statement and associated process for periodic communication will be incorporated in the next revision to OEDO Procedure 0960. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC staff and to update OEDO Procedure 0960. Target Completion Date: September 29, 2023

Recommendation 2: Revise agency policies and guidance to:
(a) Designate the official agency risk profile document and remove references to it as an 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.

Status: Open: Resolved.
a/b. The staff is revising agency policy and guidance to designate the official agency risk profile document, remove references of OMB deliverables, and fully address risk profile components and elements in accordance with OMB Circular A-123. The staff will revise MD 4.4 and OEDO Procedure 0960 as proposed in this recommendation. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC and to update OEDO Procedure 0960 as described in the updated response to Recommendation 1. Target Completion Date: September 29, 2023

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.

Status: Open: Resolved.
The NRC staff anticipated that OMB would revise and issue its primary guidance document for maturity models by late 2021. To date, this guidance document has not been issued, and the staff has not been able to obtain a revised date for publication. However, the staff will use the one-page maturity model that OMB has already developed to draft and implement the NRC's ERM maturity model. The implementation of this maturity model will include the development of an action plan with milestones to assess current practices and advance the model. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC. Target Completion Date: September 29, 2023.

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.

Status: Open: Resolved.
The NRC staff has begun implementing this recommendation by ensuring that QPR practices are fully performed by September 29, 2023. The staff plans to update OEDO Procedure 0960 with best practices based on this recommendation, including, but not limited to completion of QPR Dashboard entries, and recordation of all management decisions of risk in the QPR meeting summaries and the Executive Committee on ERM (ECERM) meeting minutes. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC and to update OEDO Procedure 0960 as described in the updated response to Recommendation 1. Target Completion Date: September 29, 2023.

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).

Status: Open: Resolved.
The OEDO is working with OCFO staff to establish and maintain a common business lines structure list. Upon completion, the staff will update ERM-related guidance. Any deviation from this business line structure will be identified with written justification in the resulting product. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC and update the ERM-related guidance. Target Completion Date: September 29, 2023.

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 QPR and reasonable assurance processes to accurately reflect that both agency processes address different aspects of 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."

Status: Open: Resolved.
The NRC staff is revising the guidance documents as mentioned in this recommendation. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC and update the guidance documents. Target Completion Date: September 29, 2023.

Recommendation 7: Update policies and guidance to clarify the effective date of the quarterly risks in the QPR process.

Status: Open: Resolved.
The OEDO is working with OCFO to update policies and guidance to clarify the effective date of the quarterly risks in the QPR process. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC and update the guidance documents. Target Completion Date: September 29, 2023.

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

Status: Open: Resolved.
The staff is developing ERM training that will address OMB Circular A-123 requirements and best practices. This training will periodically be provided to staff with ERM responsibilities. Additional time to complete this item is necessary to facilitate further staff collaboration within the NRC to finalize the training. Target Completion Date: September 29, 2023.

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)

15 of 18 Recommendations open since December 20, 2021

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

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

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

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

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

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

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

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

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

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)

3 of 8 Recommendations open since February 9, 2022

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.

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.

Audit of the U.S. Nuclear Regulatory Commission's Vacancy Announcement Process (OIG-23-A-03)

4 of 4 Recommendations open since April 2023

Recommendation 1: Develop and implement a systematic approach to record complete, accurate, and easily retrievable vacancy announcement data.

Recommendation 2: Develop and implement WTTS training for all applicable managers and staff.

Recommendation 3: Revise agency policy to include and clarify DHA requirements.

Recommendation 4: Develop and provide recurring DHA training for all current and future NRC management and staff involved with the hiring process.

Audit of the U.S. Nuclear Regulatory Commission's Oversight of Irretrievable Well Logging Source Abandonments (OIG-23-A-04)

5 of 5 Recommendations open since May 4, 2023

Recommendation 1: Collaborate with the regions and the NMSS to establish policy and agencywide positions related to well logging source abandonments.

Recommendation 2: Review and standardize processes and guidance related to the handling and processing of irretrievable well logging source abandonments.

Recommendation 3: Develop an environmental assessment to be used in support of exemptions related to the approval of temporary storage locations for abandoned well logging sources.

Recommendation 4: Develop guidance to support analysis of exemption requests.

Recommendation 5: Develop consistent guidance across all regions to clarify the processes and procedures for documenting abandonment notifications and licensee reports, and to ensure consistency and completeness for abandonment event documentation in ADAMS.

Audit of the U.S. Nuclear Regulatory Commission's Processes for Deploying Reactive Inspection Teams (OIG-23-A-06)

3 of 3 Recommendations open since May 10, 2023

Recommendation 1: Update agency policies to require that staff provide complete information on screening evaluation forms, correctly profile evaluation forms in ADAMS, and publicly share non-sensitive reactive inspection screening decision-making, whenever possible.

Recommendation 2: Update agency policies so that they provide a well-defined incident screening process with examples for screening reactor safety and security events.

Recommendation 3: Periodically assess the effectiveness of MD 8.3 and IMC 0309 implementation.

Audit of the U.S. Nuclear Regulatory Commission's Oversight of the Federally Funded Research and Development Center Contract (OIG-23-A-08)

2 of 2 Recommendations open since August 7, 2023

Recommendation 1: Develop a strategy to address the backlog of closeout of CNWRA contracts/tasks orders, to include the payment of all final invoices.

Recommendation 2: Allocate resources with cost reimbursement contract knowledge, as necessary, to eliminate the backlog of CNWRA final invoice billings and closeouts in a timely manner.

Audit of the U.S. Nuclear Regulatory Commission's Voluntary Leave Transfer Program

6 of 6 Recommendations open since August 21, 2023

Recommendation 1: Update roles and responsibilities in appropriate agency guidance to ensure program oversight and continuous monitoring of VLTP participant eligibility.

Recommendation 2: Revise applicable policies and procedures to reflect current practices and address inconsistencies and outdated information.

Recommendation 3: Establish a process to identify voluntary leave recipients who have stayed in the program for an extended time period and provide guidance for OCHCO staff on what actions, if any, they should take regarding such recipients.

Recommendation 4: Implement a means of capturing required voluntary leave recipient information, and use this information to conduct continuous monitoring to ensure leave recipients remain affected by a medical emergency.

Recommendation 5: Develop and implement quality assurance measures to ensure recordkeeping of voluntary leave recipient documents complies with federal and agency record retention requirements.

Recommendation 6: Conduct quality assurance checks to validate voluntary leave recipients' enrollment and termination dates, and to ensure dates are captured correctly in the FPPS.

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

3 of 3 Recommendations open since September 29, 2023

Recommendation 1: Review all ITI POA&Ms to ensure that they are accurate and contain detailed information on the status of corrective actions, including changes to scheduled completion dates.

Recommendation 2: Implement a revised ITI Core Services 90-day account disablement script to ensure all non-privileged and privileged Active Directory accounts are captured and disabled in accordance with NRC policies.

Recommendation 3: Increase the current SIEM tool licensing level and acquire funding to adequately support the procurement, onboarding, and implementation of requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.

U.S. Nuclear Regulatory Commission Vulnerability Assessment and External Penetration Test Results (OIG-23-A-11)

2 of 2 Recommendations open since September 29, 2023

Recommendation 1: Implement corrective actions to address vulnerabilities identified in this report.

Recommendation 2: Improve the patch and vulnerability management program to patch security deficiencies within the NRC's defined patching time frame.

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.

Status: Open: Resolved.
HR to coordinate with OTD Q4 2023, to lay foundation for developing a recruitment plan in coordination with OEDO EEO Program Manager to address DEIA item for 2024. Awaiting Human Capital Plan prioritization of this action item.

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

Status: Open: Resolved.
HR to prioritize development of step-by-step hiring process metric in agreement with priority assigned in the Human Capital Plan currently under development for publication anticipated end 2023. Upon completion of DN staffing operating procedure the step-by-step hiring process will be finalized to review, and report anticipated in 2024.

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.

Status: Open: Resolved.
HR anticipates completion of DN staffing operating procedure to include technical qualifications standards for DN-2 through DN-5 due for draft completion Q4, 2023 and publication TBD in 2024.

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

Status: Open: Resolved.
HR anticipates delivery of training on hiring process for all DNFSB pay plans Q4, 2023.

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.

Status: Open: Resolved.
HR anticipates preliminary study to be shared with new EDO: anticipated hire by 2024.

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

Status: Open: Resolved.
HR anticipates development of action plan post EDO hire 2024.

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)

5 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.

Status: Open: Resolved.
The DNFSB requested this recommendation be closed. Since the conclusion of the FY19 FISMA audit, DNFSB has implemented multiple tools that maintain an up-to-date, complete, accurate and readily available Agency-wide view of the security configurations for all GSS components. These include:
- Qualys Cloud platform: provided by the DHS CDM program, DNFSB has installed a Qualys scanner on the GSS internal network and installed Qualys agents on all GSS components for which an agent exists, which includes all Windows end-user computers and servers. Qualys performs both uncredentialed IP-based scans of the entire GSS IP address space and credentialed scans of all supported devices. These scans provide a complete asset inventory of all hardware devices connected to the GSS and all software installed on devices with Qualys agents, along with any identified vulnerabilities and misconfigurations. The Qualys data is then used to create DNFSB's CDM Agency Dashboard, which applies scoring algorithms (the "AWARE Score") to the Qualys scan data.
- Microsoft 365 Defender Portal: The Microsoft 365 (M365) Defender portal integrates multiple Microsoft security tools including Microsoft Defender for Endpoint (MDE), Microsoft Defender for Identity (MDI), Microsoft Defender for Cloud Apps (MDCA), Microsoft Intune and Azure AD Premium P2. MDE clients are installed on all Windows end-user computers and servers, and all end-user computers and mobile devices (agency-issued iPhones) are managed by Intune. The M365 Defender portal also provides a hardware inventory of all Windows computers and IoT devices connected to the GSS, and all software installed on all Windows computers.

- ForeScout CounterAct Appliance: DNFSB continues to refine the configuration of its CounterAct appliance, which provides visibility into all devices that connect to the DNFSB network. CounterAct performs network-based inventory of all devices connected to the GSS using a variety of scanning methods (IP ports & protocols, HTTP, NetBIOS and SNMP).
OIG assessment: The DNFSB has not completed the recommended items. The DNFSB anticipates completing these tasks by Q4, FY 2023.

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.

Status: Open: Resolved.
The DNFSB requests closure of this recommendation. The DNFSB required all members of the IT team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that addressed changes to the Change Control Board and Security Impact Analysis form process.
DNFSB's User Agreement/Rules of Behavior form that all users are required to sign includes the language: "I understand that non-compliance with the DNFSB's directives and policies may be cause for disciplinary action up to and including system privilege revocation, dismissal from the DNFSB or removal from contract, and criminal and/or civil penalties."

The OIG assessment: Neither the DNFSB Configuration Management Policy nor the DNFSB GSS SSP security control implementation details for Configuration Management (CM) family controls define consequences for not adhering to change control requirements or reflect details about conduct of remedial training as necessary for change control requirement reinforcement. Additionally, the DNFSB did not provide evidence supporting the completion of configuration management training.

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

Status: Open: Resolved.
The DNFSB requested closure of this recommendation. The DNFSB continues to work towards implementation of a stronger ICAM architecture. A new certificate authority (CA) server has been implemented which has facilitated the use of local multifactor authentication on privileged accounts within the DNFSB GSS.

The OIG assessment: The DNFSB continues to work towards implementation of a stronger ICAM architecture. A new certificate authority (CA) server has been implemented which has facilitated the use of local multifactor authentication on privileged accounts within the DNFSB GSS. This recommendation will be closed when the OIG verifies that the DNFSB has continued efforts to meet milestones of the DNFSB ICAM strategy.

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

Status: Open: Resolved.
The DNFSB requested closure of this recommendation. The DNFSB has updated its Risk Management Framework Handbook to refine existing monitoring and assessment procedures to support ongoing authorization of DNFSB information systems more effectively.

The OIG assessment: Progress has been made in refining procedures such as the DNFSB GSS Continuous Monitoring Policies and Procedures Guide to support adoption of an ongoing authorization model. However, ongoing authorization of the DNFSB GSS is not yet in place. Specifically, the last traditional ATO lasted for three years from the date of signature, expiring November 8, 2018. Also, at the time of our review, an external security assessment to receive an updated authorization was not yet completed.

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.

Status: Open: Resolved.
The DNFSB requested this recommendation be closed. The DNFSB developed a Supply Chain Risk Management (SCRM) Strategic Plan, which addresses the items included in the recommendation. A draft version of this document was provided to the FISMA auditors during their fieldwork in response to a PBC item request and a final version has been approved by the DNFSB CIO. Many of the government-wide contract vehicles that the DNFSB utilizes, such as GSAdvantage and NASA SEWP, have internal processes to ensure approved vendors perform SCRM-related actions such as complying with Section 889 requirements. In addition, discussions with the DNFSB's Contracting Officer indicated that additional internal agency policies for IT acquisitions are being developed that will mandate the inclusion of FAR clauses related to SCRM in all future contracts for IT acquisitions.

The OIG assessment: ICT supply chain risk was not addressed in the DNFSB's contingency planning policies and procedures, Supply Chain Risk Management Strategic Plan, or in the DNFSB GSS SSP.

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

11 of 14 recommendations open since March 25, 2021

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

Status: Open: Resolved.
In response to EO 14028, OMB M-22-09, and other recent OMB Memoranda related to Zero Trust, the DNFSB has developed a Zero Trust Architecture Implementation Plan. This plan will serve as the equivalent of both an Enterprise Architecture and Information Security Architecture. The DNFSB anticipates completing these actions by end of Q4, FY23.

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.

Status: Open: Resolved.
The DNFSB is continuing to refine its risk management processes to document risk for all information systems used by the agency, which will then allow risk to be evaluated at the business process and enterprise level. The DNFSB will determine the most effective way to perform an organization wide security and privacy risk assessment given the agency's size and available resources. The DNFSB will determine the most effective way to perform a supply chain risk assessment given the agency's size and available resources and then update contingency planning policies and procedures and related supply chain risk management (SCRM) policies and procedures. The DNFSB anticipates completing these tasks by Q4 FY23.

Recommendation 3:

(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 NIST 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.

Status: Open: Resolved.
The DNFSB anticipates completing these tasks by Q4, FY 2023.

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.

Status: Open: Resolved.
The DNFSB is implementing a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. The solution will leverage data from the CDM Agency Dashboard, Defender for Microsoft 365, and the agency's ForeScout CounterAct appliance.

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.

Status: Open: Resolved.
The DNFSB required all members of the IT team that are authorized to submit change request tickets to take remedial "CCB and Change Request Training" in August 2022 and then take an updated remedial training in December 2022 that addressed changes to the Change Control Board and Security Impact Analysis form process.

The OIG assessment: The DNFSB did not provide evidence supporting the development and delivery of remedial training for all members of the IT staff to reinforce 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 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.

Status: Open: Resolved.
The DNFSB developed and published New Hire Procedures that require DNFSB Help Desk staff to ensure that new users (federal employees & contractors) have completed all mandatory security-related training (as documented in the Security Awareness Training Policy) and have submitted a signed DNFSB Information Systems User Agreement/Rules of Behavior + IT Equipment Agreement form prior to network accounts being created and access to these accounts being given to new users.

The OIG assessment: Evidence supporting implementation of the technical capability restricting granting of access until after a non-disclosure agreement is signed and uploaded was not provided. Also, for a sample of six non-privileged users from the population of 17 created since October 1, 2022, we noted:
• For one new user, the agreements were signed after access was provisioned.
• For two of the new users, we were unable to verify when the agreements were signed as they did not include the date next to the wet signatures / were not digital signatures with a date/timestamp.

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.

Status: Open: Resolved.
The DNFSB has procedures in place to automate the process of identifying privileged accounts that are inactive but wants to have a formal approval process for disabling or deleting privileged accounts; given the small number of privileged users at the DNFSB, this is an acceptable risk. The DNFSB will request a risk acceptance for this recommendation.

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

Status: Open: Resolved.
The DNFSB developed a Security Awareness Training Policy that outlines the requirements for annual IT-security related training DNFSB users are required to complete every year. A draft version of this document was provided to the FISMA auditors during their fieldwork in response to a PBC item request and a final version has been approved by the DNFSB CIO. The annual cybersecurity awareness training and phishing and social engineering awareness training that all DNFSB users must take, address privacy and data protection responsibilities, and the role-based privileged user training that all users identified as privileged users must complete, contains additional information regarding privacy and data protection responsibilities. In addition, dedicated Annual Privacy Act Training was given to all DNFSB users.

The OIG assessment: Upon inspection of the training records provided, evidence of all DNFSB users completing Privacy Act Training was not provided and specific role-based privacy training was not called out.

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

Status: Open: Resolved.
The DNFSB conducted a breach response exercise on 9/29/2022 and will request this Recommendation be closed.

The OIG assessment: Inspected the incident response and contingency planning exercises completed and noted they did not include an evaluation of the breach response plan.

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

Status: Open: Resolved.
The DNFSB published the updated version of its "Risk Management Framework" on 9/29/22 and will request this Recommendation be closed.

The OIG assessment: Progress has been made in refining procedures such as the DNFSB GSS Continuous Monitoring Policies and Procedures Guide to support adoption of an ongoing authorization model. However, ongoing authorization of the DNFSB GSS is not yet in place. Specifically, the last traditional ATO lasted for three years from the date of signature, expiring November 8, 2018. Also, at the time of our review, an external security assessment to receive an updated authorization was not yet completed.

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.

Status: Open: Resolved.
The DNFSB will determine the most effective way to perform a supply chain risk assessment given the agency's size and available resources and then update contingency planning policies and procedures and related supply chain risk management (SCRM) policies and procedures. The DNFSB anticipates completing these tasks by Q4, FY23.

The OIG assessment: ICT supply chain risk was not addressed in the DNFSB's contingency planning policies and procedures, Supply Chain Risk Management Strategic Plan, or in the DNFSB GSS SSP.

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)

15 of 24 recommendations open since December 21, 2021

Recommendation 1: Update the Information Security Architecture (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 NIST 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 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 13: Continue current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.

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

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)

4 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 5: Complete the implementation of the configuration management training program and provide periodic refreshers to ensure evidence requirements are captured for change tickets.

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.

Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2023 (DNFSB-23-A-04)

1 of 1 Recommendation open since September 29, 2023

Recommendation 1: Acquire resources to adequately support the procurement, onboarding and implementation of requirements across all EL maturity tiers to ensure events are logged and tracked in accordance with OMB M-21-31.

ABBREVIATIONS AND ACRONYMS

C.F.R.	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CLA	CliftonLarsonAllen
DCAA	Defense Contract Audit Agency
DCNPP	Diablo Canyon Nuclear Power Plant
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
EDG	Emergency Diesel Generators
EDO	Executive Director for Operations
FAR	Federal Acquisition Regulation
FFRDC	Federally Funded Research and Development Center
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GLINDA	Global Infrastructure and Development Acquisition
IAM	Issue Area Monitoring
IG	Inspector General
ISFSI	Independent Spent Fuel Storage Installation
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OI	Office of Investigations
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act of 2019
RTR	Research and Test Reactors

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 to be 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 to be 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 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 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 OIG's policies and procedures.

Investigations

The OIG investigative program was peer reviewed by the Department of Commerce OIG. The peer review final report, dated November 1, 2019, reflected that the 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
https://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, Maryland 20852-2738