Semiannual Report to Congress
April 1, 2022—September 30, 2022

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

THE OIG VISION

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

THE OIG MISSION

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

COVER PHOTO:

Vogtle Electric Generating Plant

A MESSAGE FROM THE INSPECTOR GENERAL

On behalf of the Office of the Inspector General, U.S. Nuclear Regulatory Commission and Defense Nuclear Facilities Safety Board, it is my pleasure to present this Semiannual Report to Congress, covering the period from April 1, 2022 to September 30, 2022. 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 10 audit and evaluation reports, and recommended several ways to improve NRC and DNFSB safety, security, and corporate management programs. We also opened fourteen investigative cases and completed eight, one of which was referred to the Department of Justice, and six of which were referred to NRC or DNFSB management for action.

Our reports are intended to strengthen the NRC's and the DNFSB's oversight of their myriad endeavors and reflect the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse. Summaries of the reports herein include reviews of: the NRC's compliance with the Federal Information Security Modernization Act; strategic workforce planning; drop-in meeting policies and procedures; management controls for material export licensing; compliance with improper payment laws; processes for licensing emerging medical technologies; DNFSB compliance with the Federal Information Security Modernization Act; and, DNFSB compliance with Improper Payments Laws. Further, this report includes summaries of cases involving several concerns, including: the NRC's oversight of the auxiliary feedwater system at Diablo Canyon Nuclear Power Plant; alleged discrimination against an NRC manager; unauthorized storage of nuclear gauges; improper concurrence process on issuing internal guidance; and, the DNFSB's nonpublic collaborative discussions.

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

Robert J. Feitel

Robert J. Feitel

Highlights

OFFICE of AUDITS

Defense Nuclear Facilities Safety Board		U.S. Nuclear Regulatory Commission
2 **Reports Issued**		**8** **Reports Issued**
29	**Recommendations Made**	25
6	**Recommendations Closed**	37

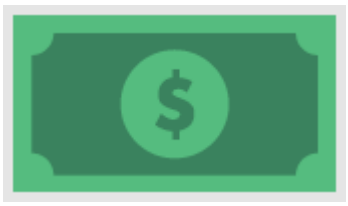
$2,295,007

Questioned and Unsupported Costs

Highlights

OFFICE of INVESTIGATIONS

1
Civil/Administrative Recovery
$ 1,385.86



1
Criminal Charge

1
Criminal Matter Referred for Prosecution

Open Investigations

14

Closed Investigations

8

In Progress Investigations

27

CONTENTS

Highlights **8**
Audits 8
Investigations 12
Overview of the NRC and the OIG **16**
The NRC's Mission 16
OIG History, Mission, and Goals 17
OIG Programs and Activities **20**
Audit Program 20
Investigative Program 22
OIG General Counsel Regulatory Review 24
Other OIG Activities 28
NRC Management and Performance Challenges **31**
NRC Audits **32**
Audit Summaries 32
Audits in Progress 38
NRC Investigations **44**
Investigative Case Summaries 44
Defense Nuclear Facilities Safety Board **50**
DNFSB Management and Performance Challenges **51**
DNFSB Audits **52**
Audit Summaries 52
Audits in Progress 53
DNFSB Investigations **54**
Summary of OIG Accomplishments at the NRC **58**
Investigative Statistics 58
Audits Completed 61
Contract Audit Reports 62
Audit Resolution Activities 63
Summary of OIG Accomplishments at the DNFSB **66**
Investigative Statistics 66
Audits Completed 69
Audit Resolution Activities 70
Unimplemented Audit Recommendations **72**
NRC 72
DNFSB 86
Abbreviations and Acronyms **96**
Reporting Requirements **97**
Appendix **98**

The NRC Headquarters Complex

HIGHLIGHTS

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

Audits

Nuclear Regulatory Commission

- The Federal Information Security Modernization Act (FISMA) of 2014 established the information security management requirements for agencies, including the requirement for an annual independent assessment by each agency's Inspector General (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 Office of the Inspector General (OIG) contracted with CliftonLarsonAllen, LLP (CLA) to conduct an independent audit of the U.S. Nuclear Regulatory Commission's (NRC's) overall information security program and practices in response to the fiscal year (FY) 2022 Inspector General FISMA Reporting Metrics.

- Strategic Workforce Planning (SWP), also called human capital planning, is the development of long-term strategies for acquiring, developing, and retaining an organization's total workforce to meet future needs. SWP aligns an organization's human capital program with its current and emerging mission and programmatic goals. SWP aids in the development of long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals. The OIG assessed the effectiveness of the NRC's SWP process.

- A drop-in meeting is a type of non-public meeting that occurs at the NRC. The NRC staff uses both public and non-public meetings to interact with external stakeholders. The agency's policy exempts drop-in meetings from certain requirements governing its public meetings, including the requirements to post a meeting notice and summary. The OIG assessed whether the NRC's policies and procedures for non-public interactions with

industry stakeholders are adequate to prevent compromise of the independence of agency staff or the appearance of conflicts of interest.

- The NRC is authorized to license the export of special nuclear material, source material, and byproduct material. The NRC reviews each license application to ensure the proposed material export will not be inimical to the safety and security of the United States, and will be consistent with applicable agreements for peaceful use. The OIG assessed the effectiveness of the NRC's management controls of material export licensing.

- 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 the audit conclusions, monitoring their staff qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management, and follow up on agency actions initiated due to this report. At the request of the OIG, the DCAA audited Qi Tech LLC, and Advanced Systems Technology Management Inc., and provided the OIG with two audit reports.

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

- The NRC develops specific licensing guidance, reviews license applications, and issues decisions on applications for the use of emerging medical technologies regulated under Title 10 of the Code of Federal Regulations (C.F.R.), Part 35, Subpart K. Due to an anticipated growth in medical applications of radioisotopes and advancements in medical technologies, the NRC predicted that in FYs 2020–2023, there will be the potential need to evaluate up to 15 emerging medical technologies. The OIG assessed the NRC's efficiency in licensing the use of emerging

medical technologies, including the agency's development of technology-specific guidance for licensing the use of emerging medical technologies under 10 C.F.R. Part 35, Subpart K.

Defense Nuclear Facilities Safety Board

- The FISMA established the 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 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 Inspector General FISMA Reporting Metrics.

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

Investigations

Nuclear Regulatory Commission

- Over the last few years, we reviewed multiple allegations reported to us regarding the NRC's oversight at Diablo Canyon Nuclear Power Plant (DCNPP), a plant with two reactors, in Avila Beach, California. Several of those concerns involved the NRC's oversight of safety-related structures, systems, and components (SSCs). One such SSC is the auxiliary feedwater (AFW) system, which is important to a commercial nuclear power plant because it is a backup water supply that can be used to cool the reactor if normal feedwater is out of service. After a July 2020 AFW system failure that required Unit 2, one of DCNPP's nuclear reactors, to enter a shutdown mode for 8 days, we received specific allegations that the NRC had inadequately inspected the AFW system prior to the event. These allegations further raised questions as to whether there is less than optimal NRC oversight at the DCNPP. Therefore, we initiated an event inquiry to review the adequacy of the NRC's inspections of the AFW system prior to the July 2020 event.

- We received an allegation that the NRC discriminated against a now former Senior Executive Service (SES) employee when the employee returned to work after being on sick leave. The employee informed the employee's supervisor that the employee would be on sick leave for approximately 2 months. Upon returning to the office, the employee was not placed back into the employee's position, and instead was relegated to perform "busy work" not commensurate with the duties required of an SES employee. The employee subsequently chose to retire from the NRC.

- We received an allegation that the NRC is "failing the American people by allowing nuclear gauges to be stored at places not 'authorized' under the NRC rules." The alleger said, "apparently, the NRC found that the company was storing nuclear gauges at a location not on the license but didn't follow up on the incident," and questioned if the NRC was "waiting for someone to build a dirty bomb before doing their job."

- We received an allegation that a risk assessment white paper on newly developed methods was signed without having addressed

objections from the Office of the General Counsel (OGC) and without reconciling an open non-concurrence program item. The alleger stated the paper's author and another employee removed the OGC from the paper's concurrence process to avoid addressing the OGC's initial objections to the paper. The alleger also claimed retaliation when he was excluded from a leadership meeting.

Defense Nuclear Facilities Safety Board

- We received an allegation that the DNFSB improperly conducted nonpublic collaborative discussions (NCDs) regarding technical matters. The use of NCDs allegedly bypassed meetings that would have produced a public record showing what transpired during the meetings. We also assessed whether the DNFSB violated any law by holding NCDs prior to November 29, 2021, the effective date of the DNFSB's new regulation reflecting its new authority to hold NCDs. In addition, we reviewed whether the DNFSB held informal votes during NCDs, in violation of the National Defense Authorization Act (NDAA) Section 3202 and the Atomic Energy Act (AEA) Section 313(k)(1)(A). Finally, we reviewed whether the DNFSB properly documented summaries of the meetings for public review and whether the agency properly communicated information discussed during NCDs to agency staff.

Vogtle Electric Generating Plant

OVERVIEW OF THE NRC AND THE OIG

The NRC's Mission

The NRC began operations in 1975 as an independent agency within the executive branch with responsibility for regulating the various commercial and institutional uses of nuclear materials. The agency succeeded the Atomic Energy Commission, which previously had responsibility for both developing and regulating nuclear activities. The NRC's mission is to license and regulate the nation's civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. The NRC's regulatory mission covers three main areas:

- **Reactors** – Commercial reactors that generate electric power, and research and test reactors used for research, testing, and training;

- **Materials** – Use of nuclear materials in medical, industrial, and academic settings, and facilities that produce nuclear fuel; and,

- **Waste** – Transportation, storage, and disposal of nuclear materials and waste, and decommissioning of nuclear facilities from service.

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

The NRC maintains a current website and a public document room at its headquarters in Rockville, Maryland; holds public hearings and public

meetings at NRC offices and in communities throughout the United States; and, engages in discussions with individuals and organizations.

OIG History, Mission, and Goals

OIG History

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

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

Today, the IG concept is a proven success. IGs continue to deliver significant benefits to our nation. Thanks to IG audits and investigations, billions of dollars have been returned to the federal government or have been better spent based on recommendations identified through those audits and investigations. IG investigations have also contributed to ensuring that thousands of wrongdoers are held accountable for their actions. The IG concept and its principles of good governance, accountability, and monetary recovery have been adopted by foreign governments as well, contributing to improved governance in many nations.

OIG Mission and Goals

The NRC OIG was established as a statutory entity on April 15, 1989, in accordance with the 1988 amendments to the IG Act, to provide oversight of NRC operations. The Consolidated Appropriations Act of 2014 subsequently authorized the NRC IG to exercise the same authorities concerning DNFSB operations. The OIG's mission is to provide independent, objective audit and investigative oversight of the operations of these agencies, in order to protect people and the environment.

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

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

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

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

The Inspector General, pictured right, and the Assistant Inspector General for Investigations, Malion Bartley, inside the containment building under construction at Vogtle.

OIG PROGRAMS AND ACTIVITIES

Audit Program

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

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

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

- **Reporting** – The auditors present the information, findings, conclusions, and recommendations that are supported by the evidence gathered during the survey and fieldwork phases. 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 misconduct by employees and contractors, interfacing with the U.S. Department of Justice on OIG-related criminal and civil matters, and coordinating investigations and other OIG initiatives with federal, state, and local investigative agencies, and other OIGs.

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

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

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

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

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

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

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

The OIG has also implemented a series of proactive initiatives designed to identify specific high-risk areas that are most vulnerable to fraud, waste, and abuse. A primary focus is electronic-related fraud in the business environment. The OIG is committed to improving the security of this constantly changing electronic business environment by investigating unauthorized intrusions and computer-related fraud, and by conducting computer forensic examinations. Other proactive initiatives focus on determining instances of procurement fraud, theft of property, government credit card abuse, and fraud in federal programs.

OIG General Counsel Regulatory Review

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

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

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

From April 1, 2022 to September 30, 2022, the OIG reviewed a variety of regulatory documents. In its reviews, the OIG remained cognizant of how the proposed rules or policies could affect the OIG's functioning or independence. The OIG also considered whether the rules or policies could significantly affect NRC or DNFSB operations or be of high interest to NRC or DNFSB staff and stakeholders. In conducting its reviews, the OIG applied its knowledge and awareness of underlying trends and overarching developments at the agencies and in the areas they regulate.

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

NRC Management Directives

- MD 3.4, "Release of Information to the Public," which establishes a policy of making as much information as possible available to the public regarding the NRC's health and safety mission, while at the same time accounting for the agency's legal responsibility to protect specific types of information. The OIG reviewed revisions to this MD to ensure they account for all legal requirements pertaining to information disclosure, including requirements in the Freedom of Information Act and the Privacy Act. The OIG also reviewed the revisions to ensure the MD accurately describes how information-disclosure determinations are made within the OIG. The OIG provided substantive comments to clarify various aspects of the MD, including the general standards for withholding information, the roles various NRC offices have in disclosure determinations, and the terminology used in certain sections of the MD.

- MD 6.1, "Resolution and Followup of Audit Recommendations," which provides guidance for the NRC staff on responding to audit reports from the OIG and the U.S. Government Accountability Office. The OIG reviewed revisions to this MD to ensure they are consistent with the NRC staff's obligations under both the IG Act and Office of Management and Budget Circular A-50, "Audit Followup." The OIG recommended that the staff clarify the terminology it uses to describe certain types of audit reports, as well as language referring to the manner in which the OIG distributes contract audit reports. The OIG also recommend clarifying various terms used in the MD and updating hyperlinked text so that it directs the reader to www.oversight.gov.

- MD 7.7, "Securities Ownership," which helps implement the NRC's supplemental ethics rule prohibiting NRC employees, their spouses, and their minor children from owning securities issued by NRC-regulated entities and other entities in the commercial nuclear sector. The revisions to this MD included changes the NRC made in response to report OIG-21-A-17, "Audit of the NRC's Prohibited Security Ownership Process." The OIG reviewed the revisions and determined they are consistent with the actions the NRC committed to taking in response to the OIG's report. The OIG also reviewed additional revisions to the MD, recommending that the NRC clarify certain terms in the MD and reorder various sections. The OIG also recommended that the NRC provide hyperlinks or otherwise cross-reference informational material from the Office of Government Ethics that explains how employees can request a

certificate of divestiture in connection with the sale of prohibited securities.

- MD 10.161, "Civil Rights Program and Affirmative Employment and Diversity Management Program," which describes the NRC's equal employment opportunity (EEO) programs and explains how the agency complies with federal EEO laws and regulations. The NRC proposed revising this MD to consolidate existing agency policies, provide more specific references to support those policies, and add language addressing recent court decisions, executive orders, and Equal Employment Opportunity Commission guidance. The OIG reviewed these revisions and recommended further changes to clarify that, given the NRC's status as an independent regulatory agency, not all executive orders to which the MD refers are necessarily binding on the agency. The OIG also recommended editorial changes to clarify the responsibilities of various NRC officials identified in the MD.

- MD 11.1, "NRC Acquisition of Supplies and Services," which provides general policy guidance for commercial and non-commercial NRC acquisitions. The OIG reviewed revisions to the MD that reflect organizational changes within the NRC, the deployment of new contract-writing software, and efforts to better align the MD with the Federal Acquisition Regulation (FAR). The OIG recommended changes to align the MD even better with the FAR and to clarify statements regarding the authority of certain NRC officials. The OIG also recommended changes to improve the organization of the MD and update certain references or citations within the document.

- MD 11.4, "NRC Small Business Program," which helps implement the agency's policy of providing the maximum practicable prime and subcontract opportunities to small businesses. The OIG reviewed revisions to this MD that incorporated changes to small-business-related laws, identified new duties and activities for the NRC's Small Business Program, clarified organizational responsibilities, and updated certain delegations of authority. The OIG provided comments on a section of the MD that describes the Inspector General's responsibilities and authorities. Specifically, the OIG recommended that the NRC staff revise the language in this section to emphasize that the OIG has general authority to investigate matters involving abuse related to the procurement system, including claims of whistleblower retaliation.

- MD 14.2, "Relocation Allowances," which provides guidance for the NRC staff in applying relocation provisions in the Federal Travel Regulation,

related executive orders, and Comptroller General decisions, as well as decisions of the United States Civilian Board of Contract Appeals. The OIG reviewed the addition of a Directive Handbook to this MD, as well as new language describing the role of a shared-service provider, and the services it provides, in connection with NRC relocations. The OIG recommended various changes to better align the MD's language with relevant provisions of the Federal Travel Regulation, as well as various editorial and formatting changes.

The OIG also reviewed the following MDs during the period covered by this Semiannual Report: MD 4.1, "Accounting Policy and Practices;" MD 9.6, "Organization and Functions, Office of Commission Appellate Adjudication;" MD 9.10, "Organization and Functions, Office of the Secretary;" MD 10.6, "Use of Consultants and Experts;" and, MD 10.12, "Use of Advisory Committee Members." While the OIG provided editorial or formatting suggestions for some of these MDs, we had no substantive comments on these documents.

DNFSB Directives

- D-421.1, "Defense Nuclear Facilities Safety Board Records Management Program," which establishes policies and assigns responsibilities for managing records at the DNFSB. The OIG reviewed revisions to this directive, recommending changes that provide context for certain statements and clarify the responsibilities of various DNFSB officials. The OIG also recommended certain editorial or organizational changes to the directive.

- D-22.1, "Internal Control Program," which establishes the policy, requirements, and responsibilities through which the DNFSB implements provisions in the Federal Managers' Financial Integrity Act of 1982 and OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control." The DNFSB's revisions to this directive focused on capturing organizational changes within the agency, including the role of its Executive Director for Operations. The OIG suggested minor editorial changes to the directive but did not have substantive comments.

Other OIG Activities

Newly Appointed Deputy Inspector General

On May 2, 2022, Ziad Buhaissi became the OIG's new Deputy Inspector General. Mr. Buhaissi joined the NRC OIG in February 2012 as a Senior Auditor. Since then, he has served the OIG in several progressively more responsible positions, including as Audit Manager for the Nuclear Materials and Waste Safety/Security audit team, Audit Manager for the Corporate Support audit team, and most recently, Director of Resource Management and Operations Support.

Prior to coming to the NRC OIG, Mr. Buhaissi served as Senior Auditor for the Special Inspector General for Iraq Reconstruction from 2007 to 2012, and as a Senior Program Analyst for the U.S. State Department for several years. He is the recipient of the 2016 and 2018 Council of the Inspectors General on Integrity and Efficiency Audit Awards for Excellence, the Department of State Meritorious Honor Award, the Defense of Freedom Medal (Civilian Purple Heart) and the Global War on Terrorism Medal from the Secretary of Defense.

Mr. Buhaissi holds a Bachelor's degree in Business Administration with a minor in Management Information Systems from the University of Wisconsin-Milwaukee.

Newly Appointed Assistant Inspector General for Audits

On September 12, 2022, Hruta Virkar became the new Assistant Inspector General for Audits (AIGA) in the NRC OIG. Previously Ms. Virkar served as the Director for the Division of Financial Advisory Services at the National Institutes of Health, overseeing contracts and grants for all commercial organizations within the U.S. Department of Health and Human Services. Ms. Virkar's previous assignments over her 22 year, 0511 series auditing career include: The Department of Energy, Office of the Inspector General, Team Leader; the former Washington Telephone Federal Credit Union (now known as Signal Financial Federal Credit Union), Internal Auditor and Compliance Officer; Deleon & Stang, CPA, Senior Auditor and Accountant; and, Cambridge Scientific Abstracts, Staff Accountant.

Ms. Virkar is a Certified Public Accountant and Certified Compliance Officer. She holds an Associate's Degree in Accounting from Montgomery College, as well as a Bachelor's Degree in Physics, and a Master's Degree in Computer Science, both from the University of Mumbai (formerly the University of Bombay) in India.

Newly Created Technical Services Office

TSO Team Members: Pictured left to right are William Schuster, Senior Engineer, Terri Spicher, Team Leader, and Andy Hon, Senior Engineer.

On August 15, 2022, the NRC OIG announced the creation of the Technical Services Office (TSO). The TSO will oversee the execution of the OIG's technical program, providing customer-service and operational support within the OIG. This support will include expert engineering and technical analysis, as well as advice and assistance on investigations, audits, evaluations, event inquires, and other OIG work. The TSO team consists of nuclear engineers and technical advisors with extensive scientific and engineering backgrounds, and with both federal agency and private sector work experience.

The Inspector General along with OIG staff and NRC senior resident inspectors, touring Vogtle Electric Generating Plant.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

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

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

NRC AUDITS

Audit Summaries

Audit of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA for Fiscal Year 2022

OIG Strategic Goal: Corporate Management

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 CLA to conduct an independent audit of the NRC's overall information security program and practices in response to the FY 2022 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 weaknesses in the risk management, supply chain risk management, identity and access management, security training, and information security continuous monitoring domains of the FY 2022 IG FISMA Reporting Metrics.

(Addresses Management and Performance Challenge #5)

Audit of the NRC's Strategic Workforce Planning Process

OIG Strategic Goal: Corporate Management

Strategic Workforce Planning (SWP), also called human capital planning, is the development of long-term strategies for acquiring, developing, and retaining an organization's total workforce to meet the needs of the future. The NRC established an agencywide SWP process that addresses two critical needs: (1) aligning the agency's human capital program with its current and emerging mission and programmatic goals; and, (2) developing long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals.

After piloting a phased SWP approach, the NRC implemented the annual, agencywide, Enhanced SWP process to help the agency plan for its workforce needs for 5 years beyond the current fiscal year.

The audit objective was to assess the effectiveness of the NRC's SWP process.

Audit Results:

The OIG found that the NRC's SWP process effectiveness can be optimized. Specifically, the Enhanced SWP process needs consistent and complete information, and timely human capital planning.

(Addresses Management and Performance Challenge #6)

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

OIG Strategic Goal: Safety

A drop-in meeting is a type of non-public meeting that occurs at the NRC. The NRC staff uses both public and non-public meetings to interact with external stakeholders. The agency's policy exempts drop-in meetings from certain requirements governing its public meetings, including the requirements to post a meeting notice and summary.

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

Audit Results:

The OIG found that little guidance exists for drop-in meetings and other informal non-public interactions with external stakeholders. The absence of a

structured process reduces transparency and places too much reliance on the ability of individual staff members to conduct such meetings appropriately. The NRC can take measures to clarify, for both the staff and the general public, its expectations regarding drop-in meetings and informal non-public interactions with external stakeholders.

(Addresses Management and Performance Challenge #1)

Audit of the NRC's Management Controls for Material Export Licensing

OIG Strategic Goal: Safety

The NRC is authorized to license the export of special nuclear material, source material, and byproduct material. The NRC reviews each application to ensure the proposed material export will not be inimical to the safety and security of the United States and will be consistent with applicable agreements for peaceful use. Within the NRC, the Office of International Programs (OIP) carries out the agency's export licensing responsibilities. The Office of Nuclear Material Safety and Safeguards (NMSS) and the Office of Nuclear Security and Incident Response (NSIR) share export licensing responsibilities by providing evaluations that contribute to the OIP's ultimate licensing decision.

The audit objective was to assess the effectiveness of the NRC's management controls of material export licensing.

Audit Results:

The OIG did not identify any ineffectiveness in the management controls over the material export licensing process.

The OIG concluded the OIP, and its partner offices, address the internal control components and underlying principles.

(Addresses Management and Performance Challenge #7)

The Defense Contract Audit Agency's (DCAA) Audit Report Number 1451-2020V10100005

OIG Strategic Goal: Corporate Management

The OIG and the 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 the audit conclusions, monitoring their staff qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management, and follow up on agency actions initiated due to this report.

Audit Results:

At the request of the OIG, the DCAA audited Qi Tech LLC and provided the OIG with an audit report. The DCAA audit report, dated June 17, 2022, did not identify any questioned costs.

(Addresses Management and Performance Challenge #8)

The Defense Contract Audit Agency's (DCAA) Audit Report Number 1451-2020M10100003

OIG Strategic Goal: Corporate Management

The OIG and the 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 the audit conclusions, monitoring their staff qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management, and follow up on agency actions initiated due to this report.

Audit Results:

At the request of the OIG, the DCAA audited Advanced Systems Technology Management, Inc. and provided the OIG with an audit report. The DCAA audit report, dated June 8, 2022, identified questioned costs to be addressed by NRC management.

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Corporate Management

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

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:

The OIG determined for FY 2021 the NRC is compliant with the PIIA requirements.

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Safety

Gamma Knife® Technology
Source: NRC

The NRC develops specific licensing guidance, reviews license applications, and issues decisions on the applications for the use of emerging medical technologies (EMTs) regulated under 10 C.F.R. Part 35, Subpart K. Due to an anticipated growth in medical applications of radioisotopes and advancements in medical technologies, the NRC predicted that in FYs 2020–2023 there will be the potential need to evaluate up to 15 emerging medical technologies.

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

Audit Results:

The OIG found that the NRC's licensing processes for EMTs are generally efficient, and the NRC's current effort to revise its guidance-development process is intended to improve the efficiency of these processes. However, the OIG also found that strengthening the NRC's knowledge management practices related to EMTs would further support the NRC's efforts to improve EMT processes.

(Addresses Management and Performance Challenge #7)

Audits in Progress

Audit of the NRC's Information Technology Services and Support

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 Information Technology (IT) services and support. The total obligated dollar value of all BPA calls under GLINDA is approximately $5,337,586.

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

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

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Safety

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

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

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

(Addresses Management and Performance Challenge #7)

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

OIG Strategic Goal: Safety

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

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

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

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

(Addresses Management Performance Challenge #1)

Audit of the NRC's Voluntary Leave Transfer Program

OIG Strategic Goal: Corporate Management

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

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

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

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

Audit of the NRC's Fiscal Year 2022 Financial Statements

OIG Strategic Goal: Corporate Management

Under the Chief Financial Officers Act, the Government Management and Reform Act, and Office of Management and Budget (OMB) Bulletin 21-04, 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, 2022.

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 Performance Challenge #8)

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

OIG Strategic Goal: Corporate Management

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

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

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

(Addresses Management Performance Challenge #8)

Audit of the NRC's Process for Announcing Technical Staff Vacancies

OIG Strategic Goal: Corporate Management

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

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

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

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

(Addresses Management Performance Challenge #8)

Cooling tower at Vogtle Electric Generating Plant---Photo courtesy of Georgia Power

NRC INVESTIGATIONS

Investigative Summaries

Event Inquiry into the Nuclear Regulatory Commission's Oversight of the Auxiliary Feedwater System at Diablo Canyon Nuclear Power Plant

OIG Strategic Goal: **Safety**

Allegation:
Over the last few years, we reviewed multiple allegations reported to us regarding the NRC's oversight at Diablo Canyon Nuclear Power Plant (DCNPP), a plant with two reactors in Avila Beach, California. Several of those concerns involved the NRC's oversight of safety-related structures, systems, and components (SSCs). One such SSC is the auxiliary feedwater (AFW) system, which is important to a commercial nuclear power plant because it is a back-up water supply that can be used to cool the reactor if normal feedwater is out of service.

After a July 2020 AFW system failure that required Unit 2, one of DCNPP's nuclear reactors, to enter a shutdown mode for 8 days, we received specific allegations that the NRC had inadequately inspected the AFW system prior to the event. These allegations further raised questions as to whether there is less than optimal NRC oversight at the DCNPP. Therefore, we initiated an Event Inquiry to review the adequacy of the NRC's inspections of the AFW system prior to the July 2020 event.

Background:
On July 23, 2020, a DCNPP operator noticed water coming down from the Unit 2 AFW pipe gallery, an area of the plant commonly called the "pipe rack." The operator identified water leaking from under the insulation covering the 3-inch, carbon steel AFW pipe. DCNPP maintenance staff removed the degraded pipe insulation and found a 1/16-inch diameter hole leaking 3.9 gallons per minute of feedwater.

The licensee identified that the AFW piping had long-standing damage to the insulation and its aluminum covering, which allowed moisture and contaminants to be absorbed by the insulation and caused corrosion on the outside of the pipe.

Diablo Canyon Nuclear Power Plant
Source: NRC

At the time of discovery, Unit 2 was not producing electricity because the licensee was addressing a hydrogen leak in the Unit 2 Main Generator, but the AFW system was in service providing coolant to the unit.

Investigative Results:

During ROP inspections, the NRC failed to identify piping insulation that had long been in a degraded condition. This degradation led to a leak in the Unit 2 AFW system piping. At no time during the NRC's January and April 2020 AFW system inspections or during weekly plant status inspections, did the NRC report findings regarding any SSCs that exhibited defects, such as degraded insulation on the AFW system, that would impact function.

The NRC had not inspected the area where the leak occurred, even though its inspection report indicated that inspectors had conducted a complete walkdown of the AFW system in April 2020. A complete walkdown is a physical inspection that verifies that the selected system is correctly aligned and able to perform its intended safety function.

The combined number of hours NRC staff spent directly inspecting the Units 1 and 2 AFW systems was fewer (5 hours) than recommended in the applicable NRC inspection procedure (12 hours) for the complete walkdown in April 2020.

Since the event, the licensee has remedied the AFW system failure and made improvements to the system, and DCNPP continues to operate safely. Additionally, the NRC has since verified that the AFW system complies with regulatory requirements.

Impact:
The staff recommended inspector training on corrosion under insulation in the Inspection Manual, including specific training on understanding inspection objectives, requirements, and guidance. The staff plans to review the applicable Inspection Procedure to ensure its requirements and guidance are clear to internal and external stakeholders. The staff also plans to review the inspection program guidance to determine if additional direction or training should be included to ensure consistent inspection expectations for multiple unit sites.

(Addresses Management and Performance Challenge #1)

Alleged Discrimination Against an NRC Manager Based on Disability

OIG Strategic Goal: Corporate Management

Allegation:
We received an allegation that the NRC discriminated against a now-former SES employee when the employee returned to work after being on sick leave. The SES employee said he informed his supervisor that he would be on sick leave for approximately 2 months. Upon returning to the office, the employee was not placed back into his position, and was relegated to perform "busy work" not commensurate with the duties required of an SES employee. The SES employee subsequently chose to retire from the NRC in June 2020.

Investigative Results:
We did not substantiate that the NRC discriminated against the SES employee because regulations state that SES employees may be given other duties for a limited time; however, we did find that the employee's supervisor failed to adequately communicate with the employee because the supervisor neither knew when the employee was coming back to work, nor asked the employee about a return date. We also found that the supervisor may have been less than candid when briefing the SES employee's plan for returning to work at an Executive Resources Board (ERB) meeting. ERB members stated that the supervisor told them the SES employee could be out for up to 2 years and requested an acting SES employee to replace him, which was approved.

Agency Response and Impact:
We issued a report to the NRC Executive Director for Operations (EDO) with our findings on February 22, 2022. The agency responded on April 27, 2022, stating the NRC staff took several actions to address needed improvements to the ERB process, including updating the Internal SES Selection Process as a

follow up to the Chief Human Capital Officer's verbal reminder to the ERB on staffing processes. The NRC also improved its guidance by adding a purpose statement, a non-discrimination statement, and a process for details and rotations, not just solicitations of interest. NRC leadership also discussed the OIG's report on this matter with the employee's supervisor.

(Addresses Management and Performance Challenge #6)

Failure of the NRC to Follow Up on Reports of Unauthorized Storage of Nuclear Gauges

OIG Strategic Goal: Security

Allegation:

We received an allegation that the NRC is "failing the American people by allowing nuclear gauges to be stored at places not 'authorized' under the NRC rules." The alleger said, "Apparently, the NRC found that the company was storing nuclear gauges at a location not on the license but didn't follow up on the incident," and questioned if the NRC was "waiting for someone to build a dirty bomb before doing their job."

Investigative Results:

Portable nuclear gauges had been stored in an unauthorized location, and the NRC failed to inspect the licensee at the time the potential violation of 10 C.F.R § 30.34, Terms and conditions of licenses, was identified. Additionally, we found that there are no policies or procedures in place to document formal communication between a regional licensing branch and an inspection branch when potential violations are discovered. This investigation revealed that during licensing activities, licensing staff discovered a potential violation for an unauthorized storage location for four portable nuclear gauges and ultimately approved a license amendment request (LAR) contrary to guidance provided in NUREG-1556. Additionally, no follow-up inspections on that issue were performed until the next routine inspection.

The IMC 2800 inspection requirements of 5 years +/- 1 year do not completely align with the record retention requirements in 10 C.F.R. § 30.51. In particular, Section 30.51(a)(1) states that a licensee "shall retain each record of receipt of byproduct material as long as the material is possessed and for 3 years following transfer or disposal of the material." Similarly, 10 C.F.R. § 34.63(a) states that each licensee "shall maintain records showing the receipts and transfers of sealed sources and devices using DU [depleted uranium] for shielding and retain each record for 3 years after it is made." For this investigation, the licensee's 3-year record retention requirement following its

transfer of portable gauges had expired by the time the NRC performed the next routine inspection in 2019, resulting in insufficient records available to determine if the gauges were appropriately stored for the previous licensed years.

During the investigation, the OIG observed that the NRC does not perform separate security inspections for Category 4 licensees. In addition, licensees are only required to conduct background investigations for individuals requesting unescorted access to Category 1 or Category 2 quantities of radioactive material (or to the devices that contain the material), not where Category 4 quantities are involved. Furthermore, there is no requirement for individuals under federal investigation to report that information to the licensee, unless an individual is required to disclose the information as part of a background investigation/reinvestigation under 10 C.F.R. § 37.25(c), a provision that applies only where Category 1 or Category 2 material is involved. Finally, even if the NRC becomes aware of federal investigations involving employees of Category 4 licensees that are being conducted by other agencies, the NRC's current policies do not provide guidance regarding what actions, if any, the NRC should take based on that information.

Agency Response:
We issued a report to the EDO with our findings on June 14, 2022. The EDO responded on August 30, 2022.

Impact:
An NRC regional office updated the checklist used by license reviewers to ensure a timely review of potential inspection issues. The updated checklist includes an explicit instruction that any issues identified during a licensing review that should be considered for an inspection (including an inspection before the next routine interval) be documented via email to the Chief of the Materials Inspection Branch and the Chief of the Materials Licensing Branch.

This change will ensure that any potential violations identified during a license review are documented and communicated to the responsible management officials before a licensing review is complete so that a decision whether to follow up immediately or during the next routine inspection can be made timely. The NRC regional office also shared its updated licensing checklist with other regional offices.

The NRC staff is also considering the OIG's findings on recordkeeping requirements and security inspections for Category 4 licensees in ongoing program improvement activities.

(Addresses Management and Performance Challenge #7)

Office of Nuclear Reactor Regulation Allegedly Bypassing OGC to Issue Internal Guidance

OIG Strategic Goal: Corporate Management

Allegation:
We received an allegation that a risk assessment white paper on newly developed methods was signed without having addressed the OGC's objections on it, and without reconciling an open non-concurrence program item. It was alleged that the paper's author and another employee were responsible for removing the OGC from the paper's concurrence process to avoid the requirement to overcome the OGC's initial objections to the paper.

In addition, the alleger informed us he had been retaliated against when he was excluded from a leadership team meeting.

Investigative Results:
The OIG did not substantiate the alleger's concerns of misconduct because the white paper was deemed an internal document that contained recommendations from an employee to his supervisor. Furthermore, the employee's exclusion from the meeting is not considered retaliation because the meeting was informational and not decisional in nature, and the employee was not subject to any adverse action that would require additional OIG review. We issued clearance letters to the white paper's author and the other employee, and did not identify any retaliatory actions taken against the employee.

(Addresses Management and Performance Challenge #6)

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

The Consolidated Appropriations Act of 2014 provided that, notwithstanding any other provision of law, the Inspector General of the NRC was authorized in 2014, and in subsequent years, to exercise the same authorities with respect to the DNFSB, as determined by the Inspector General of the NRC, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App. 3) with respect to the NRC.

DNFSB MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in FY 2022*   ***(As identified by the Inspector General)***
Challenge 1: *Managing a productive organizational culture and climate.*
Challenge 2: *Ensuring the safe and effective acquisition and management of mission-specific infrastructure, including cyber, physical, and personnel security, and data.*
Challenge 3: *Ensuring a systematic safety focus in the DNFSB's technical oversight and reviews.*
Challenge 4: *Using the COVID-19 lessons learned to strengthen the DNFSB's readiness to respond to future mission-affecting disruptions.*
Challenge 5: *Managing the DNFSB's efforts to elevate its visibility and influence and to assess and improve its relationship with the DOE.*

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

DNFSB AUDITS

Audit Summaries

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

OIG Strategic Goal: Corporate Management

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 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 weaknesses in the risk management, configuration management, data protection and privacy, information security continuous monitoring, and contingency planning domains of the FY 2022 FISMA Reporting Metrics.

(Addresses Management and Performance Challenge #2)

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

OIG Strategic Goal: Corporate Management

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

program and activity. The PIIA requires the Office of the Inspector General (OIG) of each executive agency to determine agency compliance annually.

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

Audit Results:
The OIG determined that for fiscal year (FY) 2021, the DNFSB was not compliant with the PIIA. Specifically, the DNFSB did not meet all requirements for publishing and posting the annual financial statement and accompanying materials required under the PIIA and corresponding OMB guidance. At the same time, the OIG did not report any material internal control weaknesses.

(Addresses Management and Performance Challenge #2)

Audits in Progress

Audit of the DNFSB's Fiscal Year 2022 Financial Statements

OIG Strategic Goal: Corporate Management
Under the Chief Financial Officers Act, the Government Management and Reform Act, and OMB Bulletin 21-04, Audit Requirements for Federal Financial Statements, the OIG is required to audit the DNFSB's financial statements. The report on the audit of the agency's financial statements is due on November 15, 2022.

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)

DNFSB INVESTIGATIONS

Investigative Case Summaries

Alleged Violations of Provisions Regarding Nonpublic Collaborative Discussions

OIG Strategic Goal: Corporate Management

Allegation:
We received an allegation that the DNFSB improperly conducted nonpublic collaborative discussions (NCDs) to discuss technical matters. The use of NCDs allegedly bypassed meetings that would have produced a public record showing what transpired during the meetings. We also assessed whether the DNFSB violated any law by holding NCDs prior to November 29, 2021, the effective date of the DNFSB's new regulation reflecting its new authority to hold NCDs. In addition, we reviewed whether the DNFSB held informal votes during NCDs, in violation of NDAA Section 3202 and AEA Section 313(k)(1)(A). Finally, we reviewed whether the DNFSB properly documented summaries of the meetings for public review and whether the agency properly communicated information discussed during NCDs to agency staff.

Background:
The Government in the Sunshine Act, 5 U.S.C. § 552b (Sunshine Act), requires that the deliberative meetings of certain federal agencies, including the DNFSB, be open to the public unless one of the Act's 10 specified exemptions applies. The Act also includes requirements for publicizing meetings to which it applies, notifying the public if any portion of a meeting will be closed, and keeping certain meeting-related records.

To help facilitate collegial discussions at the DNFSB, in the NDAA for Fiscal Year 2021, Congress included an exception to the Sunshine Act that allows the DNFSB's members to discuss official business in non-public meetings. This provision, which took effect when the NDAA became law on January 1, 2021, amended the AEA to add Section 313(k), Nonpublic Collaborative Discussions.

Although Section 313(k) authorizes the DNFSB to engage in NCDs, it places certain conditions on these meetings. Among these conditions, "no formal or informal vote or other official action [can be] taken at the meeting." In addition, within 2 business days after the conclusion of an NCD, the DNFSB must make publicly available, "a list of the individuals present at the meeting," and, "a

summary of the matters, including key issues, discussed at the meeting." If the DNFSB determines that a matter may be withheld from the public under the Sunshine Act's provisions, the DNFSB shall nonetheless provide a publicly available summary with, "as much general information as possible with respect to the matter."

The DNFSB began holding NCDs in February 2021. The DNFSB also initiated a rulemaking to amend its Sunshine Act regulations at 10 C.F.R. Part 1704 to reflect its new authority to hold NCDs. On August 30, 2021, the DNFSB issued a direct final rule revising its regulations to add a new Section, 10 C.F.R. Section 1704.11, Nonpublic collaborative discussions, that reflected the provisions of AEA Section 313(k)(2). Section 1704.11 took effect November 29, 2021.

Investigative Results:

We found that the DNFSB began holding NCDs in February 2021 and thereafter used the NCDs to discuss a wide variety of topics, including technical matters. The DNFSB was authorized to hold NCDs under NDAA Section 3202, which amended AEA Section 313 effective January 1, 2021, to allow for such discussions. Although it was not until November 2021 that the DNFSB's Sunshine Act regulations in 10 C.F.R. Part 1704 reflected the agency's new authority to hold NCDs, the DNFSB did not violate the Sunshine Act by holding NCDs before that date because the AEA itself, as amended by the NDAA in January 2021, gave it the authority to do so.

AEA Section 313(k)(1) does, however, place several restrictions on NCDs, including a prohibition on holding formal or informal votes or taking other official action during NCDs. Additionally, Section 313(k)(2) requires that the DNFSB provide a summary of the matters discussed during NCDs within 2 business days of the closure of the meetings.

While AEA Section 313(k)(1)(A) prohibits the DNFSB from holding an "informal vote"—or a formal vote, for that matter—during an NCD, neither this section nor the DNFSB's implementing regulation at 10 C.F.R. Section 1704.11 defines what constitutes an "informal vote." Although we found no evidence that the NCDs, so far, have involved taking informal votes, we also found that the DNFSB does not appear to have formal policies or guidance to help its members understand what may constitute an informal vote. We, therefore, found that although the DNFSB does not appear to have violated AEA Section 313(k)(1)(A), there is an opportunity for the agency to develop policies or guidance to help promote compliance with this section.

Additionally, although the DNFSB has posted summaries of the NCDs on its public website, these summaries have tended to be very brief. Under AEA Section 313(k)(2)(A)(ii), the DNFSB must provide "a summary of the matters, including key issues, discussed at" each NCD. Although we did not find a violation of this provision, if the DNFSB continues preparing very brief summaries, it is recommended that it be mindful of not inadvertently excluding matters or key issues from the summaries.

Relatedly, we reviewed whether the DNFSB violated Section 313(k) by not providing NCD summaries for DNFSB staff review. We did not find any such violation, however, because Section 313(k) relates to the DNFSB's public disclosure obligations, rather than to internal agency disclosure. At the same time, we found that DNFSB senior technical managers, who were present at all NCDs held in 2021, could have more effectively communicated relevant information from the meetings to their staff.

Agency Response:
We issued a report to the DNFSB Chair with our findings on April 4, 2022. The Chair responded June 30, 2022.

Impact:
The DNFSB's career leadership met to discuss concerns within the agency. It also hosted brown bag (educational) sessions led by the General Counsel to provide an overview of NCDs, discuss the Board's use of NCDs, and solicit questions from the staff related to NCDs. The Board also committed to revise its *Government in the Sunshine Act* Operating Procedure, which contains the agency's internal procedures for NCDs. The revisions will explain what constitutes an "informal vote," facilitate internal dissemination of information, and otherwise clarify what is permissible for the Board and agency staff in connection with NCDs.

Vogtle Electric Generating Plant---Photo courtesy of Georgia Power

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

April 1, 2022 – September 30, 2022

Allegations Received: 81 (31 received from the NRC OIG Hotline)

Investigative Statistics

Source of Allegations

NRC Employee	25
NRC Management	17
General Public	12
Other Government Agency	2
Anonymous	22
Contractor	1

Disposition of Allegations

Reviewed (no additional Action needed)	29
Correlated to Existing OIG Investigation	5
Referred to New OIG Investigation	10
Referred to Audits	3
Referred to NRC Management	29
Pending Disposition	5
TOTAL:	**81**

Status of Investigations

Federal	
DOJ Referrals	1
DOJ Declinations	0
DOJ Pending	2
Criminal Convictions (Arrests)	0
Criminal Information/Indictments	1
Criminal Penalty Fines	0
Civil/Administrative Recovery Administrative	1
Recovery Amount - $ 1,385.86	
State and Local	
State and Local Referrals	1
NRC Administrative Actions	
Review of Agency Process	2
Change of Issue Process	0
Pending Agency Action	0
Suspensions and Demotions	0

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	1	0	0	0	1
Event Inquiry	2	0	0	0	2
Internal Fraud	1	0	0	0	1
Management Misconduct	5	3	4	1	4
Miscellaneous	1	0	0	0	1
Proactive Initiatives	1	0	1	0	0
Technical Allegations	5	1	2	2	4
Critical Risk – High	2	1	0	0	3
Theft	0	1	0	0	1
Whistleblower Reprisal	0	2	0	0	2
External Fraud	0	3	0	0	3
False Statements	0	1	0	0	1
TOTAL:	**18**	**12**	7	**3**	**23**

**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
09/29/2022	Audit of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2022.	OIG-22-A-14
09/26/2022	Audit of the NRC's Strategic Workforce Planning Process	OIG-22-A-13
08/12/2022	Audit of the NRC's Drop-in Meeting Policies and Procedures	OIG-22-A-12
08/03/2022	Audit of the NRC's Management Controls for Material Export Licensing	OIG-22-A-11
07/13/2022	The Defense Contract Audit Agency's (DCAA) Audit Report Number 1451-2020V10100005	OIG-22-A-10
07/12/2022	The Defense Contract Audit Agency's (DCAA) Audit Report Number 1451-2020M10100003	OIG-22-A-09
06/06/2022	Audit of the NRC's Fiscal Year 2021 Compliance with Improper Payment Laws	OIG-22-A-08
05/09/2022	Audit of the NRC's Process for Licensing Emerging Medical Technologies	OIG-22-A-07

NRC Contract Audit Reports

OIG Issue Date	Contractor/Title/ Contractor No.	Questioned Costs	Unsupported Costs
July 13, 2022	**Advanced Systems Technology Management, Inc.** Independent Audit Report on Advanced Systems Technology Management, Inc.'s Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Year Ended December 31, 2020 NRC-HQ-7G-14-C-0001 31310020C0004	$281,079	$0
July 14, 2022	**Qi Tech LLC** Independent Audit Report on Qi Tech LLC's Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Year Ended December 31, 2020 NRC-HQ-7G-14-C-0001	$0	$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	4	$2,013,928	0
B. Which were issued during the reporting period	1	$281,079	0
Subtotal (A + B) ‡	5	$2,295,007	0
C. For which a management decision was made during the reporting period:			
i. Dollar value of disallowed costs	0	0	0
ii. Dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	5	$2,295,007	0

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

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

Table II

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

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

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

Table III

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

No data to report

SUMMARY OF OIG ACCOMPLISHMENTS AT THE DNFSB

April 1, 2022 – September 30, 2022

Source of Allegations

Allegations Received from the DNFSB OIG Hotline: 1

Investigative Statistics

Source of Allegations

DNFSB Employee	n/a
DNFSB Management	2
Intervenor	n/a
General Public	n/a
Other Government Agency	n/a
Anonymous	1
Contractor	n/a
Regulated Industry (Licensee/Utility)	n/a
OIG Self-Initiated	n/a
TOTAL:	**3**

Disposition of Allegations

Correlated to Existing Case	1
Referred to OIG Investigations	2
Referred to OIG Audit	n/a
Referred to Other Agency	n/a
Referred to DNFSB Management	n/a
Pending Review Action	n/a
TOTAL:	**3**

Status of Investigations

Federal	
DOJ Referrals	n/a
DOJ Declinations	n/a
DOJ Pending	n/a
Criminal Information/Indictments	n/a
Criminal Convictions	n/a
Criminal Penalty Fines	n/a
Civil Recovery	n/a
Other Recovery	n/a
State and Local	
State and Local Referrals	n/a
State Accepted	n/a
Criminal Information/Indictments	n/a
Criminal Convictions	n/a
Criminal Penalty Fines	n/a
Civil Recovery	n/a
DNFSB Administrative Actions	
Counseling and Letter of Reprimand	n/a
Terminations and Resignation	n/a
Suspensions and Demotions	n/a
Review of Agency Process	1

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	1	0	0	0	1
Management Misconduct	1	2	1	0	2
Proactive Initiatives	1	0	0	0	1
TOTAL:	**3**	**2**	**1**	**0**	**4**

**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
09/29/2022	Audit of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2022.	DNFSB-22-A-07
07/27/2022	Audit of the DNFSB's Fiscal Year 2021 Compliance with Improper Payment Laws	DNFSB-22-A-06

DNFSB Audit Resolution Activities

Table I

OIG Reports Containing Questioned Costs*

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

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

Table II

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

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

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

UNIMPLEMENTED AUDIT RECOMMENDATIONS

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

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

5 of 7 recommendations open since April 29, 2020

Recommendation 2: Use the fully defined ISA to:

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

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

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

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

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

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

3 of 13 recommendations open since June 2, 2020

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

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

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

Audit of the NRC's Property Management Program

(OIG-20-17)

5 of 7 recommendations open since September 30, 2020

Recommendation 2: Include the receipt, management, and proper disposal of IT assets planned and currently tracked in Remedy within the property management program. This may include, but is not limited to, actions such as:

(a) updating MD 13.1, Property Management, to designate Remedy as the property tracking system specifically for IT assets;
(b) updating MD 13.1 to include the NRC IT Logistics Index policy for inputting IT assets greater than or equal to $2,500, or which contain NRC information or data within the property management program;
(c) specify in the updated MD 13.1, the use of unique identifiers to track and manage those IT assets within the NRC property management program;
(d) Specify in the updated MD 13.1, the methods and documentation of periodic inventories using unique identifiers within the NRC property management program;
(e) provide appropriate acquisition information in excess property reporting for IT assets that contain NRC information or data; and,
(f) ensure IT assets in the property disposal process comply with documenting media sanitation in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1: *Guidelines for Media Sanitization*.

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

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

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

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

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

3 of 3 recommendations open since March 9, 2021

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

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

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

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

11 of 13 recommendations open since March 19, 2021

Recommendation 2: Use the fully defined ISA to:

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

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

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

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

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

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

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

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

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

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

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

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

2 of 4 recommendations open since March 29, 2021

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

Recommendation 4: Conduct periodic training regarding RPS data input.

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

1 of 1 recommendation open since August 4, 2021

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

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

3 of 4 recommendations open since August 19, 2021

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

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

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

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

4 of 5 recommendations open since September 23, 2021

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

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

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

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

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

8 of 8 recommendations open since September 28, 2021

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

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

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

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

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

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

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

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

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

1 of 6 recommendations open since September 30, 2021

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

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

17 of 18 Recommendations open since December 20, 2021

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

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

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

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

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

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

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

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

Recommendation 10: Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems by continuing efforts to implement these capabilities using automated tools.

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

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

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

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

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

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

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

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

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

2 of 4 Recommendations open since January 19, 2022

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

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

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

8 of 8 Recommendations open since February 9, 2022

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

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

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

Recommendation 4: Clearly define CFSI.

Recommendation 5: Include a CFSI category in the AMS.

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

Recommendation 7: Develop CFSI training for inspectors.

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

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

(OIG-22-A-07)

1 of 1 Recommendation open since May 9, 2022

Recommendation 1: Enhance the efficiency of the emerging medical technology licensing and guidance development processes by compiling a list of emerging medical technology-related guidance and information in a centralized location for NRC staff and Agreement State officials.

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

4 of 4 Recommendations open since August 12, 2022

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

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

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

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

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

3 of 3 Recommendations open since September 26, 2022

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

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

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

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

7 of 7 Recommendations open since September 29, 2022

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

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

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

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

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

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

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

DNFSB

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

6 of 6 recommendations open since January 27, 2020

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

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

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

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

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

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

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

7 of 11 recommendations open since March 31, 2020

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

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

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

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

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

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

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

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

14 of 14 recommendations open since March 25, 2021

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

Recommendation 2: Use the fully defined ISA to:
(a) Assess enterprise, business process, and information system level risks;
(b) Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions;
(c) Conduct an organization wide security and privacy risk assessment; and,
(d) Conduct a supply chain risk assessment.

Recommendation 3: Using the results of recommendation 2:

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

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

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

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

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

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

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

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

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

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

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

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

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

1 **of 2 recommendations open since November 5, 2021**

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

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

3 of 3 recommendations open since December 20, 2021

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

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

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

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

24 of 24 recommendations open since December 21, 2021

Recommendation 1: Update the ISA and use the updated ISA to:

(a) Assess enterprise, business process, and information system level risks; and,
(b) Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.

Recommendation 2: Using the results of recommendations 1:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommendation 18: Consistently test the incident response plan annually.

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

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

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

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

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

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

Results of the Audit of the Defense Nuclear Facilities Safety Board's Financial Statements for Fiscal Year 2021 (DNFSB-22-A-05)

1 of 7 recommendations remain open since January 31, 2022

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

Audit of the DNFSB's Fiscal Year 2021 Compliance with Improper Payment Laws (DNFSB-22-A-06)

3 of 3 recommendations open since July 27, 2022

Recommendation 1: Submit annual data call documentation to the OMB, as required by OMB Circular A-136.

Recommendation 2: Include the paymentaccuracy.gov link in the annual AFR, as required by Appendix C to OMB Circular A-123.

Recommendation 3: Develop and implement a process for continuous monitoring of financial statutory requirements.

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

11 of 11 Recommendations open since September 29, 2022

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

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

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

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

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

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

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

(a) Prioritizing mitigation in accordance with all requirements specified by CISA BOD 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities and Emergency Directives, as applicable;

(b) Opening plans of action and milestones to track critical and high vulnerabilities that cannot be addressed within 30 days; and,

(c) Preparing risk-based decisions in unusual circumstances when there is a technical or cost limitation making mitigation of a critical or high vulnerability infeasible with documented, effective compensating controls coupled with a clear timeframe for planned remediation.

Recommendation 8: Implement a solution to gradually automate, orchestrate and centralize patching for each device.

Recommendation 9: Develop and implement a data consistency and quality plan or similar procedure to help test and monitor data accuracy and quality of information coming from their implementation of CDM.

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

Recommendation 11: Document and implement a process to validate that the DNFSB GSS ISCP is tested annually, and any issues discovered during the contingency plan test are remediated timely.

ABBREVIATIONS AND ACRONYMS

AFW	Auxiliary Feedwater
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
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
IAM	Issue Area Monitoring
IG	Inspector General
IT	Information Technology
MD	Management Directive
NCD	Nonpublic Collaborative Discussion
NRC	Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OEDO	Office of the Executive Director for Operations
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIP	Office of International Programs
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act of 2019
SSC	Safety-related Structures, Systems, and Components
SWP	Strategic Workforce Planning

REPORTING REQUIREMENTS

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

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

APPENDIX

Peer Review Information

Audits

The NRC OIG audit program was peer reviewed by the OIG for the Smithsonian Institution. The review was conducted in accordance with Government Auditing Standards and Council of the Inspectors General on Integrity and Efficiency (CIGIE) requirements. In a report dated September 30, 2021, the NRC OIG received an external peer review rating of *pass*. This is the highest rating possible based on the available options of *pass, pass with deficiencies, or fail.* The review team issued a Letter of Comment, dated September 30, 2021, that sets forth the peer review results and includes a recommendation to strengthen the NRC OIG's policies and procedures.

Investigations

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

The NRC OIG Hotline

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

What should be reported:

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

Ways To Contact the OIG

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

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

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