U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Semiannual Report to Congress

October 1, 2020—March 31, 2021

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:

The NRC's One White Flint North Building.

A MESSAGE FROM THE INSPECTOR GENERAL

On behalf of the Office of the Inspector General, U.S. Nuclear Regulatory Commission and Defense Nuclear Facilities Safety Board, it is my pleasure to present this Semiannual Report to Congress, covering the period from October 1, 2020 to March 31, 2021. I continue to be grateful for the opportunity to lead this extraordinary group of managers, auditors, investigators, and support staff, and I'm extremely proud of their exceptional work.

During this reporting period, we issued eleven audit and evaluation reports, and recommended several ways to improve NRC and DNFSB safety, security, and corporate management programs. We also opened fourteen investigative cases and completed nineteen, two of which were referred to the Department of Justice or State's Attorney's Office, and five 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 inspection issue screening program; material control and accounting inspection program; the NRC and DNFSB information security programs and practices; and, agency compliance with applicable Executive Orders. We also highlighted our review of NRC and DNFSB financial statements, and identified the most serious management and performance challenges facing the NRC and the DNFSB in fiscal year (FY) 2021. Further, this report includes summaries of cases involving interference with inspection findings, oversight of decommissioning trust funds, improper management of safety inspection programs, possession of prohibited stocks or securities, fraudulent invoices, contract award administration, and invalid contracts.

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

Robert J. Feitel

Robert J. Feitel
Inspector General

The NRC Headquarters complex.

CONTENTS

A routine inspection at the Calvert Cliffs Nuclear Power Plant in Lusby, Maryland.

HIGHLIGHTS

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

Audits

Nuclear Regulatory Commission

- The U.S. Nuclear Regulatory Commission (NRC) inspection guidance requires inspectors to screen issues of concern identified at nuclear power plants to determine whether the issues in question fall under the agency's traditional enforcement (TE) program and the Reactor Oversight Process (ROP). Under the ROP, if an issue of concern screens positive for a performance deficiency, inspectors must determine if it has minor or more-than-minor safety or security significance. When screening issues of concern under the TE pathway, inspectors do not use the ROP screening process to screen TE violations, but rather, use the process to screen for performance deficiencies. The NRC Office of the Inspector General (OIG) assessed the consistency with which NRC staff screen issues of concern for TE and ROP in accordance with agency guidance.

- The OIG and the Defense Contract Audit Agency (DCAA) have an interagency agreement whereby the DCAA provides contract audit services for the OIG. At the request of the OIG, the DCAA audited Southwest Research Institute's (SwRI) contract costs and provided the OIG with an audit report. SwRI is an independent and nonprofit research and development organization benefiting the government, industry, and the public through innovative science and technology. The DCAA audit report did not identify any questioned costs.

- The OIG engaged SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the NRC's overall information security program and practices to respond to the FY 2020 Inspector General (IG) Federal Information Security Management Act (FISMA) Reporting Metrics. The FISMA was enacted in 2014 and outlined the information security management requirements for agencies, including the requirement for an annual independent assessment by the agency IG. Additionally, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. The report found weaknesses in the information security program and practices that may have some impact on the agency's ability to adequately protect the NRC's systems of information.

- The NRC grants licenses for the possession and use of special nuclear material (SNM) and establishes regulations to govern its possession and use. Among the NRC's licensees, fuel cycle facilities are licensed to process and handle SNM to manufacture fuel used by commercial nuclear power reactors to generate electricity. The NRC's regulations require that SNM license holders have material control and accounting (MC&A) systems to prepare and maintain

accounting records, perform measurements, and analyze the information to confirm the presence of nuclear materials. The basic objective of MC&A is to protect against the loss or misuse of SNM. MC&A are activities the licensee and the NRC use to promptly confirm that SNM has not been lost, stolen, or diverted. The OIG examined the effectiveness of the NRC's MC&A inspection program over the accounting and control of SNM at fuel facilities.

- Executive Order (Order) 13950, Combating Race and Sex Stereotyping, dated September 22, 2020, required federal agencies, federal grantees, federal contractors, and the Uniformed Services to address training sessions that included divisive concepts, race or sex stereotyping, and race or sex scapegoating. Section 6(c)(ii) of the Order stated that each agency head shall request the agency IG to thoroughly review and assess by the end of the calendar year and not less than annually thereafter, agency compliance with the requirements of this order in the form of a report submitted to the Office of Management and Budget (OMB). The OIG assessed agency compliance with the requirements of the Order. Executive Order 13950 was rescinded, however, on January 25, 2021.

- The Chief Financial Officers Act of 1990 (CFO Act), as amended, requires the IG or an independent external auditor, as determined by the IG, to annually audit the NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG retained CliftonLarsonAllen (CLA) to conduct this audit, which includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. It also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. In addition, the audit evaluated the effectiveness of internal controls over financial reporting and the agency's compliance with laws and regulations.

- The Reports Consolidation Act of 2001 (Public Law 106-531) requires the OIG to annually update our assessment of the NRC's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. In this report, we summarize what we consider to be the most critical management and performance challenges to the NRC, and we assess the agency's progress in addressing those challenges. Congress left the determination and threshold of what constitutes a most serious management and performance challenge to the IG's discretion. This year, the OIG identified eight areas representing challenges the NRC must address to accomplish its mission better. We have compiled this list based on our audit, evaluation, and investigative work; general knowledge of the agency's operations; evaluative reports of others, including the U.S. Government Accountability Office (GAO); and, input from NRC management.

Defense Nuclear Facilities Safety Board

- The OIG contracted with SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2020. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with the Council of Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. The FISMA of 2014 outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by the agency's OIG. In addition, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. SBG evaluated the effectiveness of the information security policies, procedures, and practices of the DNFSB.

- The Accountability for Tax Dollars Act of 2002 (ATDA) requires the IG or an independent external auditor, as determined by the IG, to annually audit the DNFSB's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG retained CLA to conduct this annual audit. CLA examined the DNFSB's FY 2020 agency financial report, which includes comparative financial statements for FYs 2020 and 2019.

- On September 22, 2020, the President issued Executive Order (Order) 13950, Combating Race and Sex Stereotyping. In accordance with section 6(c)(ii) of the Order, the DNFSB's Acting Chairman requested that the OIG review and assess the DNFSB's compliance with the Order in the form of a report submitted to the OMB by the end of calendar year 2020 and not less than annually thereafter. The OIG assessed agency compliance with the requirements of Executive Order 13950, which was rescinded on January 25, 2021.

- The Reports Consolidation Act of 2000 (Public Law 106-531) requires us to annually update our assessment of the DNFSB. The IG provides what he considers to be the most serious management and performance challenges facing the DNFSB in FY 2021. Congress left the determination and threshold of what constitutes the most serious management and performance challenges to the discretion of the Inspectors General. The IG has defined serious management and performance challenges as mission critical areas or programs that have the potential for a perennial weakness or vulnerability that, without substantial management attention, would seriously impact agency operations or strategic goals. The OIG identified five management and performance challenges facing the DNFSB for FY 2021.

Investigations

Nuclear Regulatory Commission

- An anonymous alleger reported that a nuclear power plant had experienced loss of shutdown cooling incidents since the early 2000s and was unable to use backup cooling systems as required by the NRC for such incidents. Though the NRC issued violations for the first incidents, the agency did not respond to the more recent incidents that occurred. The alleger said that in 2013, when visiting NRC inspectors tried to issue a violation for an incident, the then-NRC senior resident inspector (SRI) intervened on behalf of the plant, and the visiting inspectors instead issued the plant an unresolved item (URI), which remained unresolved for more than 3 years. Further, the alleger reported that when another incident occurred in 2016, the NRC ignored the fact that the plant could not use a backup cooling system, and that the SRI may have intervened on behalf of the plant concerning other violations proposed by visiting inspectors.

- The OIG initiated two separate investigations into the NRC's role in the oversight of expenditures from trust funds used for the radiological decommissioning of nuclear power plants. In one investigation, a public stakeholder and a state public utilities regulator reported concerns that the NRC does not adequately oversee individual decommissioning trust fund (DTF) expenditures. In the other investigation, a retired NRC branch chief alleged that NRC managers did not question the licensee's expenditures of $162 million on planning, insurance, and taxes from its DTF in the year prior to its sale and license transfer. Both investigations alleged possible misuse of the funds, including the inappropriate use of DTFs to dismantle cooling towers.

- An alleger reported the NRC did not completely perform its Primary Mission Essential Function of threat assessment and dissemination during 2017–2018, and that an NRC headquarters office hindered members of the region's Intelligence Liaison and Threat Assessment Team from performing its mission.

- An anonymous alleger reported that a regional nuclear materials safety inspection program had been mismanaged; specifically, required inspections were not completed and internal metrics were falsified. Further, the alleger said that unqualified inspectors performed inspections and that some inspectors were unaccompanied.

- The NRC provided information that an employee disclosed that he owned a fund listed on the NRC's Prohibited Securities List. The NRC Office of the General Counsel (OGC) addressed the issue with the employee by requiring him to divest the fund. When he did not, the OGC requested the OIG review circumstances surrounding the employee's ownership of the prohibited fund, and whether the employee was involved in any regulatory matter related to the prohibited fund.

- The agency reported that fraudulent requests for quotes and purchase orders were sent to companies across the country, purportedly from an NRC Acquisition Management employee.

Defense Nuclear Facilities Safety Board

- DNFSB Board Members expressed concerns regarding the DNFSB's award of a U.S. Small Business Administration (SBA) 8(a) set-aside contract. The Board Members requested that we evaluate the circumstances surrounding the DNFSB's award of a human resources contract and whether the procurement process was handled consistent with the SBA's processes and Federal Acquisition Regulation requirements.

- An alleger reported that a DNFSB contractor performed information technology work for the DNFSB without a valid contract and without receiving payment for those services, which may have caused the DNFSB to violate the Antideficiency Act.

Power lines from Indian Point Nuclear Power Station in Buchanan, New York.

OVERVIEW OF THE NRC AND THE OIG

The NRC's Mission

The NRC was formed in 1975, in accordance with the Energy Reorganization Act of 1974, to regulate the various commercial and institutional uses of nuclear materials. The agency succeeded the Atomic Energy Commission, which previously had responsibility for both developing and regulating nuclear activities. 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.
- **Waste** – Transportation, storage, and disposal of nuclear materials and waste, and decommissioning of nuclear facilities from service.

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

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

OIG History, Mission, and Goals

OIG History

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

In response, Congress passed the landmark legislation known as the Inspector General Act (IG) Act, which President Jimmy Carter signed into law in 1978. The IG Act created independent 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 the prosecution of thousands of wrongdoers. In addition, the IG concepts of good governance, accountability, and monetary recovery encourage foreign governments to seek advice from IGs, with the goal of replicating the basic IG principles in their own governments.

OIG Mission and Goals

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

The OIG is committed to ensuring the integrity of NRC programs and operations. Developing an effective planning strategy is a critical aspect of meeting this commitment. Such planning ensures that audit and investigative resources are used effectively. To that end, the OIG developed a *Strategic Plan* that includes the major challenges and critical risk areas facing the NRC. The plan identifies the OIG's priorities and establishes a shared set of expectations regarding the goals it expects to achieve and the strategies that will be employed to do so. 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 evolvingthreat environment; and,

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

Reactor containment building.

OIG PROGRAMS AND ACTIVITIES

Audit Program

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

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

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

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

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

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

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

- Misconduct by high-ranking NRC officials and other NRC officials, such as managers and inspectors, whose positions directly impact public health and safety;
- Failure by NRC management to ensure that health and safety matters are appropriately addressed;
- Failure by the NRC to appropriately transact nuclear regulation publicly and candidly and to openly seek and consider the public's input during the regulatory process;
- Conflicts of interest involving NRC employees and contractors and licensees, including such matters as promises of future employment for favorable or inappropriate treatment, and the acceptance of gratuities; and,
- Fraud in 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

Pursuant to 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 each agency concerning their impact on the economy and efficiency of agency programs and operations.

Regulatory review is intended to provide assistance and guidance to the agency prior to the concurrence process to avoid formal implementation of potentially flawed documents. The OIG does not concur or object to the agency's actions reflected in the regulatory documents, but rather offers comments.

Comments provided in regulatory review reflect an objective analysis of the language of proposed agency statutes, directives, regulations, and policies resulting from OIG insights from audits, investigations, and historical data and experience with agency programs. OIG review is structured to identify vulnerabilities and offer additional or alternative choices.

To effectively track the agency's response to OIG regulatory reviews, significant comments include a request for written replies within 90 days, with either a substantive reply or status of issues raised by the OIG.

From October 1, 2020 to March 30, 2021, the OIG reviewed a variety of agency documents. In its regulatory reviews, the OIG is cognizant of potential impacts to its functions as well as potentially negative impacts on its independence from the agency. In addition to impacts on OIG functions, some of the documents reviewed could have a major impact on NRC or DNFSB operations or are of high interest to NRC or DNFSB staff and stakeholders, and the OIG's regulatory reviews reflect its knowledge and awareness of underlying trends and overarching developments at each agency and in the industry it regulates. OIG regulatory reviews also reflect auditing and investigative activities. Comments may reflect issues first noted in the context of an audit or investigation.

The OIG did not identify any issues that would have a serious impact on its independence or conflict with its audit or investigatory functions during its review of agency documents during this time; however, some of its reviews identified proposed staff polices that might impact the work of the OIG. In these cases, the OIG proposed edits or changes that would mitigate these impacts and requested a response from the staff. Agency staff either accepted the OIG's proposals or offered a well-supported explanation as to why the proposed changes were not accepted. These reviews are described in further detail below.

NRC Directives

- MD 8.2, "NRC Incident Response Program." This directive outlines the NRC's policies and procedures for responding to incidents or emergencies involving facilities and materials licensed and regulated by the NRC.

This MD includes a potential role for the OIG: providing law enforcement advice, particularly with respect to computer forensics, as needed. Permitting this, even if only anticipated to be used in extremely rare exigent circumstances, has the potential to be of great benefit to the health and safety of the public and the physical and technological security of licensed facilities in the event of an emergency.

More importantly, the MD provides for notification to the OIG whenever the Incident Response Program is activated so that the OIG can send staff to observe the NRC response in each instance, if it so chooses. Observing the agency's response activities can be a precursor to audit or investigative activities that may arise from either the incident activating the NRC's incident response, or of the response itself.

OIG's review of, and comments on, the directive were focused on clarifying the provisions regarding OIG involvement and access to ensure that OIG will be informed of any initiation of an incident response, while still ensuring OIG independence.

- MD 4.6, "License Fee Management Program." This directive establishes regulations and procedures for the NRC's statutorily-mandated license fee assessment program as well as ensuring that supporting financial data is appropriately captured. Approximately 90 percent of the NRC's budget is recovered from fees issued to licensees and applicants, and the fee-billing program is governed by many statutory and regulatory requirements. The fee-billing program has been the subject of past and ongoing audits, including the annual Financial Statements Audit. While the OIG's review resulted in only minor comments on the directive, the review was focused on ensuring that the Fee Management Program continues to be conducted in a manner that supports efficiency and effectiveness of agency operations.

- MD 10.102, "Labor-Management Relations Program for Federal Employees." This directive ensures compliance with applicable laws, regulations, and agreements regarding labor-management relations, and supports a constructive climate for labor-management relations. Because of the nexus between Labor-Management Relations and investigating and addressing employee misconduct, the OIG has a particular interest in this directive. Although the OIG review did not result in any substantive comments, it assured that the directive continues to be drafted in a way that protects against misconduct, and supports the efficient and effective conduct of agency business.

- MD 2.6, "Information Technology Infrastructure." This directive provides information and usage guidance for the NRC's Information Technology (IT) infrastructure for NRC employees and contractors. Among the topics covered in this directive is the reporting of any misuse of technology infrastructure by NRC employees or contractors to the OIG for potential investigation.

The OIG's review focused on ensuring that this reporting would take place under the directive, and the OIG offered comments clarifying the procedures for reporting suspected misuse as well as the scope of the OIG's authority to review suspected misuse.

- MD 13.4, "Transportation Management." This directive establishes the policies for appropriate use of government-owned vehicles and managing the NRC parking program in addition to encouraging the use of public transportation and ride-sharing by NRC employees. The OIG's review of this directive focused on ensuring that the OIG can continue to investigate, as necessary, any vehicle misuse or fraud as well as ensuring that the agency's transportation programs will be able to be managed effectively and efficiently. The OIG offered comments that protected the OIG's ability to investigate potential misuse which have the potential to save the agency from being required to pay for costs associated with employee or contractor misuse or negligence.

DNFSB Directive

Directive D21.1, "Directives Program." This directive provides the framework for the DNFSB's entire directives program, including provisions detailing OIG review of directives and disposition of OIG comments on directives. The OIG's review focused on ensuring that the OIG maintains its independence and ability to complete a thorough and necessary review of all future directives so each directive protects against fraud, waste, and abuse, and supports the effectiveness and efficiency of DNFSB operations.

Other OIG Activities

OIG General Counsel Awarded a CCIG Leadership Award

Support for CCIG COVID-19 Response

In response to the COVID-19 public health crisis, the Council of Counsels to Inspectors General (CCIG) created a COVID-19 Working Group to facilitate information-sharing among counsels to Inspectors General government-wide, and to create an efficient means of sharing legal research resources across the OIG community. The NRC OIG General Counsel joined the COVID-19 working group (CV19WG), and was in charge of creating a uniform organization and nomenclature system on the OMB-MAX platform. Her efforts simplified CCIG-community access to diverse CV19WG documents, and kept the system up-to-date with real-time filings. For her work in this leadership role, the NRC OIG General Counsel was awarded a CCIG Leadership Award.

Deputy Inspector General David C. Lee, Retired

David Lee, Former Deputy Inspector General

In March 2021, Mr. David C. Lee, OIG Deputy Inspector General, retired after 56 years of distinguished federal service. Upon his retirement, Mr. Lee had served as the NRC Deputy Inspector General since October 27, 1996. He also served as the Acting Inspector General for the NRC and the DNFSB from January 2019 until July 2019, and, as Deputy Inspector General, continued to exercise the delegated authority of the Inspector General until May 2020.

Prior to working at the NRC, Mr. Lee served 31 years with the U.S. Secret Service. Mr. Lee was a member of the Senior Executive Service as the Assistant Director of the Office of Protective Research, and earlier as the Assistant Director for the agency's Office of Administration.

Newly Appointed Assistant Inspector General for Investigations

Malion Bartley, Assistant Inspector General for Investigations

Malion Bartley has been appointed the Assistant Inspector General for Investigations for the NRC OIG. Mr. Bartley has been a federal civilian special agent for more than 25 years, serving at the Air Force Office of Special Investigations (OSI) and the NRC OIG. His previous assignments include NRC Deputy Assistant Inspector General for Investigations, cybercrimes special agent, Department of Defense certified polygraph examiner, Air Force special agent, and the leader of the Air Force OSI Surveillance Detection Team.

Mr. Bartley is a graduate of the Federal Executive Institute and the Council of Inspectors General on Integrity and Efficiency (CIGIE) Experienced Leaders Program. He holds a bachelor's degree from Howard University and a master's degree from Central Michigan University. Mr. Bartley is also a member of several national level law enforcement and professional organizations.

Mr. Bartley has received numerous professional and military awards, including CIGIE Awards of Excellence, the Inspector General Award for significant contributions to an OIG, and the Meritorious Civilian Service Award for conducting law enforcement operations that greatly protected the safety of U.S. personnel in high threat areas from foreign intelligence services and terrorism.

Prototype concrete casks at the Palo Verde Energy Education Center.

NRC MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Nuclear Regulatory Commission in FY 2021*

(as identified by the Inspector General)

Challenge 1: *Strengthening Risk-Informed Regulation.*

Challenge 2: *Regulatory Oversight of Decommissioning Trust Funds.*

Challenge 3: *Management of the NRC's Response to the COVID-19 Pandemic.*

Challenge 4: *Readiness for New Technologies for Reactor Design and Operation.*

Challenge 5: *Continuous Improvement Opportunities for Information Technology (IT), Internal IT Security and Information Management.*

Challenge 6: *Strategic Workforce Planning.*

Challenge 7: *NRC and Agreement State Coordination on Oversight of Materials and Waste.*

Challenge 8: *Management and Transparency of Financial and Acquisitions Operations.*

** For more information on these challenges, see OIG-21-A-01, "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC." (https://www.nrc.gov/docs/ML2029/ML20290A681.pdf).*

NRC AUDITS

Audit Summaries

Audit of the NRC's Power Reactor Inspection Issue Screening

OIG Strategic Goal: Safety

NRC guidance (Inspection Manual Chapter 0612) requires inspectors to screen issues of concern identified during nuclear power reactor inspections to determine whether the issues in question fall under the agency's traditional enforcement (TE) program and Reactor Oversight Process (ROP). Under the ROP, if an issue of concern screens positive for a performance deficiency, inspectors must determine if it has minor or more-than-minor safety or security significance. When screening issues of concern under the TE pathway, inspectors do not use the ROP screening process to screen TE violations. Rather, they use that process to screen for performance deficiencies.

The objective was to assess the consistency with which NRC staff screen issues of concern for TE and ROP under agency guidance.

Audit Results:

NRC staff screen issues of concern under agency guidance. However, the NRC could benefit from clarifying guidance to periodically review the consistency with which the staff documents inspection results in the agency's reactor program system, and in inspection reports.

(Addresses Management Challenge # 1)

The Defense Contract Audit Agency (DCAA Audit Report Number 3311-2019W10100001

OIG Strategic Goal: Corporate Management

The OIG and the DCAA have an interagency agreement whereby the DCAA provides contract audit services for the OIG. At the request of the OIG, the DCAA audited SwRI and provided the OIG with an audit report. SwRI is an independent and nonprofit research and development organization benefiting the government, industry, and the public through innovative science and technology. Founded in 1947, SwRI provides contract research and development services to industrial and government clients in the United States and abroad. SwRI's headquarters is in San Antonio, Texas, and the firm has supporting offices throughout the United States. SwRI's total revenue was $673.7 million for FY ended September 27, 2019. Approximately 60 percent of the FY 2019 revenue was derived from U.S. government contracts, and the remaining revenue relates to commercial contracts and subcontracts. SwRI had 3,001 employees in FY 2019.

Audit Results:
The DCAA audit report did not identify any questioned costs.

(Addresses Management and Performance Challenge #8)

Independent Evaluation Report of the NRC's Implementation of the FISMA for FY 2020

OIG Strategic Goal: Security
The FISMA was enacted in 2014 and outlined the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. Additionally, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and develop strategies and best practices to improve information security.

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

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

Evaluation Results:
The evaluation found weaknesses in the information security program and practices that may have some impact on the agency's ability to adequately protect the NRC's systems of information.

(Addresses Management and Performance Challenge #5)

Audit of the NRC's Material Control and Accounting Inspection Program for Special Nuclear Material

OIG Strategic Goal: Safety
The NRC grants licenses for the possession and use of special nuclear material (SNM) and establishes regulations to govern the possession and use of those materials. Among the NRC's licensees, fuel cycle facilities are licensed to process and handle SNM to manufacture fuel used by commercial nuclear power reactors, in order to generate electricity. The NRC's regulations require that SNM license holders have material control and accounting (MC&A) systems to prepare and maintain accounting records, perform measurements, and analyze the information to confirm nuclear materials' presence. The basic objective of MC&A is to protect

against the loss or misuse of SNM. MC&A are activities the licensee and the NRC use to promptly confirm that SNM has not been lost, stolen, or diverted.

The Office of Nuclear Material Safety and Safeguards (NMSS) is responsible for the MC&A Inspection program. NMSS typically performs routine inspections on a semiannual to annual basis. However, the NRC can conduct reactive inspections as necessary in response to an event. Certified inspectors with specialized training and experience in material control and accounting perform all inspections.

The audit objective was to assess the effectiveness of the NRC's inspection program for the accounting and control of special nuclear material at fuel fabrication facilities.

Audit Results:
The NRC's implementation of the MC&A program has opportunities to improve communication between agency offices, to strengthen the human capital approach to MC&A qualifications, and to update training. The report made three recommendations to enhance the MC&A program.

(Addresses Management and Performance Challenge #7)

Audit of the NRC's Compliance with Executive Order 13950, Combating Race and Sex Stereotyping

OIG Strategic Goal: Corporate Management
Executive Order (the Order) 13950, Combating Race and Sex Stereotyping, dated September 22, 2020, required federal agencies, federal grantees, federal contractors, and the Uniformed Services to address training sessions that included divisive concepts, race or sex stereotyping, and race or sex scapegoating. Section 6(c)(ii) of the Order stated that each agency head shall request the agency Inspector General to thoroughly review and assess agency compliance with the requirements of this Order in the form of a report submitted to the OMB. The OIG assessed agency compliance with the requirements of the Order.

The audit objective was to review and assess agency compliance with the requirements of Executive Order 13950.

Audit Results:
The OIG found that the NRC was in the process of becoming fully compliant with the Order. Of the nine requirements reviewed, eight were complete and one was in progress. The Executive Order was rescinded on January 25, 2021.

(Addresses Management and Performance Challenge #6)

Audit of the NRC's Fiscal Year 2020 Financial Statements

OIG Strategic Goal: Corporate Management

The Chief Financial Officers Act of 1990, as amended (CFO Act), requires the IG or an independent external auditor, as determined by the IG, to annually audit the NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG retained CLA to conduct this annual audit. CLA examined the NRC's FY 2020 Agency Financial Report, which includes financial statements for FY 2020.

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

Audit Results:

In CLA's opinion, the NRC's financial statements present fairly, in all material respects, the NRC's financial position as of September 30, 2020 and 2019, its net cost of operations, changes in net position, and budgetary resources in accordance with U.S. generally accepted accounting principles. Also, in CLA's opinion, because of a material weakness in internal control over leases and leasehold improvements, the NRC did not maintain, in all material respects, effective internal control over financial reporting as of September 30, 2020, based on criteria established under the Federal Manager's Financial Integrity Act of 1982.

(Addresses Management Challenge #8)

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

OIG Strategic Goal: Corporate Management, Safety, and Security

The Reports Consolidation Act of 2001 (Public Law 106-531) requires the IG to annually update our assessment of the NRC's most serious management and performance challenges facing the agency, and the agency's progress in addressing those challenges. In this report, we summarize what we consider to be the most critical management and performance challenges to the NRC, and we assess the agency's progress in addressing those challenges.

Congress left the determination and threshold of what constitutes a most serious management and performance challenge to the Inspector General's discretion. We identify management challenges as those that meet at least one of the following criteria:

1. The issue involves an operation critical to the NRC Mission or an NRC Strategic Goal;

2. There is a risk of fraud, waste, or abuse of NRC or other government assets;

3. The issue involves strategic alliances with other agencies, the Office of Management and Budget, the Administration, Congress, or the public; and,

4. The issue involves the risk of the NRC not carrying out a legal or regulatory requirement.

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

(Addresses Management and Performance Challenges #1–7)

Audits in Progress

Audit of the NRC's Grants Pre-Award Program

OIG Strategic Goal: Corporate Management

In FYs 2018 - 2019, the NRC awarded 53 and 45 grants, respectively, totaling $15.5 million and $14.8 million to universities for scholarships, fellowships, and faculty development grants. In addition, the agency awarded grants to trade schools and community colleges. The NRC intends grant funding to help support education in nuclear science, engineering, and related trades to develop a workforce capable of the design, construction, operation, and regulation of nuclear facilities and the safe handling of nuclear materials. NRC's grant program benefits the nuclear sector broadly, not primarily the NRC.

The NRC's grant program supported over 500 students annually during that time, but directed most grant money to university faculty and university curriculum development. At the same time, the NRC notes a critical workforce need in the trade and craft areas of nuclear education and observes that outreach to pre-college students is essential to enable students to make informed decisions about pursuing the study of nuclear technology.

The audit objectives are to determine if the NRC's policies and procedures for reviewing proposals for grants, and for making awards: (1) comply with applicable federal regulations and agency guidance; and, (2) establish and maintain adequate internal controls over the program.

(Addresses Management Challenge # 8)

Audit of the NRC's Oversight of Licensee Use of Decommissioning Trust Funds

OIG Strategic Goal: Corporate Management

The NRC must obtain reasonable assurances from nuclear reactor licensees that funds will be available for the decommissioning process before operations begin. As a means of oversight of licensees decommissioning funding assurance (DFA), licensees are required to provide a DFA status report to the NRC biennially. Five years prior to permanent cessation of operations, licensees are required to provide the DFA status reports annually. Prior to, or within two years after permanent cessation of operations, licensees are required to submit a Post Shut-Down Decommissioning Activity Report that includes a description and schedule for the planned decommissioning activities, and a site-specific cost estimate.

Decommissioning trust funds may be used by licensees if: (a) the withdrawals are for expenses for legitimate decommissioning activities consistent with the definition of decommissioning in § 50.2; (b) expenditures would not reduce the value of the decommissioning trust below an amount necessary to place and maintain the reactor in a safe storage condition if unforeseen conditions or expenses arise; and, (c) withdrawals would not inhibit the ability of the licensee to complete

funding of any shortfalls in the decommissioning trust needed to ensure the availability of funds to ultimately release the site and terminate the license.

The audit objective is to determine if the NRC's oversight of licensee use of decommissioning trust funds is adequate.

(Addresses Management Challenge # 2)

Audit of the NRC's Prohibited Securities Program

OIG Strategic Goal: Corporate Management

NRC employees at a certain professional level are prohibited from owning stock in companies that would conflict with NRC work. These NRC employees, as well as their spouses and minor children, are prohibited by regulation from owning any securities issued by entities on the most recent list published annually by the Office of the General Counsel. The NRC policies and procedures on this regulation are contained in Management Directive 7.7, "Security Ownership."

Employees who become subject to this restriction as a result of initial employment or subsequent assignment to a covered position are required to certify that they are following the NRC security ownership restrictions. The employee has 90 days from the date of appointment to divest those securities. The employee should inform the Office of the General Counsel when the securities are divested. The deadline can be extended in cases of unusual hardship, and the divestiture requirement can be waived under extremely limited circumstances, such as legal constraints that prevent divestiture.

The objective of this audit is to determine whether the NRC has established and implemented an effective internal control system over the NRC security ownership process.

(Addresses Management Challenge # 8)

Audit of the NRC's Pandemic Oversight of Nuclear Power Plants

OIG Strategic Goal: Safety

On January 31, 2020, the U.S. Department of Health and Human Services declared a public health emergency (PHE) for the United States to aid the nation's healthcare community in responding to Coronavirus Disease 2019 (COVID-19). On March 11, 2020, the COVID-19 outbreak was characterized as a pandemic by the World Health Organization. State and local jurisdictions rapidly enacted social distancing guidelines recommended by the Centers for Disease Control. NRC offices and NRC-licensed facilities took steps to protect their employees and mitigate the spread of a novel disease in their communities.

The NRC's Reactor Oversight Process Baseline Inspection Program requires resident and regional inspectors to complete a minimum number of samples in various inspection procedures. NRC inspectors continued to inspect licensed nuclear power facilities, using new tools and guidance from NRC Headquarters and Regions.

However, staffing changes at both the NRC and licensee facilities limited inspectors' ability to complete some scheduled baseline activities.

The audit objective is to assess the NRC's policies and procedures for conducting reactor inspections during the COVID-19 public health emergency, and identify best practices that could be during future pandemics or other public health emergencies.

(Addresses Management Challenge # 3)

Audit of COVID-19 Impact on Nuclear Materials and Waste Oversight

OIG Strategic Goal: Safety

On January 31, 2020, the U.S. Department of Health and Human Services declared a public health emergency (PHE) for the United States to aid the nation's healthcare community in responding to the Coronavirus Disease 2019 (COVID-19). The NRC recognized that during the COVID-19 PHE, licensees may experience challenges in meeting certain regulatory requirements. The NRC has increased communications with licensees to understand the impact of COVID-19 on facility operational status, and any potential compliance issues.

The NRC issued a letter to its byproduct material, uranium recovery, decommissioning, fuel facilities, and spent fuel storage licensees, outlining the regulatory options to seek regulatory relief, including: (1) exemptions from regulatory requirements; (2) amendments to license conditions or technical specifications; and, (3) enforcement discretion. Typical requests involve relief from routine actions such as conducting audits, inventories, and completing employee retraining/recertification. The NRC considers the exemption requests on a case-by-case basis and, if the requirements for an exemption are met, provides written approval of an exemption for a specific period of time.

Requests for relief are only granted if the NRC staff finds that they do not have a significant impact on safety or security. While providing relief from regulatory requirements, the NRC continues to assure that licensed facilities are operating safely during the COVID-19 PHE.

The audit objective is to assess and evaluate the NRC's nuclear materials and waste oversight processes during the COVID-19 pandemic.

(Addresses Management Challenge # 3)

Audit of the NRC's Implementation of the Enterprise Risk Management Process

OIG Strategic Goal: Corporate Management

The OMB substantively updated OMB Circular No. A-123 (OMB A-1213) in 2016. It includes Enterprise Risk Management (ERM), as a means to coordinate with strategic planning and strategic review established by the Government Performance

and Results Modernization Act of 2010, and the internal control processes required by the Federal Manager's Financial Integrity Act, and the Government Accountability Office's Standards for Internal Control in the Federal Government. This change to OMB A-123 is meant to integrate governance structure to improve mission delivery, reduce costs, and focus corrective actions toward key risks. Implementation of the revised OMB A-123 will engage all agency management beyond the traditional ownership of OMB Circular No. A-123 by the Chief Financial Officer community. It requires leadership from the agency's Chief Operating Officer and Performance Improvement Officer, and close collaboration across all agency mission and mission-support functions.

The NRC revised its MD 4.4, Enterprise Risk Management and Internal Control, in December 2017, to address the updates to OMB A-123. MD 4.4 establishes the agency's ERM framework, and provides a structured approach to managing risk that incorporates internal control, risk management, and enterprise risk management in the context of agency governance.

The objective of this audit is to determine whether the NRC's Enterprise Risk Management process is being implemented following OMB A-123.

(Addresses Management Challenge # 8)

Resident Inspectors perform a walk-down at Calvert Cliffs Nuclear Power Plant.

NRC INVESTIGATIONS

Investigative Case Summaries

Alleged NRC Staff Interference with Inspection Findings at a Nuclear Power Plant

OIG Strategic Goal: Safety

Allegation:

We initiated this investigation based on an anonymous allegation that a nuclear power plant had experienced loss of shutdown cooling incidents since the early 2000s, and was unable to use backup cooling systems as required by the NRC for such incidents. Further, though the NRC issued violations for the first incidents, the agency did not respond to the more recent incidents that occurred. The alleger said that in 2013, when visiting NRC inspectors tried to issue a violation for an incident, the then-NRC SRI intervened on behalf of the plant, and the visiting inspectors instead issued the plant a URI, which remained unresolved for more than 3 years. Further, when another incident occurred in 2016, the "NRC ignored the fact that the plant could not use a backup cooling system." The alleger also said it was rumored that the SRI intervened on behalf of the plant concerning other violations proposed by visiting inspectors.

Investigative Results:

There were four incidents at this power plant between 2004 and 2016 when shutdown cooling equipment was inoperable, and the plant did not have an alternate decay heat removal system available, in violation of a plant technical specification (TS). The NRC enforced the compliance concerns inconsistently by reacting to each incident of the same noncompliance differently: twice the NRC chose not to issue a violation, and twice it issued an NCV against two different regulations. The licensee has been allowed to not fully address a TS violation since 2004, and further changes to the standard technical specifications are still being considered by the licensee for compliance.

We did not find evidence that the SRI intervened on behalf of the licensee, but determined that a visiting inspector and the SRI had a disagreement regarding the proposed violation, which resulted in an open URI.

We provided our results of this case to the agency because of the inconsistent enforcement of compliance concerns and the lack of a time limit to remedy URIs. Although in this case a URI was open for more than 3 years, this is not an isolated problem because as of August 2020, the agency had 12 URIs, and some of them date back to 2013.

Agency Response:

The agency responded to our findings regarding the timeliness of URI resolution, the inconsistency in addressing a licensee's repeat noncompliance with technical specifications, and the status of the noncompliance specific to the plant. The agency

reported that there has been noticeable improvement in the timely closure of URIs within the 1-year metric. As of November 13, 2020, there were 11 open URIs, only 3 of which have been open for longer than 1 year. Agency management communicated the expectation that staff work to resolve URIs within 1 year of issuance, and that all URIs are discussed with licensees at each End of Cycle meeting.

The agency also reported that staff are reviewing related guidance to ensure overall consistency and transparency across all inspection procedures, and are working to provide additional guidance on the threshold of minor versus more-than-minor performance deficiencies.

In addition, cross-regional panels, with the support of headquarters staff, have been established to review proposed inspection findings with the intent of providing consistency in dispositioning issues. Furthermore, a weekly agency-wide inspector knowledge transfer session was hosted by an NRC Program Office to discuss various technical subjects. Both forums allowed inspectors and headquarters staff to discuss a variety of plant issues, and gain a common understanding of operating experience and reasoning for dispositioning technical issues, including design basis requirements.

(Address Management and Performance Challenge #1)

NRC's Oversight of Decommissioning Trust Fund Expenditures

OIG Strategic Goal: Safety

Allegation:

We initiated two separate investigations into the NRC's role in the oversight of expenditures from trust funds used for the radiological decommissioning of nuclear power plants. In one investigation, a public stakeholder and a state public utilities regulator reported concerns that the NRC does not adequately oversee individual decommissioning trust fund (DTF) expenditures. In the other investigation, a retired NRC branch chief alleged that NRC managers did not question the licensee's expenditures of $162 million on planning, insurance, and taxes from its DTF in the year prior to its sale and license transfer. Both investigations alleged possible misuse of the funds, including the inappropriate use of DTFs to dismantle cooling towers.

Investigative Results:

We did not identify misconduct by NRC staff or managers during these investigations, and determined that NRC managers reviewed the alleger's concerns by submitting them to the NRC's Allegation Review Board (ARB), which inspected the plant's financial and cooling tower information and issued requests for information to validate it. We reviewed the ARB's results and determined that the NRC followed its allegation process in reviewing the alleger's claims. The NRC

also concluded in correspondence to the stakeholder that there was no evidence of any violations of the NRC's DTF program requirements. We determined that NRC senior managers were aware of the licensee's administrative expenditures disbursed from the plant's DTF, as reported in the staff's Safety Evaluation Report (SER) for the license transfer and the licensee's Pre-Notice of Disbursement from Decommissioning Trust, and that the radiologically-contaminated cooling towers were included in the SER, and approved by the NRC in the plant's Post-Shutdown Decommissioning Activities Report.

We did find that though NRC staff members were aware of the DTF expenses, they did not review individual trust fund expenditures, and managers lacked specific guidance that would help them determine appropriate DTF use. In one plant that we reviewed, no entity except one had ever inspected or done a prudency review to verify that individual expenditures were used for authorized purposes. Although NRC inspection procedure (IP) 36801, "Organization, Management, and Cost Controls at Permanently Shutdown Reactors," includes evaluating decommissioning cost expenditures among matters NRC staff may inspect, we found that from 2010 to 2018, decommissioning cost expenditures had not been discussed in NRC inspection reports for this plant. We also learned that regional decommissioning inspectors had not evaluated expenditures because they did not have adequate knowledge to perform that objective of IP 36801. As a result, approximately $1.2 billion of this plant's individual decommissioning expenditures had not been verified.

We learned that an NRC Reactor Decommissioning Financial Assurance Working Group (WG) has already recommended improvements to existing DTF oversight guidance documents. For example, prior to requesting withdrawals from a decommissioning trust, the licensee must complete and submit to the NRC, a Pre-Notice of Disbursement from Decommissioning Trust. The WG found that the required notices do not provide sufficient detail for the staff to review and determine that the funds will be used for authorized radiological decommissioning purposes. We found that there is no formal review of these notices, nor are they included in IPs.

Senior executives at the plant agreed that the current information required by the NRC is not sufficient to verify the funds are being spent appropriately. Furthermore, NRC inspectors have never requested to review expenditure documentation despite a license condition at this plant giving the NRC 30 days to review the withdrawal request prior to disbursement, and all financial expenditure information being readily available onsite for review by inspectors. We found that such a license condition for review is not required by NRC regulations, so other plants in decommissioning without one would not be subject to notifying the NRC prior to withdrawing funds from the trust.

Agency Response:

The agency responded to our findings with the results of the WG's report, which concluded that the NRC has a robust regulatory, licensing, and oversight framework for power reactor decommissioning financial assurance. The WG, however, did draft a report recommending enhancements to the NRC power reactor

decommissioning financial assurance guidance and procedures implementing the licensing and oversight processes, to improve program effectiveness, efficiency, and transparency. The WG invited public comment to its draft report, which yielded additional items that were addressed through the ongoing efforts of the WG and the Steering Committee for Reactor Decommissioning Financial Assurance.

Impact:
With approximately 17 power plants nationwide currently in decommissioning, and more than $10 billion residing in DTFs, the NRC's current and planned oversight process leaves the DTF program susceptible to fraud, waste, and abuse. As a result of these investigations, the OIG has committed to continue reviewing whether and to what extent the NRC is overseeing DTFs, and their potential for misuse and fraud. The OIG currently has an audit in process on this issue and will plan future investigations and audits as needed.

(Addresses Management and Performance Challenge #2)

Concerns Pertaining to A Lack of Program Management within an NRC Headquarters Office

OIG Strategic Goal: Security

Allegation:
We completed an investigation into allegations that the NRC did not completely perform its Primary Mission Essential Function of threat assessment and dissemination during 2017 and 2018, and that the NRC headquarters Intelligence Liaison and Threat Assessment Branch (ILTAB) hindered members of the regional Intelligence Liaison and Threat Assessment Team (ILTAT) from performing its mission.

Investigative Results:
We found that the ILTAT identified what it felt were three credible threats that were not disseminated to NRC licensees, which appeared to violate NRC Management Directive (MD) 8.2, "Incident Response Program." Specifically, during 2017 and 2018, the ILTAT identified threats to licensees regarding: (1) suspicious activity at hospitals; (2) multiple flyovers of unmanned aerial vehicles (UAVs) over two licensee sites; and, (3) 3-D printed weapons passing undetected through certain magnetometers.

We provided our results of this case to the agency and, while we did not find evidence that the ILTAB actively hindered the ILTAT's execution of duties, we did find that the ILTAB's failure to disseminate the threats stemmed from conflicting opinions between the ILTAT and the ILTAB regarding what constituted a credible threat. We found that NRC guidance lacked specific criteria on how to determine credible threats, and how to reconcile different staff and management opinions. Further, we found that the NRC's procedures for Information Assessment Team Advisories (IATAs) and Security Advisories (SAs), the two primary communication

means for disseminating threat information to licensees, require multiple staff and management involvement in a single task, which reduces the efficiency and effectiveness of the processes.

Impact:
The agency responded to our findings, explaining that the relationship between ILTAB and ILTAT had not been effective due to mistrust between them. In addition, they did not use agency processes, such as the Differing Professional Opinion or Non-Concurrence Process, to resolve any disagreements.

Working Relationship
To resolve this issue, NRC headquarters worked with the region to develop and implement a corrective action plan to improve the working relationship, which included having ILTAB and ILTAT staff review pertinent guidance regarding the use of IATAs and SAs, and elevate disputes to the agency's division director or deputy division director. Since these actions have been implemented, staff from both ILTAB and ILTAT have stated that the relationship has greatly improved.

Criteria for Determining Threats
The agency committed to review relevant documents to determine whether the procedures contain adequate instructions to determine which identified threats are credible and warrant issuance of a generic communication. If revision is needed, the agency pledged to complete the action by July 30, 2022, and continues to work closely with regions to ensure the procedures to evaluate and identify potential credible threats for dissemination to applicable licensees, are consistent and effective.

IATAs and SAs
The agency committed to assess the procedures for disseminating threat information to licensees to improve efficiency and agility. This will include identifying opportunities to streamline concurrences or timelines for generic communications, and identifying approaches to provide prompt situational awareness to licensees. This action is scheduled to be completed by July 30, 2021.

(Addresses Management and Performance Challenge #1)

Improper Management of Safety Inspection Programs

OIG Strategic Goal: Safety

Allegation:
The OIG completed an investigation into anonymous allegations that a regional nuclear materials safety inspection program had been grossly mismanaged. Specifically, it was alleged that required inspections were not completed and internal metrics were falsified. Further, the alleger said that unqualified inspectors performed inspections, and that some inspectors were unaccompanied.

Investigative Results:
We found that a region's uranium recovery (UR) inspection program was mismanaged. First, between 2014 and 2018, the program failed to meet inspection

requirements and contained document deviations from Inspection Manual Chapters (IMC) 2641 and 2801. More than 30 UR licensee sites had required inspections that were overdue, including 6 where inspections were more than 1,000 days overdue. Second, although we did not substantiate that the NRC falsified metrics, we did determine that the region's metric calculation for UR timeliness gave the incorrect appearance that the region met 100 percent of its timeliness goals. Furthermore, we found that the metric excludes UR operating site inspections.

We did not substantiate that unqualified inspectors performed inspections; however, we did determine that supervisors or senior staff did not conduct annual accompaniments of each uranium recovery inspector to assess performance and ensure consistent application of inspection policies.

In addition, we found that MD 9.26, "Organization and Functions Office of Nuclear Material Safety," was last updated in 1989, and no longer reflects current practice.

We proactively investigated potential management misconduct regarding an Integrated Materials Performance Evaluation Program (IMPEP) Inspection, and did not substantiate management misconduct.

Impact:

The agency responded to our investigation by addressing three issues: (1) documentation of deviations from inspection manuals; (2) timeliness metrics for UR inspections; and, (3) the age of NRC MD 9.26.

Documentation Deviations

NRC headquarters agreed that expectations should be made clearer for the documentation of program adjustments, such as deviations and variances from IMCs. Moreover, headquarters has tasked that expectations be updated to: (1) specify a timeframe for periodic review of each IMC; (2) clearly define program adjustments or deviations and determine the decisionmaker for such adjustments; and, (3) require documentation of such adjustments be sent to the business line lead.

The agency also provided programmatic direction clarifying that deviations from the prescribed inspection interval should accommodate extenuating circumstances, specifically but not exclusively due to COVID-19, and should be documented and signed by regional management with a courtesy copy to the respective program owner in NRC headquarters. The agency believes this programmatic direction should also help resolve the OIG observation that the methodology for calculating the timeliness performance indicator involves rescheduled inspections still being considered on time, though outside the IMC timeliness provisions. The region also developed a process to document management decisions when inspections needed to be deferred or rescheduled, and created desk guides intended to reduce the occurrence of overdue inspections, and ensure inspection findings are communicated to the licensee in a timely manner.

In addition, the region developed a supervisory job aid to better identify and document when supervisory inspection accompaniments are necessary and completed.

Timeliness Metric Calculation

A new FY 2021 business line performance indicator was added to the agency's organizational performance management system. The indicator is designed to comprehensively cover inspection completion timeliness for both operating and decommissioning UR facilities that track the percent of required UR decommissioning inspections completed in accordance with IMC 2801. The new performance indicator provides internal controls for the UR oversight program which are consistent with other NRC oversight programs, and will help ensure a system of tracking, accountability, enterprise risk management, and management attention for overdue inspections.

MD 9.26

A revised MD 9.26 is nearing issuance, and its format and content have been updated to be consistent with other Volume 9 MDs, and to reflect business line lead responsibilities.

(Addresses Management and Performance Challenge #1)

Employee Possessing Prohibited Stocks or Securities

OIG Strategic Goal: Corporate Management

Allegation:

The OIG completed an investigation based on information from the NRC that an employee disclosed, on his Office of Government Ethics Form 450, Confidential Financial Disclosure, that he owned a fund that was listed on the NRC's Prohibited Securities List. The alleger told the OIG that the OGC addressed the issue with the employee by requiring him to divest the fund. When he did not, the agency requested the OIG review circumstances surrounding the employee's ownership of the prohibited fund, and whether the employee was involved in any regulatory matter related to the prohibited fund.

Investigative Results:

We determined that since 2008, the employee held the prohibited fund and retired on August 31, 2020, in lieu of divesting the holdings. We also found that as a technical reviewer, responsible for conducting reviews of such items as license amendment requests and task interface agreements, the employee was not able to influence the result, or make any final decisions, regarding these requests or agreements. We could not determine, however, if the employee's involvement in such activities had a direct impact on his financial interest or the financial interest of the prohibited fund. The employee requested a waiver from the NRC Chairman, explaining that his loss would be more than $50,000 if the stocks were sold. When the employee's waiver request was denied, he opted to retire. The OIG referred this investigation to the Department of Justice, which declined to prosecute the matter.

(Addresses Management and Performance Challenge #8)

Fraudulent Invoices Purportedly From the NRC

OIG Strategic Goal: Corporate Management

Allegation:

The OIG completed an investigation based on information provided by the Office of the Chief Information Officer that fraudulent requests for quotes and purchase orders were sent to a Colorado company and other companies across the country, purportedly from an NRC Acquisition Management employee.

Investigative Results:

We found that the NRC employee was not involved in the scheme and that the perpetrators had used his email address to commit the fraudulent purchases. We could not determine the identity of those responsible for sending the fraudulent request to any of the companies. Although we traced the fraudulent activity to overseas origination, websites, and final shipment destinations, we could not determine the exact location of the originating emails. We shared the information with the FBI, which was already investigating similar allegations.

(Addresses Management and Performance Challenge #8)

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 at the Department of Energy's (DOE) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. Since the DOE is a self-regulating entity, the DNFSB constitutes the only independent technical oversight of operations at 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 Nuclear Regulatory Commission was authorized in 2014, and subsequent years, to exercise the same authorities with respect to the Defense Nuclear Facilities Safety Board, as determined by the Inspector General of the Nuclear Regulatory Commission, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the Nuclear Regulatory Commission.

DNFSB MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in FY 2021*

(as identified by the Inspector General)

Challenge 1: *Management of a Healthy and Sustainable Organizational Culture and Climate.*

Challenge 2: *Management of Security Over Internal Infrastructure (Personnel, Physical, and Cyber Security).*

Challenge 3: *Management of Administrative Functions.*

Challenge 4: *Management of Technical Programs.*

Challenge 5: *Management of the DNFSB's COVID-19 Pandemic Response.*

* *For more information on the challenges, see DNFSB-21-A-01, "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB" https://www.nrc.gov/docs/ML2029/ML20290A389.pdf*

DNFSB AUDITS

Audit Summaries

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

OIG Strategic Goal: Corporate Management

The OIG contracted with SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2020. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with the Council of Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. The FISMA of 2014 outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by the agency's OIG. In addition, the FISMA includes provisions, such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems.

All agencies must implement the requirements of the FISMA and report annually to the Office of Management and Budget and Congress on the effectiveness of their security programs.

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

Evaluation Results:

SBG found that the DNFSB's information security practices and programs were generally effective for the period October 1, 2019, through September 30, 2020. However, the evaluation identified areas that need improvement.

(Addresses Management and Performance Challenge #2)

Audit of the DNFSB's Financial Statements for Fiscal Year 2020

OIG Strategic Goal: Corporate Management

The Accountability for Tax Dollars Act of 2002 (ATDA) requires the Inspector General (IG) or an independent external auditor, as determined by the IG, to annually audit the DNFSB's financial statements in accordance with applicable standards. In compliance with this requirement, the Office of the Inspector General (OIG) retained CliftonLarsonAllen (CLA) to conduct this annual audit. CLA examined the DNFSB's Fiscal Year (FY) 2020 Agency Financial Report, which includes financial statements for FY 2020.

CLA's audit report contains the following subparts:

- Opinion on Financial Statements;
- Opinion on Internal Control over Financial Reporting; and,
- Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements.

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

Audit Results:
In CLA's opinion, the DNFSB's financial statements present fairly, in all material respects, the DNFSB's financial position as of September 30, 2020 and 2019, respectively, and its net cost of operations, changes in net position, and budgetary resources in accordance with U.S. generally accepted accounting principles. In addition, in CLA's opinion, although certain internal controls could be improved, the DNFSB maintained, in all material respects, effective internal control over financial reporting as of September 30, 2020, based on criteria established under the Federal Manager's Financial Integrity Act of 1982.

(Addresses Management and Performance Challenge #3)

Audit of the DNFSB's Compliance with Executive Order 13950, Combating Race and Sex Stereotyping

OIG Strategic Goal: Corporate Management
On September 22, 2020, the President issued Executive Order 13950, Combating Race and Sex Stereotyping (the Order). In accordance with section 6(c)(ii) of the Order, the DNFSB Acting Chairman requested that the OIG review and assess the DNFSB's compliance with the Order in the form of a report submitted to the U.S. OMB by the end of calendar year 2020, and not less than annually thereafter.

The audit objective was to review and assess agency compliance with the requirements of the Order.

Audit Results:
The OIG found that the DNFSB was in the process of becoming fully compliant with the Order. Of the nine requirements reviewed, seven were complete, one was in progress, and one was not applicable. The Executive Order was rescinded on January 25, 2021.

(Addresses Management and Performance Challenge #3)

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

OIG Strategic Goal: Corporate Management, Safety, and Security

The Reports Consolidation Act of 2000 (Public Law 106-531) requires us to annually update our assessment of the DNFSB. The IG provides what he considers to be the most serious management and performance challenges facing the DNFSB in FY 2021. Congress left the determination and threshold of what constitutes the most serious management and performance challenges to the discretion of the Inspectors General. The IG has defined serious management and performance challenges as mission critical areas or programs that have the potential for a perennial weakness or vulnerability that, without substantial management attention, would seriously impact agency operations or strategic goals.

Audit Results:

The OIG identified five management and performance challenges facing the DNFSB for FY 2021.

(Addresses Management and Performance Challenges #1-5)

Audits in Progress

No Audits in Progress to Report for this Period

DNFSB INVESTIGATIONS

Investigative Case Summaries

Concerns Regarding the DNFSB's Small Business Administration Contract Award

OIG Strategic Goal: Corporate Management

Allegation:
The OIG completed an investigation based on concerns from the Board regarding the DNFSB's award of a U.S. Small Business Administration (SBA) 8(a) set-aside contract. Board Members requested that the OIG evaluate the circumstances surrounding the DNFSB's award of a human resources contract, and whether the procurement process was handled consistent with the SBA's processes and Federal Acquisition Regulation requirements.

Investigative Results:
We found the DNFSB properly awarded the SBA 8(a) set-aside human resources contract, and did not find any contract irregularities or misconduct by the DNFSB employees involved. We verified that the SBA approved the DNFSB's request to negotiate the terms of a new contract with the SBA 8(a) company, and reviewed documents that confirmed the DNFSB handled the procurement process consistent with SBA processes and Federal Acquisition Regulation requirements.

(Addresses Management and Performance Challenge #3)

DNFSB IT Contractor Performing Work without a Valid Contract

OIG Strategic Goal: Corporate Management

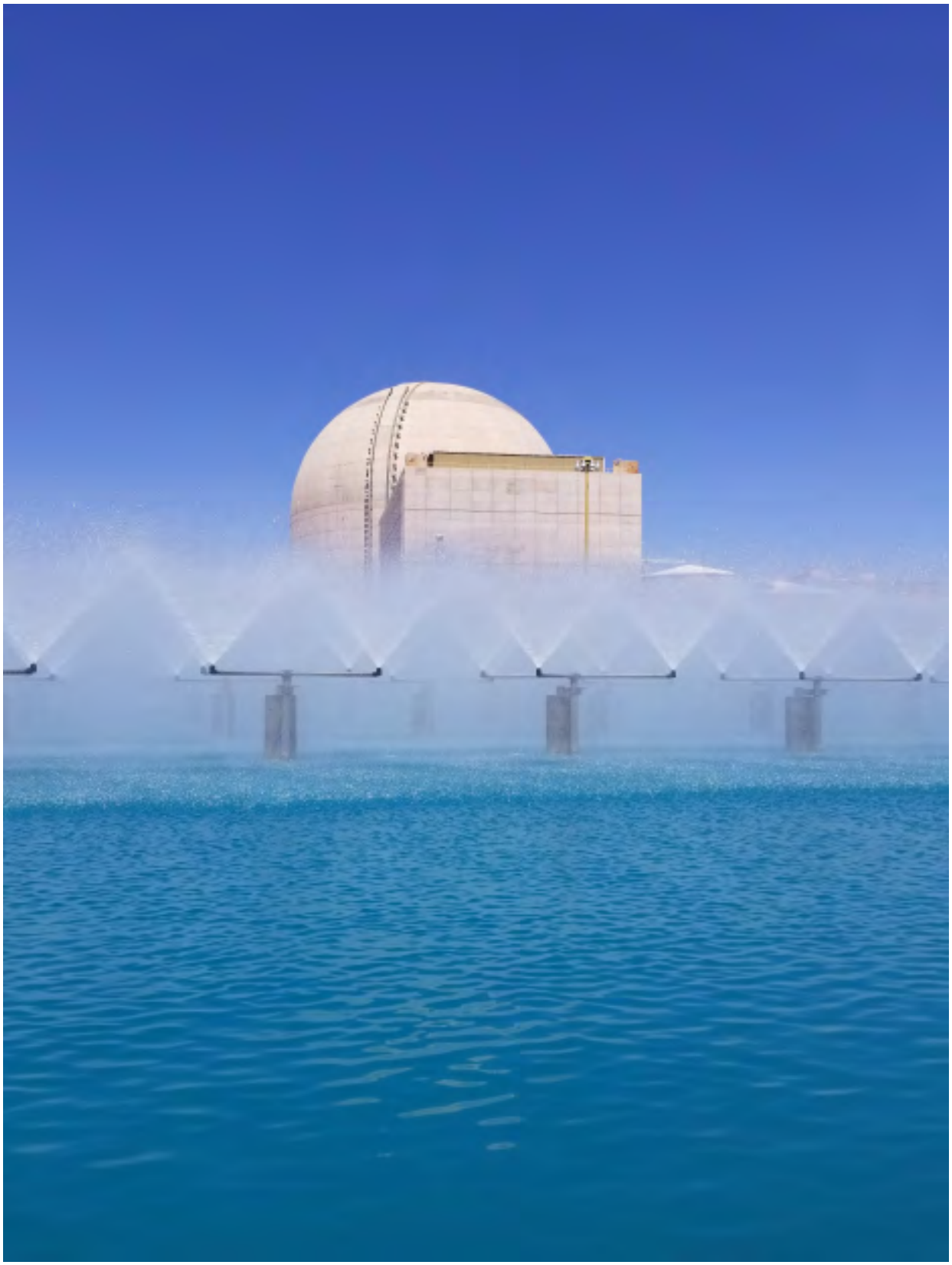
Allegation:
The OIG completed an investigation into an allegation that a DNFSB contractor performed information technology work for the DNFSB without a valid contract, and without receiving payment for those services, which may have caused the DNFSB to violate the Antideficiency Act.

Investigative Results:
We did not substantiate the allegation, having determined the contractor did not provide the DNFSB with any free IT services once its contracts had expired, and thus, there was no Antideficiency Act violation. We did find, however, that the DNFSB lacked policies or standard operating procedures for acquiring and tracking contracts. As a result, personnel roles and responsibilities were not clearly defined, which contributed to contract expiration escaping the notice of associated DNFSB employees, and uncertainty about whether the DNFSB was receiving and paying for services.

The Board's Response:

The Board told us it is committed to improving the management and administration of the DNFSB acquisitions portfolio, and has developed a corrective action plan (CAP) toward achieving that goal. The agency has already completed several of the CAP's actions, such as verifying all DNFSB Contracting Officer Representative (COR) certifications, and identifying and providing training to the CORs. Ongoing CAP actions include the development of agencywide acquisitions processes and procedures, documentation of all current processes as a baseline, initiation of an interagency procurement workgroup, and an extensive review of older contract files. These activities will be ongoing throughout FY 21 and FY 22, and are being reported and tracked through the DNFSB's Executive Committee on Internal Controls.

(Addresses Management and Performance Challenge #3)



A spray pond at the Palo Verde Generating Station in the middle of the Arizona desert allows the plant to efficiently disperse heat from water used to cool some plant components.

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

October 1, 2020 – March 31, 2021

Allegations Received from NRC OIG Hotline: 36

Investigative Statistics

Source of Allegations

NRC Employee	23
NRC Management	16
Intervenor	1
General Public	25
Other Government Agency	3
Anonymous	11
Contractor	2
Regulated Industry (Licensee/Utility)	3
OIG Self-Initiated	3
Total:	**87**

Disposition of Allegations

Closed After Reviewed	29
Correlated to Existing Investigation	3
Initiated OIG Investigation	10
Referred to OIG Audit	3
Referred to Another Agency	4
Referred to NRC Management	29
In Review for Disposition	9
Total	**87**

Status of Investigations

Federal	
DOJ Referrals	0
DOJ Declinations	0
DOJ Accepted	1
Criminal Information/Indictments	0
Criminal Convictions	0
Criminal Penalty Fines	0
Civil Recovery	0
Other Recovery	0
State and Local	
State and Local Referrals	1
State Accepted	1
Criminal Information/Indictments	1
Criminal Convictions	0
Criminal Penalty Fines	0
Civil Recovery	0
NRC Administrative Actions	
Counseling and Letter of Reprimand	2
Terminations and Resignations	0
Suspensions and Demotions	1
Other (e.g., PFCRA)	3*

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued†	Cases in Progress
Employee Misconduct	7	1	5	0	3
Event Inquiry	1	0	0	0	1
External Fraud	1	0	1	0	0
Internal Fraud	0	1	0	0	1
Management Misconduct	12	4	7	5	9
Miscellaneous	0	1	0	0	1
Proactive Initiatives	1	0	0	0	1
Technical Allegations	6	4	3	0	7
Theft	1	1	1	1	1
Total	**29**	**12**	**17**	**6**	**24**

**Review of Agency Process.*

†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
3/29/2021	Audit of the NRC's Nuclear Power Reactor Inspection Issue Screening	OIG-21-A-07
03/23/2021	The Defense Contract Audit Agency (DCAA) Audit Report Number 3311-2019W10100001	OIG-21-A-06
03/19/2021	Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2020	OIG-21-A-05
03/09/2021	Audit of the NRC's Material Control and Accounting Inspection Program for Special Nuclear Material	OIG-21-A-04
12/21/2020	Audit of the NRC's Compliance with Executive Order 13950, Combating Race and Sex Stereotyping	OIG-21-A-03
11/16/2020	Results of the Audit of the NRC's Financial Statements for Fiscal Year 2020	OIG-21-A-02
10/16/2020	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC in Fiscal Year 2021	OIG-21-A-01

NRC Contract Audit Reports

OIG Issue Date	Contractor/Title/Contract No.	Questioned Costs	Unsupported Costs
03/23/2021	**Southwest Research Institute** Independent Audit Report on Southwest Research Institute's Proposed Amounts on Select Unsettled Flexibility Priced Contracts for Fiscal Year 2019 NRCHQ12C020089 NRCHQ5014E0001 31310018D0001 31310018D0002	$0	$0

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	$3,571,892	0
B. Which were issued during the reporting period	0	0	0
Subtotal (A + B)	4	$3,571,892	0
C. For which a management decision was made during the reporting period:	0	0	0
(i) Dollar value of disallowed costs	0	0	0
(ii) Dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	4	$3,571,892	0

* *The OIG questions costs due to 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.*

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

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
C. For which a management decision was made during the reporting period:	0	0	0
(i) Dollar value of disallowed costs			
(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			

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

Table III

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

No Data to Report

SUMMARY OF OIG ACCOMPLISHMENTS AT THE DNFSB

October 1, 2020 – March 31, 2021

Source of Allegations

Investigative Statistics

DNFSB Employee	0
DNFSB Management	0
General Public	0
Anonymous	0
Contractor	0
Intervenor	0
Regulated Industry (Licensee/Utility)	0
OIG Self-Initiated	2
Other Government Agency	0
Total	**2**
Allegations Received from NRC OIG Hotline	0

Disposition of Allegations

Closed Administratively	0
Referred for OIG Investigation	2
Referred to OIG Audit	0
Referred to Another Agency	0
Referred to NRC Management	0
Pending Review Action	0
Processing	0
Correlated to Existing Case	0
Total	**2**

Status of Investigations

Federal	
DOJ Referrals	0
DOJ Declinations	0
DOJ Pending	0
Criminal Information/Indictments	0
Criminal Convictions	0
Civil Penalty Fines	0
Civil Recovery	0
Other Recovery	0
State and Local	0
State and Local Referrals	0
Criminal Information/Indictments	0
Criminal Convictions	0
Civil Penalty Fines	0
Civil Recovery	0
DNFSB Administrative Actions	
Counseling and Letter of Reprimand	0
Terminations and Resignations	0
Suspensions and Demotions	0
Other (e.g., PFCRA)	1

Summary of Investigations

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

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

DNFSB Audits Completed

Date	Title	Audit Number
03/25/2021	Independent Evaluation of the DNFSB's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020	DNFSB-21-A-04
12/21/2020	Results of the Audit of the DNFSB's Financial Statements for Fiscal Year 2020	DNFSB-21-A-03
12/18/2020	Audit of the DNFSB's Compliance with Executive Order 13950, Combating Race and Sex Stereotyping	DNFSB-21-A-02
10/16/2020	Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the DNFSB in Fiscal Year 2021	DNFSB-21-A-01

DNFSB Audit Resolution Activities

Table I

OIG Reports Containing Questioned Costs*

Reports	Number of Reports	Questioned Costs ($)	Unsupported Costs ($)
A. For which no management decision had been made by the commencement of the reporting period	0	0	0
B. Which were issued during the reporting period ***Subtotal (A + B)***	0	0	0
C. For which a management decision was made during the reporting period: (i) Dollar value of disallowed costs (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 due to 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
C. For which a management decision was made during the reporting period:	0	0	0
(i) Dollar value of disallowed costs			
(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.*

UNIMPLEMENTED AUDIT RECOMMENDATIONS

NRC
Audit of the NRC's Safeguards Information Local Area Network and Electronic Safe (OIG-13-A-16) **2 of 7 recommendations open since April 1, 2013**
Recommendation 3: Evaluate and update the current folder structure to meet user needs. **Recommendation 7:** Develop a structured access process that is consistent with the SGI need-to-know requirement and least privilege principle. This should include (1) Establishing folder owners within SLES and providing the owners the authority to approve the need-to-know authorization (as opposed to branch chiefs); (2) Conducting periodic reviews of user access to folders; and, (3) Developing a standard process to grant user access.
Audit of the NRC's Budget Execution Process (OIG-13-A-18) **1 of 8 recommendations open since May 7, 2013**
Recommendation 3: Enforce the use of correct budget object codes.
Audit of the NRC's Oversight of Spent Fuel Pools (OIG-15-A-06) **1 of 4 recommendations open since February 10, 2015**
Recommendation 1: Provide a generic regulatory solution for spent fuel pool criticality analysis by developing and issuing detailed licensee guidance along with NRC internal procedures.
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: Complete and fully implement current initiatives: (1) Finalize and provide records management training for authorized classifiers; (2) Complete the current inventories of classified information in safes and secure storage areas; (3) Develop declassification training to prepare and authorize declassifiers; (4) Develop an updated declassification guide; (5) Identify classified records requiring transfer to the National Archives and Records Administration and complete the transfers; and, (6) Complete the Office Instruction for performing mandatory declassification reviews.

Audit of the NRC's Foreign Assignee Program **(OIG 17-A-07)** **2 of 3 recommendations open since December 19, 2016**
Recommendation 2: Develop a secure, cost-efficient method to provide foreign assignees an email account which allows for NRC detection and mitigation of inadvertent transmission of sensitive information, and seek Commission approval to implement it. **Recommendation 3:** When an NRC approved email account is available, develop specific Computer Security Rules of Behavior for foreign assignees using the approved email.
Audit of the NRC's PMDA/DRMA Functions to Identify Program Efficiencies **(OIG-17-A-18)** **1 of 1 recommendation open since July 3, 2017**
Recommendation 1: Complete implementation of all Mission Support Task Force recommendations that may assist in optimizing the use of resources and result in improving standardization and centralization throughout the agency.
Audit of the NRC's Consultation practices with Federally Recognized Native American Tribal Governments **(OIG-18-A-10)** **1 of 5 recommendations open since April 4, 2018**
Recommendation 2: Update NRC office procedures to include more specific direction on how to coordinate with the FSTB and how to work with Tribes.
Audit of the NRC's Cyber Security Inspections at Nuclear Power Plants (OIG-19-A-13) **1 of 2 recommendations open since December 1, 2019**
Recommendation 2: Use the results of operating experience and discussions with industry to develop and implement suitable cyber security performance measure(s) (e.g., testing, analysis of logs, etc.) by which licensees can demonstrate sustained program effectiveness.
Evaluation of the NRC's Oversight of the Voice over Internet Protocol Contract and Implementation **(OIG-19-A-17)** **2 of 6 recommendations open since October 3, 2019**
Recommendation 5: Update the relevant management directives to include a) current telecommunications infrastructure and current organizational responsibilities, and b) a requirement to comply with MD 10.162 "Disability Programs and Reasonable Accommodation," when deploying any IT projects. **Recommendation 6:** Identify and implement a solution to address the issue pertaining to diverting an assigned phone line.

Audit of the NRC's Oversight of Supplemental Inspection Corrective Actions (OIG-19-A-19)
2 of 2 recommendations open since October 10, 2019

Recommendation 1: Update NRC inspection guidance to support documentation of significant planned corrective actions associated with 95001 and 95002 supplemental inspections.
Recommendation 2: Implement an efficient means for inspectors to readily identify and retrieve information about completed and planned corrective actions associated with 95001 and 95002 supplemental inspections.

Audit of the NRC's Process for Placing Official Agency Records in ADAMS (OIG-19-A-20)
3 of 5 recommendations open since October 31, 2019

Recommendation 3: Conduct an initial review of ADAMS to identify and remove personal papers, and implement a policy to conduct such reviews on a periodic basis.
Recommendation 4: Strengthen internal controls to prevent individuals from entering personal papers in ADAMS.
Recommendation 5: Strengthen internal controls to ensure use of the Capstone tool and compliance with NARA requirements.

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)
6 of 7 recommendations open since July 9, 2020

Recommendation 1: Fully define the NRC ISA across the enterprise and business processes and system levels.
Recommendation 2: Use the fully defined ISA to:

(a) Assess enterprise, business process, and information system level risks;
(b) Update the list of high value assets by considering risks from the supporting business functions and mission impacts;
(c) Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions;
(d) Conduct an organization-wide security and privacy risk assessment;
(e) Conduct a supply chain risk assessment; and,
(f) 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: Updates 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) **6 of 13 recommendations open since July 8, 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 10:** Verify or update training or guidance that reminds personnel about their use of locked screen savers for computers that are not in their immediate control. The training/guidance should contain a reference to the consequences of violating the safeguarding procedures. **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. **Recommendation 12:** Verify or update training for the NRC cleaning staff so that they are not using methods to keep corridor doors open during cleaning operations. Perform spot checks to ensure that they are complying with all security procedures. **Recommendation 13:** Provide the OIG with a strategy to ensure the risk sensitive information is not left unattended in NRC office desks or uncontrolled spaces.
Audit of the NRC's Nuclear Power Plant Surveillance Test Inspection Program (OIG-20-A-11) **2 of 2 recommendations open since July 16, 2020**
Recommendation 1: Implement policies and procedures to periodically review the completeness and accuracy of data generated from the Replacement Reactor Program System. **Recommendation 2:** Periodically test data generated from the Replacement Reactor Program System for completeness and accuracy.
Audit of the NRC's Emergency Preparedness Program (OIG-20-A-12) **2 of 3 recommendations open since July 23, 2020**
Recommendation 1: Revise the existing guidance in SL-100 to capture best practices and serve as a knowledge management tool for the Regional State Liaison Officer role. **Recommendation 2:** Coordinate with government partners at the federal, state, and local levels to identify resources, such as recorded training videos or presentations, to supplement Regional State Liaison Officers' outreach.
Audit of the NRC's Drug-Free Workplace Program Implementation (OIG-20-A-13) **2 of 4 recommendations open since August 7, 2020**
Recommendation 1: Revise the NRC Drug-Free Workplace Plan to reflect the most up-to-date U.S. Department of Health and Human Services requirements. **Recommendation 2:** Revise the NRC Drug Testing Manual to reflect the most up-to-date U.S. Department of Health and Human Services Requirements.

Audit of the NRC's Regulatory Oversight of Radiation Safety Officers (OIG-20-A-15)
1 of 1 recommendation open since September 9, 2020

Recommendation 1: Evaluate and document the benefits of strengthening internal controls to ensure temporary RSOs appointments are established and terminated in accordance with NRC policy.

Audit of NRC's Employee Reentry Plans (OIG-20-A-16)
1 of 1 recommendation open since September 21, 2020

Recommendation 1: Capture and document lessons learned for future use during public health emergencies or other events that could cause prolonged disruption of agency operations.

Audit of NRC's Property Management Program (OIG-20-A-17)
7 of 7 recommendations open since September 21, 2020

Recommendation 1: Modify the definition of accountable property to align with the agency's procedures for accounting for property under the property management program. This encompasses defining and addressing the accountability of items not tracked in the Space and Property Management System (SPMS) including pilferable property.
Recommendation 2: Include the receipt, management, and proper disposal of IT assets planned and currently tracked in Remedy within the property management program. This may include, but is not limited to actions such as:

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

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

(a) Decentralized property receipt and tagging functions; and,
(b) Providing property staff with acquisition information such as the cost and shipping information necessary to perform their property-related duties through automated notification.

Recommendation 4: Limit the regional and the Technical Training Center (TTC) property item assignments to regional property custodians.
Recommendation 5: Consolidate the notification of stolen NRC property to one NRC form.
Recommendation 6: Digitize the property process to facilitate reconciliation and property management workflow.
Recommendation 7: Self-reassess the risk to the agency for the policy changes of the tracking

threshold increase and removal of cell phones, laptops, and tablets from the sensitive items list, for loss or theft of property items.

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

Recommendation 1: Perform a more robust review of the future lease payments schedule to ensure it reflects all changes and updates to occupancy agreements. This review should include a documented review by the group responsible for negotiating and signing occupancy agreements, since they would be most familiar with all current occupancy agreements.
Recommendation 2: Perform a more robust review of leasehold improvements and require accurate communication from accountable property managers to ensure that, as occupancy agreements change, projects begin, or projects are completed, any impact to leasehold improvements in the financial statements is recorded timely and accurately. This review should also include timely and completely documenting the status of leasehold improvements in process.
Recommendation 3: Strengthen its internal control to ensure funds are de-obligated timely, including identifying amounts to be de-obligated and posting the de-obligation to the accounting system.
Recommendation 4: Maintain adequate documentation, including correspondence, for the reasons why an aged, unliquidated obligation should not be de-obligated.
Recommendation 5: Review the process for generating the unliquidated obligation subsidiary details report (management report); ensure that amounts that are not ULOs, are not included in the management report; and reconcile the management report to the general ledger.

Audit of 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)
13 of 13 recommendations open since March 22, 2021

Recommendation 1: Fully define the NRC's ISA across the enterprise, business processes, and system levels.
Recommendation 2: Use the fully defined ISA to:

(a) Assess enterprise, business process, and information system level risks;
(b) Update the list of high value assets, if necessary, based on reviewing the ISA to identify risks from the supporting business functions and mission impacts;
(c) If necessary, update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions;
(d) 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;
(e) 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,

(f) 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 3: Continue to monitor the remediation of critical and high vulnerabilities and identify a means to assign and track progress of timely remediation of vulnerabilities.

Recommendation 4: Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems, (findings noted in bullets 1, 3, and 4 above) by continuing efforts to implement these capabilities using the Splunk QAudit, Sailpoint, and Cyberark 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 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 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 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)
4 of 4 recommendations open since March 29, 2021

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

Recommendation 2: Periodically review RPS data, and test RPS controls for accuracy and completeness.

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

Recommendation 4: Conduct periodic training regarding RPS data input.

DNFSB

Audit of the DNFSB's Telework Program
(DNFSB-17-A-06)
3 of 3 recommendations open since July 13, 2017

Recommendation 1: Revise the telework directive and operating procedure to: (a) clarify the process for telework denials; (b) list information technology security training as part of the requirements; and, (c) incorporate a requirement to update agency telework training to reflect changes made in policy.
Recommendation 2: Finish updating all telework agreements in accordance with the telework agreement template.
Recommendation 3: Develop and implement a checklist for telework recordkeeping to ensure employee telework files are consistent.

Audit of the DNFSB's Issue and Commitment Tracking System (IACTS) and Its Related Processes
(DNFSB-19-A-02)
1 of 8 recommendations open since November 1, 2018

Recommendation 5: Create and implement a policy to consistently track RFBAs through a tracking mechanism, or through the IACTS.

Audit of the DNFSB's Compliance under the Digital Accountability and Transparency (DATA) Act of 2014
(DNFSB-20-A-02)
1 of 2 recommendations open since November 12, 2019

Recommendation 1: The DNFSB should work with its FSSP to correct the PIIDs for new obligations in its accounting system, and correct the mapping of certain data elements to ensure that data elements are in accordance with the data standards established by the OMB and the Treasury.

Audit of the DNFSB's Human Resources Program
(DNFSB-20-A-04)
6 of 6 recommendations open since March 24, 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 its 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)
11 of 11 recommendations open since April 30, 2020

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 recommendations one (1) and two (2) above:

(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. Export metrics and vulnerability reports (Cybersecurity Team) and send 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 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: 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 6: Implement procedures and define roles for reviewing configuration change activities to DNFSB information system production environments, by those with privileged access to verify that activity was approved by the system CCB and executed appropriately.

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 Potential Compromise of Systems (Social Engineering) (DNFSB-20-A-07)
1 of 3 recommendations open since July 8, 2020

Recommendation 2: Within the next year, perform follow-on checks to see if passwords are being protected.

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 recommendations in bullets one (1) and two (2) above:

(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 in 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 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 FY 2020 Financial Statement
(DNFSB-21-A-03)
2 of 2 recommendations open since December 16, 2020

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

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

ABBREVIATIONS AND ACRONYMS

ATDA	Accountability for Tax Dollars Act of 2002
CCIG	Council of Counsels to Inspectors General
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CLA	CliftonLarsonAllen
COVID-19	Coronavirus Disease 2019
DCAA	Defense Contract Audit Agency
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
ILTAB	Intelligence Liaison and Threat Assessment Branch
ILTAT	Intelligence Liaison and Threat Assessment Team
IPERA	Improper Payments Elimination and Recovery Act
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
MC&A	Material Control and Accounting
MD	Management Directive
NMSS	Office of Nuclear Material Safety and Safeguards
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SBG	SBG Technology Solutions, Inc.
SNM	Special Nuclear Material
SRI	Senior Resident Inspector
SwRI	Southwest Research Institute
URI	Unresolved Item

REPORTING REQUIREMENTS

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

Citation	Reporting Requirements	Page(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
Section 5(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 Department of the Treasury Office of the Inspector General (Treasury OIG) conducted a required, modified, external peer review to assess the extent to which the NRC OIG met the seven Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation* (Blue Book) standards: Quality Control, Planning, Data Collections and Analysis, Evidence, Records Maintenance, Reporting, and Follow-up. The Treasury OIG conducted the Blue Book peer review from July 16, 2020 through August 27, 2020. The review team determined that the NRC OIG's policies and procedures generally met the seven Blue Book standards addressed in the external peer review. The review team issued a Letter of Comment, dated October 28, 2020, that sets forth the peer review results, and includes a recommendation to strengthen the NRC OIG's policies and procedures.

The NRC OIG audit program was peer reviewed by the OIG for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau. The review was conducted in accordance with Government Auditing Standards and CIGIE requirements. In a report dated September 4, 2018, 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.

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 OIG STRATEGIC GOALS FOR THE NRC

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

THE OIG STRATEGIC GOALS FOR THE DNFSB

1. Strengthen the DNFSB's efforts to oversee the safe operation of DOE defense nuclear facilities.
2. Strengthen the DNFSB's security efforts in response to an evolving threat environment.
3. Increase the economy, efficiency, and effectiveness with which the DNFSB manages and exercises stewardship over its resources.

The NRC OIG Hotline

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

What should be reported:

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

Ways To Contact the OIG

Call:
OIG Hotline
1-800-233-3497
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.nrc.gov
Click on Inspector General
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

NUREG-1415, Vol. 35, No. 1 March 2021

@NRCgov