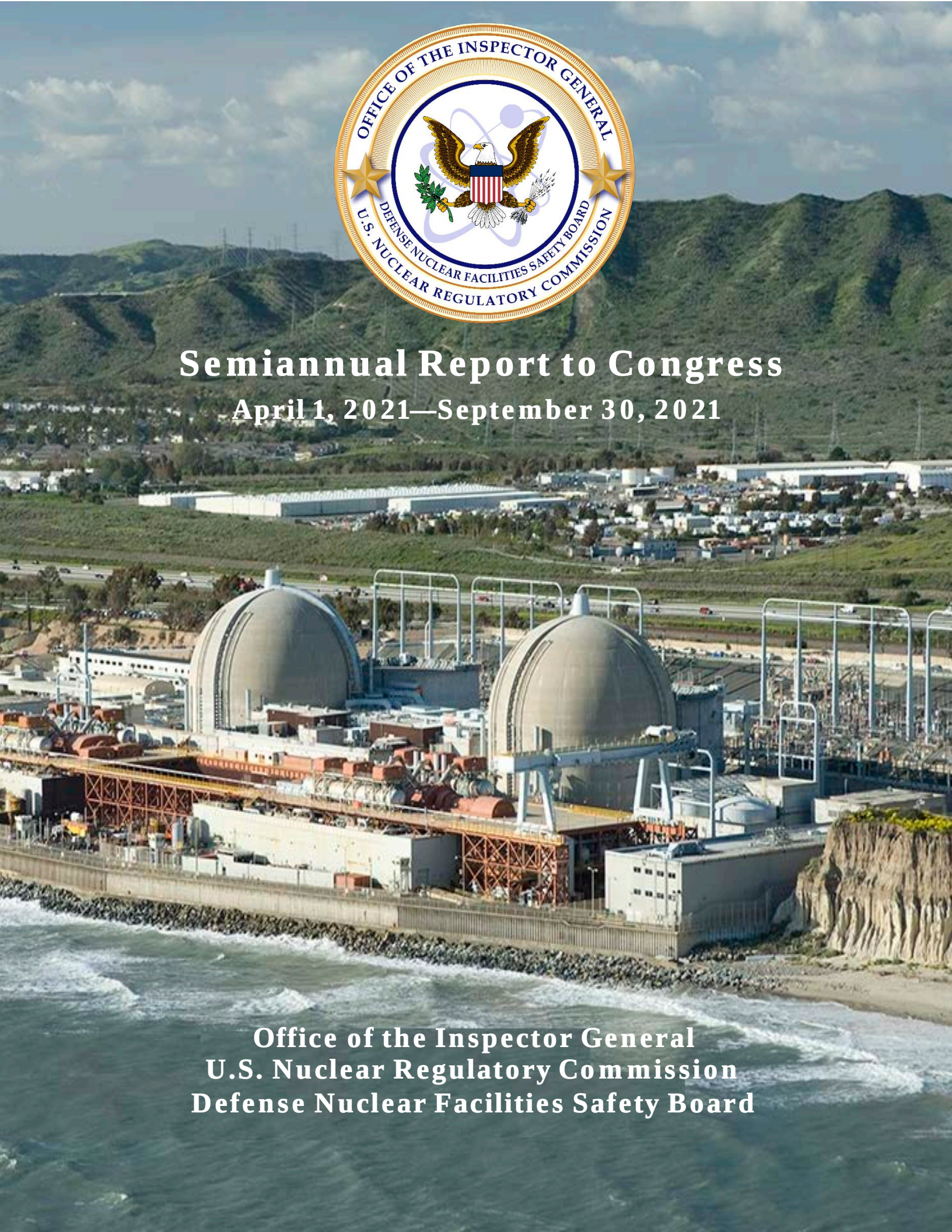


Semiannual Report to Congress

April 1, 2021—September 30, 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:

San Onofre Nuclear Generating Station (SONGS)

A MESSAGE FROM THE INSPECTOR GENERAL

On behalf of the Office of the Inspector General, U.S. Nuclear Regulatory Commission and Defense Nuclear Facilities Safety Board, it is my pleasure to present this Semiannual Report to Congress, covering the period from April 1, 2021 to September 30, 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 twelve audit and evaluation reports, and recommended several ways to improve NRC and DNFSB safety, security, and corporate management programs. We also opened nine investigative cases and completed nine, three of which were referred to the Department of Justice, and seven of which were referred to NRC management for action.

Our reports are intended to strengthen the NRC's and the DNFSB's oversight of their myriad endeavors and reflect the legislative mandate of the Inspector General Act, which is to identify and prevent fraud, waste, and abuse. Summaries of the reports herein include reviews of the NRC's prohibited security ownership process; enterprise risk management process; nuclear materials and waste oversight process; use of request for additional information process; oversight of decommissioning trust funds; grant proposals and awards oversight; DNFSB compliance with Improper Payment Laws; and, the DNFSB safety culture and climate survey. Further, this report includes summaries of cases involving interference with inspection findings, inaccurate information in an inspection test report, theft of the NRC's laptop computers, retaliation for a differing professional opinion, mismanagement of a desk audit, and claim of a hostile work environment.

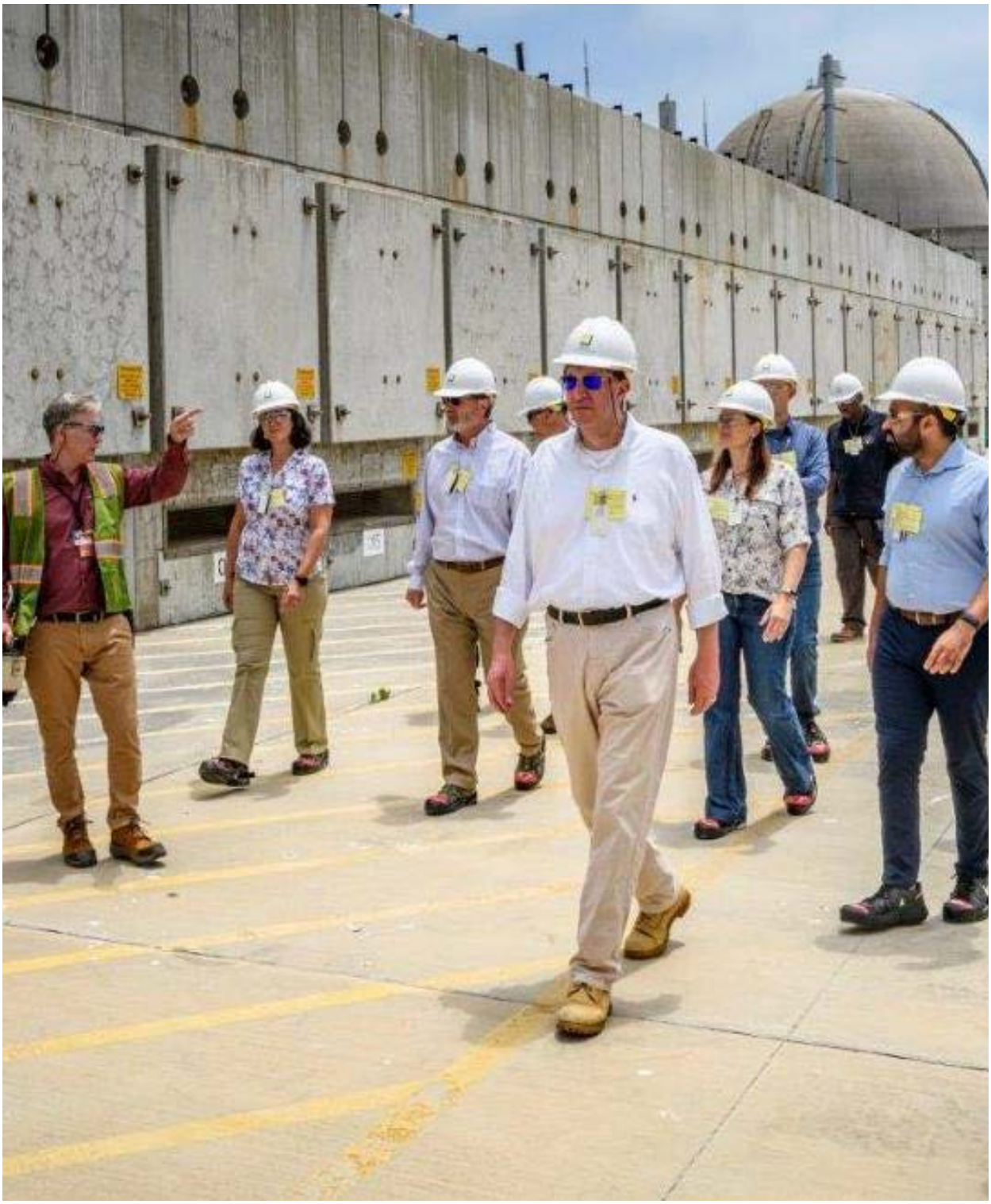
Our team dedicates their efforts to promoting the integrity, efficiency, and effectiveness of NRC and DNFSB programs and operations, and I greatly appreciate their commitment to that mission. Our success would not be possible without the collaborative efforts between my staff and those of the NRC and 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 Office of the Inspector General's New Seal

CONTENTS



The Inspector General and staff tour SONGS.

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

- Nuclear Regulatory Commission (NRC) employees at a certain professional level are prohibited from owning stock in companies that might present conflicts 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 NRC Office of the General Counsel. 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 Office of the Inspector General (OIG) assessed whether the NRC has established and implemented an effective internal control system over the NRC security ownership process.

- The Office of Management and Budget (OMB) updated OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (OMB A-123), in 2016. The update includes Enterprise Risk Management (ERM) 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. The OIG assessed whether the NRC's ERM process is being implemented in accordance with OMB A-123.

- 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 current COVID-19 PHE, licensees may experience challenges in meeting certain regulatory requirements, and therefore 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. While providing relief from regulatory requirements, the NRC continues to assure that licensed facilities are operating safely during the COVID-19 PHE. The OIG assessed and evaluated the NRC's nuclear materials and waste oversight processes during the COVID-19 pandemic.

- The NRC requires power reactor licensees to establish decommissioning trust funds. The purpose of these trust funds is to ensure there will be sufficient funds to pay for decommissioning costs when reactors permanently cease operations. Pursuant to this requirement, the NRC independently analyzes decommissioning funding status reports to determine whether licensees have provided reasonable assurance that sufficient funding for radiological decommissioning of each reactor and site will remain available until license termination. The OIG evaluated the adequacy of the NRC's oversight of the sufficiency of licensees' decommissioning trust funds.

- As the COVID-19 public health emergency unfolded in early 2020, the NRC and licensees operating nuclear power plants responded to protect their employees and continue operations. The NRC and licensees implemented an array of COVID-19 precautionary measures and protocols to protect employees. The NRC used inherent flexibilities in the Reactor Oversight Process and hybrid inspection approaches to complete baseline inspection procedures while protecting the health and safety of NRC and licensee personnel. The OIG assessed the NRC's policies and procedures for conducting rector inspections during the COVID-19 public health emergency.

- The Omnibus Appropriations Act of 2009 (the Act) established the Integrated University Program between the NRC, the U.S. Department of Energy, and the National Nuclear Security

Administration. The Act authorized the appropriation of $45 million per year from fiscal year (FY) 2009 through FY 2019 with $15 million for each agency. Combined, the NRC grants program from FY 2008 through FY 2019 comprised 533 grants and totaled roughly $185 million. The OIG examined the NRC's policies and procedures for reviewing grant proposals and awards compliance with applicable federal regulations, and the adequacy of internal controls over the pre-award and award processes.

- The OIG and the Defense Contract Audit Agency (DCAA) have an interagency agreement whereby the DCAA provides contract audit services for the OIG. The DCAA is responsible for the audit methodologies used to reach the audit conclusions, monitoring their staff's qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management and follow-up on agency actions initiated due to this report. At the request of the OIG, the DCAA audited Advanced Systems Technology Management, Inc., and provided the OIG with an audit report. The DCAA audit report identified questioned costs to be addressed by NRC management.

- The NRC licenses and regulates the storage of spent fuel, both at commercial nuclear power plants and at separate storage facilities. The NRC conducts a safety review prior to granting a license or certificate for the storage of spent fuel. A request for additional information is the mechanism by which NRC staff collect the information needed in order to make a regulatory decision regarding whether a license or certificate should be granted, renewed, modified, or denied. The OIG assessed the efficiency and effectiveness of the NRC's use of requests for additional information during the spent fuel storage licensing process.

Defense Nuclear Facilities Safety Board

- Enacted in 2020, the Payment Integrity Information Act of 2019 (PIIA) requires federal agencies to periodically review all programs and activities the agencies administer, and identify all programs and activities that may be susceptible to significant improper payments. An improper payment is:

  > (a) any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements; and,
  >
  > (b) includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts.

  The OIG assessed the Defense Nuclear Facilities Safety Board's (DNFSB's) compliance with the PIIA.

- Beginning in the Fall of 2020, Willis Towers Watson partnered with the OIG to assess the DNFSB safety culture and climate as well as other aspects of employee experience such as engagement. This survey served as a follow-up to the 2015 DNFSB Culture and Climate Survey. Willis Towers Watson conducted the 2021 DNFSB Safety Culture and Climate Survey for approximately 95 employees in January of 2021. The survey was designed based on information gathered from leadership interviews and staff focus groups.

Investigations

Nuclear Regulatory Commission

- The OIG investigated concerns from NRC employees, interest groups, and the public that NRC management was not following established processes for the licensing and use of accident tolerant fuel (ATF) lead test assemblies (LTAs) in U.S. commercial power reactors. During our investigation, we observed that NRC regulations allow staff leeway to accept licensees' variations in approach to installing LTAs, including pursuing license amendment requests or changes per 10 Code of Federal Regulations (C.F.R) 50.59. This resulted in inconsistent oversight over the years. The NRC should consider reviewing this inconsistent approach in light of the 2019 Nuclear Energy Innovation and Modernization Act (NEIMA) and ATF's emerging prevalence. We also found that confusion about roles and responsibilities between the regions and headquarters led to an inaccurate quarterly inspection report that may have misled the industry and public by indicating that a Core Operating Limits Report had been reviewed for Clinton Power Station, but had not.

- The OIG investigated allegations that an NRC senior manager released predecisional information to a licensee regarding an NRC report that found nonlicensed operators willfully neglected to conduct required rounds to check equipment at a plant. We substantiated the allegation and validated that the agency had taken corrective action against the NRC senior manager for releasing predecisional information to the licensee. We found that NRC managers had varied opinions about what constitutes predecisional information, and when to transact the NRC's two enforcement processes. After we briefed the NRC Office of the Executive Director for Operations (OEDO) on our discoveries, the OEDO committed to developing agencywide training to assess and disposition violations of NRC requirements using the Traditional Enforcement Process and the Reactor Oversight Process.

- The OIG investigated an allegation of the theft of 63 NRC laptops, and found that a former NRC Information Technology (IT) contractor used his personal email account to communicate with a

buyer regarding the purchase of used and new laptops. We determined that one of the laptops sold to the buyer by the former NRC IT contractor was a confirmed stolen NRC laptop, which was advertised for sale on Facebook Marketplace.

- The OIG investigated but did not substantiate an allegation of retaliation. The alleger claimed that an NRC senior manager retaliated against him by influencing the interview panel not to select him to be a part of a Senior Executive Service Candidate Development Program, but we found that the process was fair and there was no evidence of influence.

- The OIG investigated but did not substantiate a claim that two NRC senior managers conspired to deny a promotion to an NRC employee following a desk audit that found the NRC employee's position duties should be at a higher level than they were. We investigated whether the two NRC senior managers conspired against the NRC employee, whether an NRC senior manager denied the NRC employee a promotion, and whether the agency denied the NRC employee and her supervisor the right to appeal the senior manager's decision.

- The OIG investigated allegations that an NRC senior manager created a hostile work environment that included disparate treatment of staff members. We brought this to the attention of the OEDO because we had previously referred complaints about this NRC senior manager to the agency and have continued to receive additional complaints. Some staff members told us the NRC senior manager had a hostile and intimidating management style and showed preferential treatment to members within the office based on their race. Additionally, most staff members feared retaliation. Although we did not find evidence or substantiate race-based claims of harassment or retaliation, all employees we interviewed told us they perceived a chilled work environment.

- The OIG investigated an allegation from a public stakeholder that NRC staff violated federal regulations and agency procedures with its handling of the public notice for the exigent license amendment request submitted by a licensee at a nuclear power plant. We substantiated these allegations that the NRC violated Management Directive 3.4 , Release of Information to Public, by not

adhering to the 5-day goal of releasing documents to the public in the Agencywide Document Access Management System, and 10 C.F.R § 50.91 by not affording a reasonable opportunity for the public to comment.

Defense Nuclear Facilities Safety Board

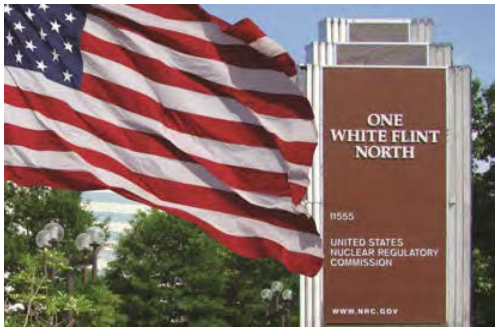
While the OIG did not close any DNFSB investigations during this reporting period, we did initiate two proactive efforts to identify fraud within DNFSB programs and operations and potential computer misuse and cybersecurity issues.

An aerial view of SONGS

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 evolving threat environment; and,

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

Dry Cask Storage at SONGS

OIG PROGRAMS AND ACTIVITIES

Audit Program

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

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

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

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

- **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 U.S. Department of Justice on OIG-related criminal and civil matters, and coordinating investigations and other OIG initiatives with federal, state, and local investigative agencies and other OIGs.

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

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

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

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

- Failure by the NRC to 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, 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 the 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 so as to avoid formal implementation of potentially flawed documents. The OIG does not concur or object to the agency 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. The OIG review is structured so as to identify vulnerabilities and offer additional or alternative choices. In addition, regulatory reviews often focus on ensuring that agency policy and procedures do not negatively impact OIG operations or independence.

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

From April 1, 2021 to September 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. Further, the OIG's regulatory reviews reflect its knowledge and awareness of underlying trends and overarching developments at the 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 Management Directives

MD 3.2, Privacy Act, which establishes the NRC's policy for ensuring that systems of records are established and maintained in accordance with the Privacy Act of 1974 and the NRC's implementing regulation at 10 C.F.R. Part 9, Subpart B. This revision reflected amendments to NRC regulations to comply with the Social Security Fraud Amendment Act of 2017. The OIG reviewed the draft revisions to ensure that they would have no negative impact on OIG access to information and that statutory and regulatory requirements would continue to be implemented effectively and efficiently and had no substantive comments.

MD 4.5, Contingency Plan for Periods of Lapsed Appropriations, which provides guidance and instructions for suspending nonexcepted agency activities following a lapse in appropriations. No substantive changes were made to the MD; it was certified as up-to-date. Although the OIG reviewed it, due to the lack of revision to the MD, it offered no substantive comments or edits.

MD 10.72, Awards and Recognition, which contains the policy for recognizing and rewarding NRC employees who contribute to meeting organizational goals or increasing the efficiency and effectiveness of the organization. The OIG offered several edits designed to safeguard the independence of the IG with respect to personnel matters, as established in the IG Act, and to ensure that the IG acts as head of the agency when proposing awards to OIG personnel.

MD 10.8, Clearances Before Separation or Reassignment, which establishes processes and procedures for ensuring orderly out-processing of NRC employees prior to reassignment between headquarters and regional

NRC offices or separation from the agency. The MD had last been updated in 2002. The OIG's review was focused on ensuring that the clearance process would not have a negative impact on the OIG's operations or mission. While no such concerns were identified, the OIG review raised other potential areas for change. Most notably, the OIG identified the potential for conflict between this MD and another directive also currently in the process of being revised. This comment was a direct result of the OIG's broad knowledge of agency operations.

MD 3.5, Attendance at NRC Staff-Sponsored Meetings, which ensures that members of the public are informed of and have access to agency decision making and activities by ensuring that NRC staff meetings with licensees and others are properly noticed and, where appropriate, open to the public. Access to meetings and information has been raised to the OIG as a concern by numerous members of the public and non-governmental organizations, and the OIG's review reflected its understanding of these concerns. Among its comments, the OIG suggested clarifications to the explanation of what meetings would and would not be open to the public, thus contributing to public understanding and comfort with policies regarding open meetings.

MD 8.10, NRC Assessment Program for a Medical Event or an Incident Occurring at a Medical Facility, which governs the NRC's policy for assessing and responding to medical events and incidents occurring at medical facilities involving NRC licensees and NRC licensed activities. The OIG reviewed the draft changes, which largely reflected a reorganization of the relevant offices, and had no comments.

MD 10.159, NRC Differing Professional Opinion Program, which authorizes the NRC's program for allowing eligible employees and contractors to formally raise differing views regarding established technical and policy matters and the process for considering such claims. This process has been the subject of concerns raised regarding its effectiveness as well as concerns regarding potential reprisal against employees who participate in the program. The OIG's review of this MD first considered areas in which the revisions to the program could impinge upon the independence of the OIG. The OIG offered edits to ensure that employees participating in the Differing Professional Opinion (DPO) process understand their right to bring both technical concerns and allegations of reprisal to the OIG or the Office of Special Counsel. The OIG's proposed edits also clarified the OIG's very limited role in tracking

the number and outcome of reprisal allegations, if any, arising from the DPO process. In addition, based on its extensive knowledge of the current DPO process, the OIG offered comments designed to enhance the efficiency and effectiveness of the DPO process by further safeguarding the technical objectivity of the evaluation of DPO claims.

MD 10.14, Employee Trial Period, which describes a description of trial periods for employees under initial appointments to the NRC sufficient to effectively assess the ability of an employee to perform adequately in his or her assigned position and whether the employee will be an asset to the federal government prior to the finalization of the appointment. As part of its review, the OIG offered edits ensuring that the IG has authority under this program over OIG employees, thus ensuring IG independence consistent with the IG Act.

DNFSB Directives

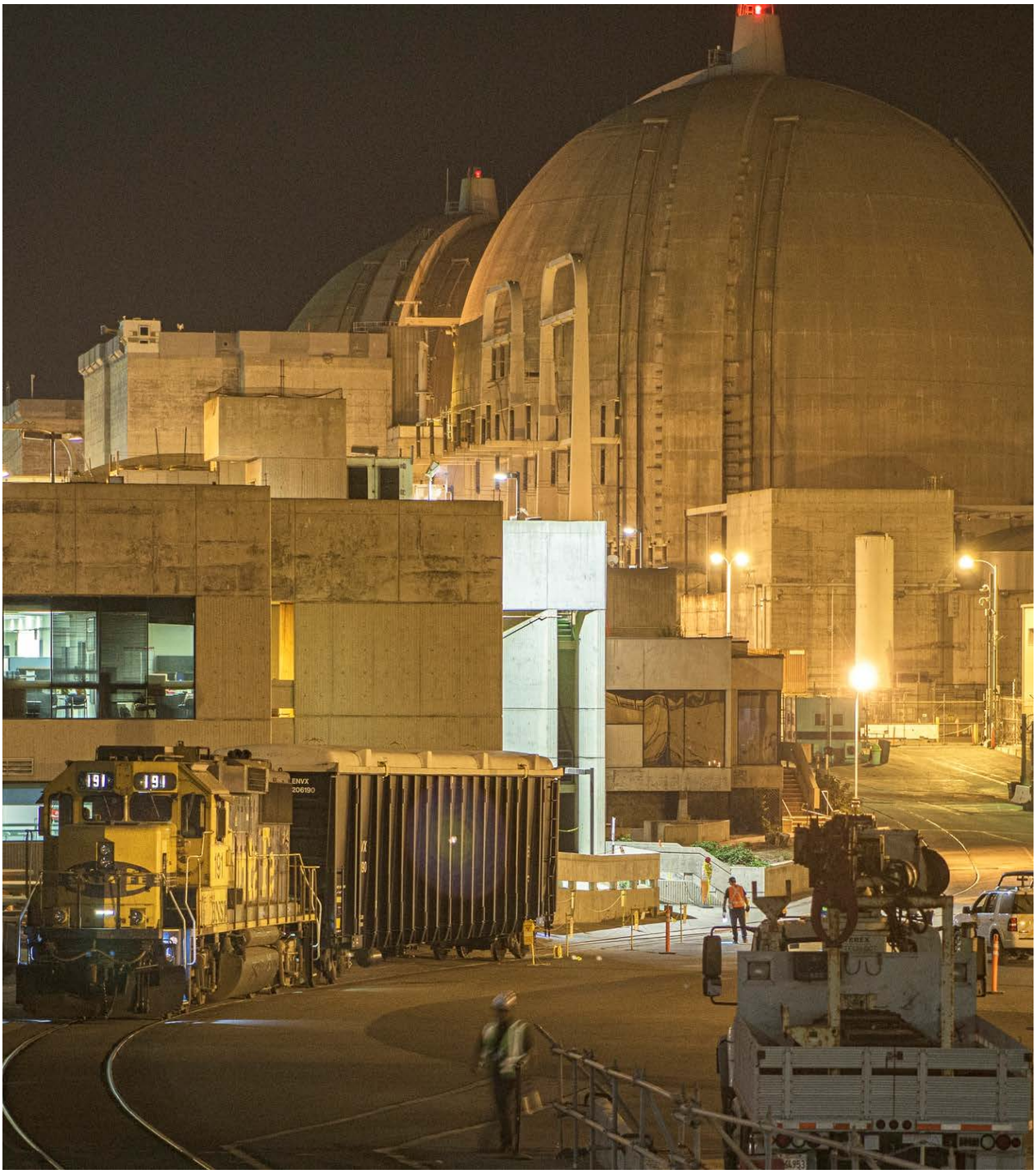
Directive D-125.1, Telework and Remote Work Program. This directive is a major revision of the prior DNFSB telework program and is being instituted as the agency reopens following extensive telework during the COVID-19 pandemic. The OIG's comments ensured that the policy remains in compliance with applicable governmentwide guidance, even as that guidance may be subject to change as the federal government moves away from large-scale telework due to the COVID-19 pandemic.

Other OIG Activities

Newly Appointed Chief of Staff

Eddie A. O'Connell, Chief of Staff

Edward (Eddie) A. O'Connell has been appointed the Chief of Staff for the NRC OIG. Prior to coming to the OIG, Mr. O'Connell served for almost 19 years as an Assistant United States Attorney for the District of Columbia (D.C.), where he prosecuted a wide variety of complex criminal matters in both U.S. District Court and D.C. Superior Court. Upon the completion of his Clerkship with the Honorable Rufus King III on D.C. Superior Court, Mr. O'Connell began his legal career as an Assistant State's Attorney for the City of Baltimore, Maryland. Mr. O'Connell earned his Bachelor of Arts degree in History and English from The Catholic University of America, and his Juris Doctor degree from Quinnipiac University School of Law.



Railcar at SONGS

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 Prohibited Securities Program

OIG Strategic Goal: Corporate Management

Employees at a certain professional level are prohibited from owning stock in companies that might present conflicts 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 NRC Office of the General Counsel. The NRC policies and procedures on this regulation are contained in MD 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 any prohibited 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 was to determine whether the NRC has established and implemented an effective internal control system over the NRC security ownership process.

Audit Results:

The OIG found that the NRC has not established and implemented an effective system of internal controls over the NRC's prohibited security ownership process.

(Addresses Management and Performance Challenge # 8)

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, Management's Responsibility for Enterprise Risk Management and Internal Control (OMB A-123) in 2016. The updated circular includes 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 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.

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 audit objective was to determine whether the NRC's ERM process is being implemented in accordance with OMB A-123.

Audit Results:

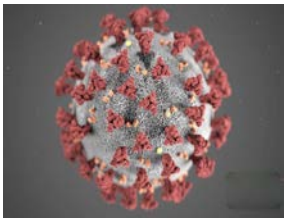
The OIG found that the NRC has implemented an ERM process with a governance framework. However, the effectiveness of the process can improve through better alignment with OMB Circular A-123 and enhanced quality assurance measures over the ERM process.

(Addresses Management and Performance Challenge # 6)

Audit of COVID-19's 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 PHE for the United States to aid the nation's healthcare community in responding to COVID-19. The NRC recognized that during the current 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 exemptions from regulatory requirements, amendments to license conditions or technical specifications, and enforcement discretion. Typical requests involve relief from routine actions, such as conducting audits and 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 requests do not significantly impact on safety or security. While providing relief from regulatory requirements, the NRC continues to ensure that licensed facilities are operating safely during the COVID-19 PHE.

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

Audit Results:

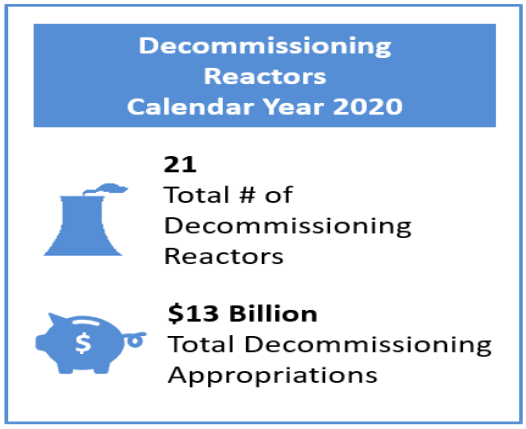
The OIG found that the NRC's nuclear materials and waste oversight processes during the COVID-19 PHE have generally been effective in helping the NRC accomplish its mission. However, opportunities exist for strengthening the process during prolonged work disruptions.

(Addresses Management and Performance Challenge # 3)

Audit of the NRC's Oversight of the Adequacy of Decommissioning Trust Funds

OIG Strategic Goal: Corporate Management

The NRC requires power reactor licensees to establish decommissioning trust funds. The purpose of these trust funds is to ensure that there will be sufficient funds to pay for decommissioning costs when reactors permanently cease operations. Licensees in the process of decommissioning their reactors must submit annual financial assurance status reports to the NRC. Pursuant to this requirement, the NRC independently analyzes decommissioning funding status reports to determine whether licensees have provided reasonable assurance that sufficient funding for radiological decommissioning of each reactor and site will remain available until license termination. As of December 2020, the average decommissioning trust fund was valued at approximately $619 million dollars.



The audit objective was to determine if the NRC's oversight of the sufficiency of licensees' decommissioning trust funds is adequate.

Audit Results:

The OIG found that the NRC could improve its oversight of licensees' sufficiency of decommissioning trust funds through more consistent adherence to agency guidance for reviewing licensee decommissioning funding status reports, and by monitoring and enforcing Title 10 C.F.R 50.75 restrictions on decommissioning trust fund investments.

(Addresses Management and Performance Challenge # 2)

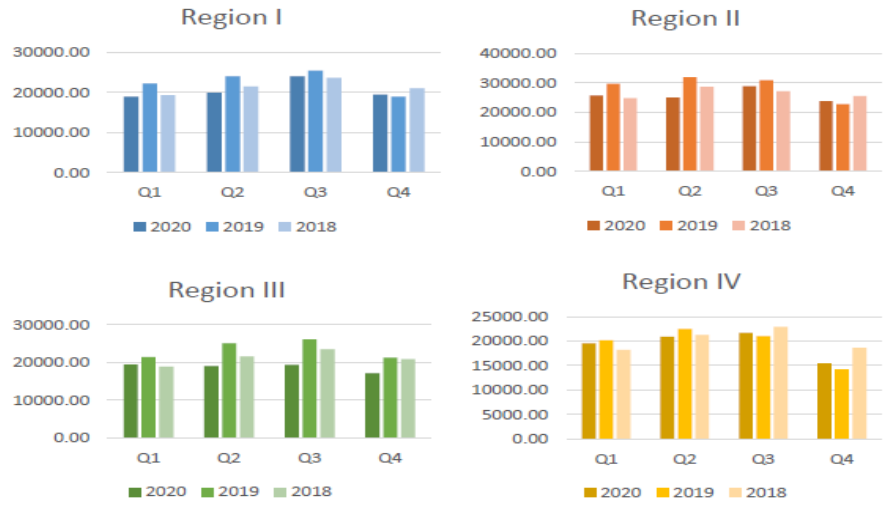
Audit of the NRC's Pandemic Oversight of Nuclear Power Plants

OIG Strategic Goal: Safety

As the COVID-19 PHE unfolded in early 2020, the NRC and licensees operating nuclear power plants responded to protect their employees and continue operations. The NRC and licensees implemented an array of COVID-19 precautionary measures and protocols to protect NRC inspectors and licensee employees. The NRC used inherent flexibilities in the Reactor Oversight Process (ROP) and hybrid inspection approaches to complete baseline inspection procedures while protecting NRC and licensee personnel health and safety.

NRC inspectors largely exceeded the minimum baseline inspection procedure sample requirements, but COVID-19 conditions presented challenges for completing of some inspection procedures.

Chart 1: Total Quarterly Regional Inspection Hours, Calendar Years 2020, 2019, 2018



Source: OIG analysis of NRC data.

The audit objective was to assess policies and procedures for conducting reactor inspections during the COVID-19 PHE and to identify best practices that could be applied during future pandemics or other public health emergencies.

Audit Results:

The OIG found that the NRC successfully adapted its inspections of nuclear power plants to meet its mission of obtaining reasonable assurance of adequate protection during the PHE while mitigating the

risks of COVID-19 to NRC inspectors and licensee staff. However, the agency's pandemic lessons learned process should include consideration of the possible impacts of adaptations to oversight processes on inspection results.

(Addresses Management and Performance Challenge # 3)

The Defense Contract Audit Agency Audit Report Number 01321-2019V10100018

OIG Strategic Goal: Corporate Management

The OIG and the DCAA have an interagency agreement whereby the DCAA provides contract audit services for OIG. The DCAA is responsible for the audit methodologies used to reach the audit conclusions, monitoring their staff's qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management and follow-up on agency actions initiated due to this report.

Audit Results:

At the request of the OIG, the DCAA audited Qi Tech, LLC, and provided the OIG with an audit report. The DCAA audit report, dated June 14, 2021, did not identify any questioned costs.

(Addresses Management and Performance Challenge # 8)

Audit of the NRC's Grants Pre-Award and Award Processes

OIG Strategic Goal: Corporate Management

The Omnibus Appropriations Act of 2009 (the Act) established the Integrated University Program between the NRC, the U.S. Department of Energy, and the National Nuclear Security Administration. The Act authorized the appropriation of $45 million per year from FY 2009 through FY 2019 with $15 million for each agency.

Combined, the NRC grants program from FY 2008 through FY 2019 comprised 533 grants and totaled roughly $185 million. The NRC dedicates approximately three full-time equivalent employees to grant pre-award and award processes.

The audit objectives were to determine if the NRC's policies and procedures for reviewing grant proposals and making awards comply with applicable federal regulations, and if internal controls over the pre-award and award processes are adequate.

Audit Results:
The OIG found that the NRC's policies and procedures for reviewing grant proposals and making awards comply with applicable federal regulations. The NRC has made improvements to the program, such as conducting extensive research of potential grantees prior to awarding a grant. In addition, the agency started performing a more robust analysis of grant funding and spending. However, internal controls over the pre-award and award grant processes need improvement. Specifically, the NRC should improve its grant review process and should maintain grant records in accordance with NRC policy.

(Addresses Management and Performance Challenge # 8)

Audit of the NRC's FY 2020 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management
In November 2002, Congress passed the 2002 Improper Payments Information Act (IPIA) to enhance the accuracy and integrity of federal payments. An improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. Improper payments also include any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts.

On July 22, 2010, the President signed the Improper Payments Elimination and Recovery Act (IPERA), which requires federal agencies to periodically review all programs and activities that the agency administers and identify all programs and activities that may be susceptible to significant improper payments. In addition, the IPERA requires each

agency to conduct recovery audits with respect to each program and activity of the agency that expends $1,000,000 or more annually, if conducting such audits would be cost effective. Lastly, the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA) amended the IPIA by establishing the Do Not Pay Initiative, which directs agencies to verify the eligibility of payments using databases before making payments.

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

Audit Results:
The OIG found that the NRC is compliant with the PIIA and does not have any material weaknesses in internal control. The NRC reported the required information and conducted the mandated risk assessment. The OIG concluded that agency reporting of improper payments is accurate and complete.

(Addresses Management and Performance Challenge # 8)

The Defense Contract Audit Agency (DCAA) Audit Report Number 01321-2019M10100001

OIG Strategic Goal: Corporate Management
The OIG and the DCAA have an interagency agreement whereby the DCAA provides contract audit services for OIG. The DCAA is responsible for the audit methodologies used to reach the audit conclusions, monitoring their staff's qualifications, and ensuring compliance with Generally Accepted Government Auditing Standards. The OIG's responsibility is to distribute the report to NRC management and follow-up on agency actions initiated due to this report.

Audit Results:
At the OIG's request, the DCAA audited Advanced Systems Technology Management, Inc., and provided the OIG with an audit report. The DCAA audit report, dated March 29, 2021, identified questioned costs to be addressed by NRC management.

(Addresses Management and Performance Challenge # 8)

Audit of the NRC's Use of Requests for Additional Information in Licensing Processes for Spent Nuclear Fuel

OIG Strategic Goal: Safety

The NRC licenses and regulates the storage of spent fuel, both at commercial nuclear power plants and at separate storage facilities. The NRC conducts a safety review prior to granting a license or certificate for the storage of spent fuel. A request for additional information (RAI) is the mechanism by which NRC staff collects the information needed in licensing requests to make a regulatory decision regarding whether a license or certificate should be granted, renewed, modified, or denied.

The audit objective was to assess the efficiency and effectiveness of the NRC's use of RAIs during the spent fuel licensing process.

Audit Results:

The OIG found that the NRC's use of RAIs during the spent fuel licensing process is effective and efficient. However, opportunities exist for improvement by enhancing understanding of the risk-informed concept as it relates to RAIs and facilitating effective management transition within the Division of Fuel Management.

(Addresses Management and Performance Challenges # 1 and 7)

Audits in Progress

Audit of the NRC's Fiscal Year 2021 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 contracted with Grant Thornton to conduct this annual audit.

The audit objectives are to:

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

(Addresses Management and Performance Challenge #8)

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

OIG Strategic Goal: Security

The Federal Information Security Modernization Act (FISMA) of 2014 outlines the information security management requirements for agencies, including the requirement for an annual independent assessment by agency Inspectors General. In addition, the FISMA includes provisions such as the development of minimum standards for agency systems, aimed at further strengthening the security of federal government information and information systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The evaluation objective is to conduct an independent assessment of the NRC's FISMA implementation for FY 2021.

(Addresses Management and Performance Challenge # 5)

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

OIG Strategic Goal: Corporate Management

The Digital Accountability and Transparency Act of 2014 (DATA Act) was enacted May 9, 2014 and requires federal agencies to report financial and payment data in accordance with data standards established by the U.S. Department of Treasury and the OMB. The data reported will be displayed on a public website. In addition, the DATA Act requires IGs to review the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality and accuracy of this information.

The objectives of this audit are to determine the completeness, timeliness, accuracy and quality of the data sampled, and to assess the implementation of the governing standards by the agency.

(Addresses Management Challenge #8)

Audit of the NRC's Change of Station Program

OIG Strategic Goal: Corporate Management

Within the federal government, a permanent change of station (PCS) is the transfer of an employee from one official work site to another or the assignment of a new appointee to his or her first assignment site on a permanent basis.

The Federal Travel Regulation (FTR), issued by the Administrator of General Services, governs, among other things, eligibility for relocation allowances (Chapter 302), and permanent change of station allowances for subsistence and transportation expenses. Much of the FTR, however, allows for agency discretion. The NRC's, MD 14.2, Relocation Allowances, provides NRC employees with the procedures, regulations, and

requirements necessary to relocate to a permanent official duty station or to make a last move home and to claim reimbursement for the allowable expenses.

The audit objective is to determine whether the NRC has established and implemented an effective system of internal control over the PCS program.

(Addresses Management and Performance Challenge # 8)

Audit of the NRC's Counterfeit Reactor Component Oversight

OIG Strategic Goal: Safety

Multiple NRC organizations play a role in overseeing nuclear power licensees' efforts to prevent the use of counterfeit, fraudulent, and suspect items (CFSI) in nuclear power reactors. The NRC performs vendor quality assurance inspections, which may focus on CFSI's based on risk insights. The NRC's cybersecurity inspections assess licensees' policies and procedures for ensuring the integrity of digital components that are installed in plant safety systems. In addition, the NRC's new reactor construction inspections provide oversight during reactor construction activities, and agency investigators follow up on CFSI allegations to determine if enforcement action is warranted.

The audit objective is to assess whether the NRC's oversight activities provide reasonable assurance that nuclear power reactor licensees' programs are adequately positioned to mitigate the risk of counterfeit, fraudulent, and suspect items in new and operating reactors.

(Addresses Management and Performance Challenge # 1)

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

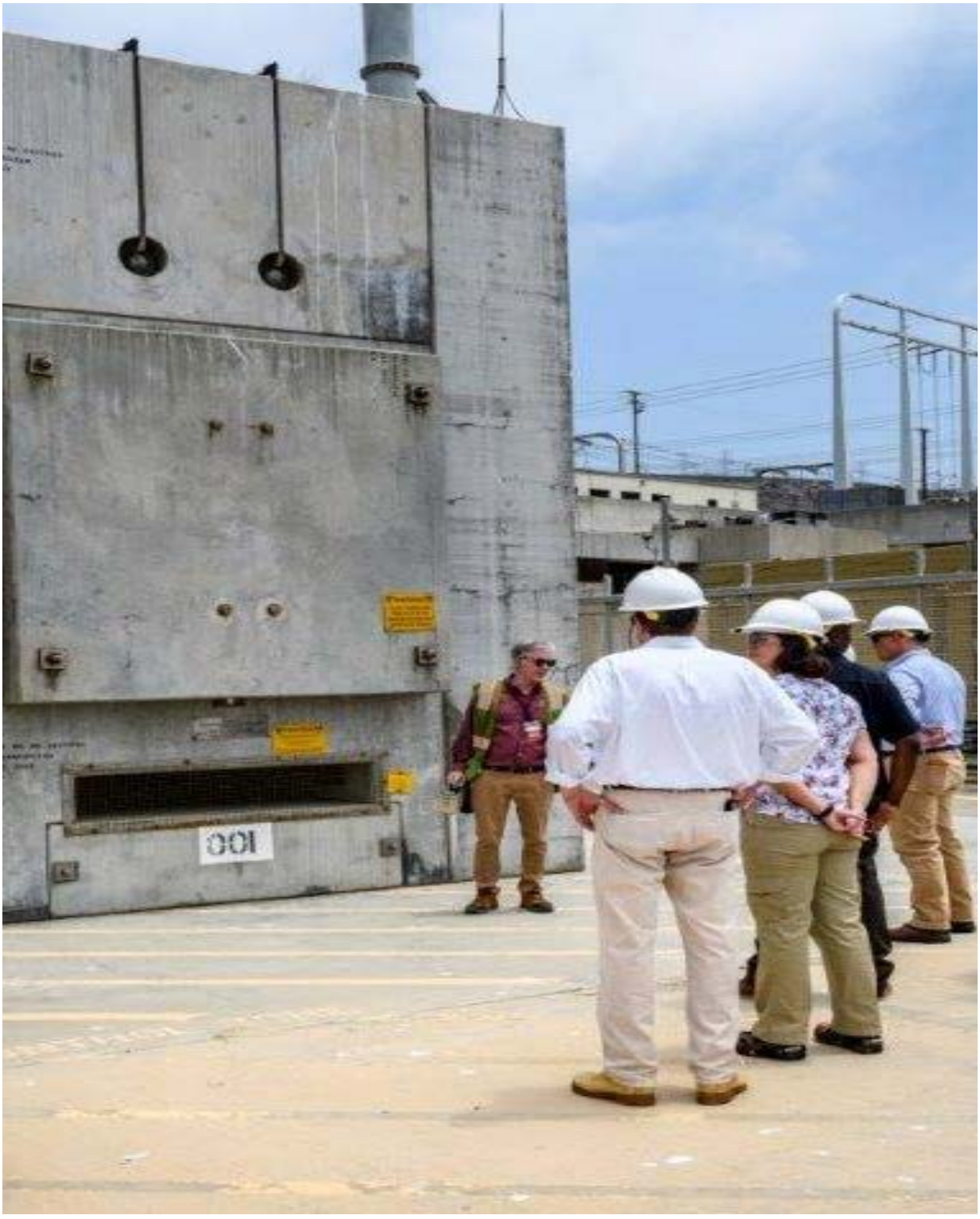
OIG Strategic Goal: Corporate Management

External stakeholders have expressed concern about the frequency of senior agency management interactions with nuclear power industry representatives, some of which coincide with regulatory decisions such as backfit appeals. The NRC guidance requires staff to avoid discussing specific details of regulatory matters with industry representatives in non-

public interactions, although staff members are permitted to discuss general information pertaining to agency activities.

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

(Addresses Management and Performance Challenge # 1)



The IG and staff view spent fuel storage canisters that are under tons of concrete at SONGS.

NRC INVESTIGATIONS

Investigative Summaries

Inaccurate Information Regarding Lead Test Assemblies In 2020 Clinton Inspection Report

OIG Strategic Goal: Safety

Allegation:
We initiated this investigation based on multiple concerns from employees, interest groups, and the public who allege that NRC senior managers have allowed inconsistent adherence to established policies required to license new accident tolerant fuel (ATF) lead test assemblies (LTAs). Specifically, despite opposing stakeholder comments, NRC senior managers have supported licensing ATF LTAs without requiring license amendments, and have approved topical reports or exemptions for compliance with 10 C.F.R § 50.59 and 10 C.F.R § 50.46. In addition, allegers report that Technical Specification 5.6.5 (TS 5.6.5), "Core Operating Limits Report," does not use NRC-approved methods as required for compliance with 10 C.F.R § 50.36.

Investigative Results:
We observed that though the NRC has established processes for approving licensee requests to use new ATF LTAs and new cladding material, the NRC staff has accepted variations and inconsistencies in the approach to meeting regulatory requirements over the years. In addition, the NRC Office of the General Counsel stated in 2017 that staff has discretion to determine when 50.46 exemptions are required for ATF LTA use. Specifically, the NRC has allowed plants to change cladding material with and without receiving exemptions from 50.46 and to install LTAs with and without license amendment requests (LARs) over the past 20 years. Between 2018 and 2019, the NRC clarified this approach to say that licensees could use LTAs under 50.59 or a LAR. The OMB reviewed the NRC's clarification and determined it was not a major rule change. The NRC should consider reviewing this inconsistent approach in light of the NEIMA and ATF's emerging prevalence.

We also found that NRC staff may have misled the OEDO, industry, and the public when it reported the completion of an OEDO tasking, but had not done so. Due to confusion over roles and responsibilities, a regional office did not review Clinton Power Station's COLR for compliance with TS 5.6.5, including "the analytical methods that were previously reviewed and approved by the NRC," as required by the OEDO tasking.

This investigation resulted in a memorandum to the OEDO that asked how the NRC would address inconsistencies in the licensees' approach for compliance with LTA regulations with emerging ATF technology and what the agency can do to prevent future confusion about staff's roles and responsibilities. The OIG asked how the agency planned to correct the inaccurate reporting that the COLR for Clinton had been reviewed, a review that was required based on an OEDO tasking.

Agency Response:
We issued a report to the OEDO in January 2021 with a response due date of April 2, 2021, and briefed the Commission on its contents.

Impact:
To date, the OIG has not received a response from the OEDO.

(Addresses Management and Performance Challenge #1)

Release of Predecisional Information Reveals Difference of Opinion Regarding the NRC's Enforcement Processes

OIG Strategic Goal: Safety

Allegation:
We initiated this investigation based on information from the NRC that an NRC senior manager released predecisional information to a licensee. The OIG investigated the circumstances and NRC's oversight as a result of this release.

Investigative Results:
We found that the NRC senior manager violated MD 3.4, Release of Information to the Public, when the senior manager released predecisional information to the licensee without prior approval. Although the senior

manager believed the information that he released was relative to the ROP and was not predecisional, the region's senior leadership disagreed and initially took actions by informing the OIG of the violation, counseling the senior manager, and requiring the senior manager to conduct a lessons-learned presentation to other regional managers. However, the OIG was then told by regional officials that after further consultation, the region had no consensus as to whether there had been a release of predecisional information.

Additionally, the OIG identified differences of opinion within the regional office and an NRC headquarters office regarding its interpretation of the NRC's Enforcement Manual, the nuances of each process, and what constitutes predecisional information. For example, instead of implementing the NRC's required Traditional Enforcement Process (TEP) as was begun in this case and issuing a choice letter to the licensee with the NRC's factual summary of apparent violations of escalated enforcement including willfulness, the licensee was informed of the agency's investigative information by a telephonic exit briefing, a procedure permitted in the ROP but not in the TEP.

This investigation resulted in a memorandum to the OEDO that asked how the NRC would address the difference of opinion regarding NRC's enforcement processes and how it would clarify what constitutes predecisional information as it relates to the enforcement process.

Agency Response:
After the OIG provided a report to and briefed the OEDO, the OEDO committed to developing agencywide training to assess and dispose of violations of NRC requirements using the TEP and the ROP.

Impact:
To date, no training has been developed.

(Addresses Management and Performance Challenge #1)

Theft Of NRC-Owned Laptop Computers

OIG Strategic Goal: Corporate Management

Allegation:
We initiated this investigation based on an allegation received from the NRC Office of the Chief Information Officer (OCIO) that reported a September 2019 inventory of NRC-owned Dell i5-8350U laptop computers identified 63 laptops missing. According to OCIO staff, the NRC received new laptops at the NRC warehouse between February and August 2019. The laptops were transferred to the NRC Logistics Management Center to be inventoried.

Investigative Results:
The report led to an extensive investigation by the NRC OIG and the Montgomery County, Maryland, Police Department that included computer forensics, suspect interviews, and the execution of search warrants. The OIG identified the perpetrator, who was an OCIO IT contractor, and on September 1, 2021, the contractor pleaded guilty in the Circuit Court for Montgomery County, Maryland, to misappropriation by a fiduciary/embezzlement for the theft of government laptops belonging to the NRC, a crime that carries a maximum penalty of 5 years' imprisonment.

Impact:
As part of the plea agreement, the contractor paid $54,384 in restitution directly to the NRC for the theft of 33 of the laptops. Additionally, his access to NRC buildings was terminated immediately after being interviewed by the OIG, and he was subsequently fired by the contactor.

(Addresses Management and Performance Challenge #5)

Retaliation For Submitting A Differing Professional Opinion

OIG Strategic Goal: Corporate Management

Allegation:
We initiated this investigation based on an allegation of retaliation. The alleger claimed that an NRC senior manager retaliated against the alleger by influencing an interview panel not to select the alleger to be a part of a Senior Executive Service Candidate Development Program (SESCDP).

The alleger claimed that retaliation stemmed from the alleger's submittal of a differing professional opinion the year before regarding security issues and because the alleger was involved in, and made negative findings during an assessment of a program implementation, both of which involved the executive's branch.

Investigative Results:
We did not find that the NRC senior manager retaliated against the alleger during the SESCDP selection process, or that the NRC senior manager influenced others on the panel to exclude the alleger from the SESCDP class. Of 450 applicants to the SESCDP, the alleger was 1 of only 54 interviewed for selection into the program, which had only 25 spots available. The OIG found that the three-person interview panel was composed appropriately, and none of the panel members felt undue influence by another. The score sheets indicated that the NRC senior manager was not always the lowest scorer and that for some of the scoring categories, the NRC senior manager scored the alleger higher than the other two panelists did.

(Addresses Management and Performance Challenge #1)

Mismanagement of A Desk Audit

OIG Strategic Goal: Corporate Management

Allegation:
We initiated this investigation based on an allegation that two NRC senior managers conspired to deny a promotion to an NRC employee following an NRC desk audit which found that the NRC employee's position duties should be at a higher level than they were. OIG investigated whether the two conspired against the NRC employee, whether a NRC senior manager denied the NRC employee a promotion, and whether the agency denied the NRC employee or the employee's supervisor the right to appeal the senior manager's decision.

Investigative Results:
We did not find that the two NRC senior managers conspired against the NRC employee. The two senior managers had conversations regarding the results of the desk audit and the options provided by NRC Human Resources (HR) for filling the position. The NRC senior manager provided HR information about another NRC employee familiar with the NRC

employee's work and who was at least minimally qualified for the position, which led HR to recommend the position be filled through the competitive promotion process. The OIG further found that the original options paper submitted to the NRC senior manager offered the noncompetitive promotion of the NRC employee to the higher grade through accretion of duties, but that paper was mistakenly sent without authorization by an HR specialist without authorization. The final, official options paper was sent to the NRC senior manager with the rest of the supporting documentation derived from the desk audit.

We did not find that the NRC senior manager denied the NRC employee a promotion. We found the NRC senior manager stayed within the bounds of the management directive. We also did not find that the agency denied the NRC employee or the employee's immediate supervisor their right to appeal the senior manager's decision not to promote the NRC employee noncompetitively.

(Addresses Management and Performance Challenge #6)

Disparate Treatment and Hostile Work Environment

OIG Strategic Goal: Corporate Management

Allegation:
We initiated this investigation based on allegations that an NRC senior manager managed staff members with threats and fear, creating a hostile work environment. The allegers claimed that NRC employees of the same race as the NRC senior manager were assigned less work, received better performance appraisals, and were approved for more training than those of a different race. The NRC senior manager is also alleged to have used an inappropriately aggressive management style that included threats, ultimatums, bullying, and intimidating behaviors to address staff performance.

Investigative Results:
We did not find evidence to substantiate the claim that the NRC senior manager violated the NRC's harassment policy or retaliated against staff. However, the OIG did find that current and former employees of the senior manager who were interviewed perceived a chilled work environment. Specifically, most told the OIG that the senior manager had

a hostile and intimidating management style, and they were afraid to raise issues involving the senior manager out of fear of retaliation. Conversely, some interviewees told us that the senior manager was supportive and did not show hostile or intimidating behavior.

Agency Response and Impact:
The NRC OEDO responded to our report, saying that it is closely monitoring the environment and that it has taken substantial actions to improve the office culture and to address past work environment issues. The OEDO also stated that it has provided the individual involved with additional mentoring and training in performance management, emotional intelligence, communications, and dealing with sensitive personnel issues.

(Addresses Management and Performance Challenge #6)

NRC Withholding Documents from the Public Concerning an Exigent License Amendment Request for Diablo Canyon Nuclear Power Plant

OIG Strategic Goal: Safety

Allegation:
We initiated this investigation based on an allegation from a public stakeholder that NRC staff violated federal regulations and agency procedures with its handling of the public notice for the exigent license amendment request (LAR) submitted by a licensee at a nuclear power plant. Specifically, the alleger claimed that the NRC violated 10 C.F.R § 50.91, Notice for Public Comment; State Consultation, and NRC MD 3.4, Release of Information to the Public.

Investigative Results:
We substantiated these allegations that the NRC violated MD 3.4 by not adhering to the 5-day goal of releasing documents to the public in the Agencywide Document Access Management System, and violated 10 C.F.R. § 50.91 by not affording a reasonable opportunity for the public to comment. MD 3.4 states that documents produced by NRC staff that are addressed to external parties are to be released no later than 5 working days after the date of the document. The cover letter for the public notice of application for amendments was dated August 13, 2020, but was not

publicly released until August 26, 2020, thus violating the 5-day requirement. The NRC sent the power plant three RAIs; however, the plant's responses to those RAIs were originally not intended to be released to the public until after the public comment period closed. At the behest of the alleger, NRC staff released these responses to the public approximately 30 minutes before the public comment period closed, which did not enable the public to comment fully.

Impact:
As a result of our investigation, the NRC issued Yellow Announcement YA-20-0075 (internal announcement) reminding employees of the NRC's policy on the timing of the release of documents to the public. The NRC Commission was also briefed on the findings.

(Addresses Management and Performance Challenge #1)

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Congress created the Defense Nuclear Facilities Safety Board (DNFSB) as an independent agency within the executive branch to identify the nature and consequences of potential threats to public health and safety at the U.S. Department of Energy's (DOE) defense nuclear facilities, to elevate such issues to the highest levels of authority, and to inform the public. 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 NRC was authorized in 2014, and subsequent years, to exercise the same authorities with respect to the DNFSB, as determined by the Inspector General of the NRC, as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the NRC.

DNFSB MANAGEMENT AND PERFORMANCE CHALLENGES

Most Serious Management and Performance Challenges Facing the Defense Nuclear Facilities Safety Board in FY 2021*   ***(as identified by the Inspector General)***
Challenge 1: *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

Audit of the DNFSB's Fiscal Year (FY) 2020 Compliance with Improper Payment Laws

OIG Strategic Goal: Corporate Management

Enacted in 2020, the Payment Integrity Information Act (PIIA) requires federal agencies to periodically review all programs and activities the agency administers, and identify all programs and activities that may be susceptible to significant improper payments. Programs are considered to be significant if, in the preceding fiscal year, the sum of a program or activity's improper payments, and payments whose propriety cannot be determined, may have exceeded $10,000,000 of all reported program or activity payments made during that fiscal year, and 1.5 percent of program outlays, or $100,000,000. Federal agencies should assess programs and activities susceptible to improper payment risk at least once every three years.

The PIIA repealed the 2002 IPIA, the IPERA, the IPERIA, and the 2015 Fraud Reduction and Data Analytics Act (FRDAA). The PIIA incorporates select provisions from the IPIA, the IPERA, the IPERIA, and the FRDAA into a single subchapter in the U.S. Code, while also introducing new aspects into the payment integrity statutory framework.

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

Audit Results:

The OIG found that the DNFSB is compliant with the PIIA and does not have any material weaknesses in internal control. The DNFSB reported the required information and conducted the mandated risk assessment. The OIG concluded that agency reporting of improper payments is accurate and complete.

(Addresses Management and Performance Challenge # 3)

Office of the Inspector General 2021 DNFSB Safety Culture and Climate Survey

OIG Strategic Goal: Corporate Management

Beginning in the Fall of 2020, Willis Towers Watson partnered with the OIG to assess the DNFSB's safety culture and climate as well as other aspects of employee experience such as engagement. This survey served as a follow-up to the 2015 DNFSB Culture and Climate Survey. Willis Towers Watson conducted the 2021 DNFSB Safety Culture and Climate Survey for approximately 95 employees in January of 2021. The survey was designed based on information gathered from leadership interviews and staff focus groups. The analysis from the interviews and focus group meetings aided in the development of the survey instrument.

The objectives of this survey were to:

(1) Measure the DNFSB's culture and climate to identify areas of strength and opportunities for improvement; and,

(2) Provide, where practical, benchmarks for the qualitative and quantitative findings against other organizations.

Survey Results:

The results of the 2021 DNFSB Safety Culture and Climate Survey show strong improvements since the 2015 survey. Improvements were made in all survey categories and only two survey items decreased from 2015. Compared to external benchmarks, the DNFSB's greatest strengths focus on work quality and supervision. Whereas, areas of opportunity concentrate on empowerment, change management, leadership, and development.

(Addresses all Management and Performance Challenges)

Audits in Progress

Audit of the DNFSB's Compliance with Standards Established by the Digital Accountability and Transparency Act of 2014

OIG Strategic Goal: Corporate Management

The Digital Accountability and Transparency Act of 2014 (DATA Act) was enacted May 9, 2014 and requires federal agencies to report financial and payment data in accordance with data standards established by the U.S. Department of Treasury and the Office of Management and Budget. The data reported will be displayed on a website available to taxpayers and policy makers. In addition, the DATA Act requires IGs to review the data submitted by the agency under the act and report to Congress on the completeness, timeliness, quality and accuracy of this information.

The objectives of this audit are to: (1) determine the completeness, timeliness, accuracy and quality of the data sampled; and, (2) assess the implementation of the governing standards by the agency.

(Addresses Management and Performance Challenge # 3)

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

OIG Strategic Goal: Corporate Management

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

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

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

(Addresses Management and Performance Challenge # 3)

Audit of the DNFSB's Fiscal Year 2021 Financial Statements

OIG Strategic Goal: Corporate Management

The CFO Act requires the IG or an independent external auditor, as determined by the IG, to annually audit the NRC's financial statements in accordance with applicable standards. In compliance with this requirement, the OIG contracted with Grant Thornton to conduct this annual audit.

The audit objectives are to:

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

(Addresses Management and Performance Challenge # 3)

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

OIG Strategic Goal: Corporate Management

The DNFSB routinely develops an annual plan to conduct oversight of DOE defense nuclear facilities. The DNFSB's independent oversight of DOE defense nuclear facilities is carried out by technical experts located at DNFSB headquarters, as well as by Resident Inspectors (RIs) who are located at the various facilities throughout the country. Together, this

cadre of highly experienced and knowledgeable staff conduct inspections to determine if the facilities are operated safely and in accordance with established regulations.

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

(Addresses Management and Performance Challenge # 4)

DNFSB INVESTIGATIONS

Investigative Case Summaries

While the OIG did not close any DNFSB investigations during this reporting period, we did initiate two proactive efforts to identify fraud within DNFSB programs and operations, and potential computer misuse and cybersecurity issues.

Fraud

This proactive initiative seeks to identify potential procurement, credit card, travel voucher, or worker's compensation fraud within DNFSB programs and operations. This project relies heavily on our fraud investigators and a collaborative effort from our entire investigative team, their input, and use of their established relationships within the DNFSB.

Computer Misuse and Cybersecurity

This proactive initiative involves our dedicated Cyber Crimes Unit (CCU), which is reviewing DNFSB employees' computer use for potential misuse and cybersecurity issues. The OIG established the CCU to focus on investigations involving computers and related digital evidence at the NRC and DNFSB. Since its establishment, this unit has successfully conducted numerous investigations, including several stemming from proactive investigative initiatives.

Fuel transfer operations at SONGS

SUMMARY OF OIG ACCOMPLISHMENTS AT THE NRC

April 1, 2021 – September 30, 2021

Allegations Received from the NRC OIG Hotline: 25

Investigative Statistics

Source of Allegations	
NRC Employee	19
NRC Management	21
Congressional	2
General Public	22
Other Government Agency	2
Anonymous	18
Media	2
Regulated Industry (Licensee/Utility)	2
TOTAL:	**88**

Disposition of Allegations	
Closed Administratively	34
Correlated to Existing Case	14
Initiated OIG Investigation	5
Referred to OIG Audit	3
Referred to NRC Management	27
Referred to Other Agency	5
TOTAL:	**88**

Status of Investigations

Federal	
DOJ Referrals	3
DOJ Declinations	2
DOJ Accepted	1
DOJ Pending	1
Criminal Information/Indictments	0
Criminal Convictions	0
Criminal Penalty Fines	0
Civil Recovery	0
State and Local	
State and Local Referrals	0
Criminal Convictions	1
Administrative Recovery	$54,384.00
NRC Administrative Actions	
Counseling and Letter of Reprimand	0
Action Pending	2
Terminations and Resignation	0
Suspensions and Demotions	0
Other (e.g., PFCRA)*	5

**Review of Agency Process*

Summary of Investigations

Classification of Investigations	Carryover	Opened Cases	Closed Cases	Reports Issued*	Cases in Progress
Employee Misconduct	3	2	1	0	4
Event Inquiry	1	1	0	0	2
Management Misconduct	8	1	4	2	5
Proactive Initiatives	4	0	0	0	4
Technical Allegations	7	4	3	1	8
Theft	1	0	1	0	0
TOTAL:	**24**	**8**	**9**	**3**	**23**

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

NRC Audits Completed

Date	Title	Audit Number
09/30/2021	Audit of the NRC's Prohibited Security Program	OIG-21-A-17
09/28/2021	Audit of the NRC's Implementation of the Enterprise Risk Management	OIG-21-A-16
09/23/2021	Audit of COVID-19's Impact on Nuclear Materials and Waste Oversight	OIG-21-A-15
08/19/2021	Audit of the NRC's Oversight of the Adequacy of Decommissioning Trust Funds	OIG-21-A-14
08/04/2021	Audit of the NRC's Pandemic Oversight of Nuclear Power Plants	OIG-21-A-13
07/08/2021	The Defense Contract Audit Agency (DCAA) Audit Report Number 01321-2019V10100018	OIG-21-A-12
06/08/2021	Audit of the NRC's Grants Pre-Award and Award Processes	OIG-21-A-11
05/13/2021	Audit of the NRC's FY 2020 Compliance with Improper Payment Laws	OIG-21-A-10
04/14/2021	The Defense Contract Audit Agency (DCAA) Audit Report Number 01321-2019M10100001	OIG-21-A-09
04/09/2021	Audit of the NRC's Use of Requests for Additional Information in Licensing Processes for Spent Nuclear Fuel	OIG-21-A-08

NRC Contract Audit Reports

OIG Issue Date	Contractor/Title/Contractor No.	Questioned Costs	Unsupported Costs
	Advanced Systems Technology Management, Inc.		
April 14, 2021	Independent Audit Report on Advanced Systems Technology Management, Inc.'s Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Year Ended December 31, 2019 NRC-HQ-7G-14-C-0001	$116,723	$0
	Qi Tech LLC		
July 8, 2021	Independent Audit Report on Qi Tech LLC's Proposed Amounts on Unsettled Flexibly Priced Contracts for Fiscal Year Ended December 31, 2019 NRC-HQ-7G-14-C-0001	$0	$0

NRC Audit Resolution Activities

Table I

***OIG Reports Containing Questioned Costs*†**

Reports	Number of Reports	Questioned Costs ($)	Unsupported Costs ($)
A. For which no management decision had been made by the commencement of the reporting period	3	$1,897,205	0
B. Which were issued during the reporting period	1	$116,723	0
Subtotal (A + B) ‡	4	$2,013,928	0
C. For which a management decision was made during the reporting period:			
i. Dollar value of disallowed costs	0	0	0
ii. Dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	4	$2,013,928	0

* *The OIG questions costs 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.*

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

Table II

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

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

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

Table III

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

No Data to report

SUMMARY OF OIG ACCOMPLISHMENTS AT THE DNFSB

April 1, 2021 – September 30, 2021

Source of Allegations

Allegations Received from the DNFSB OIG Hotline: 0

Investigative Statistics

Source of Allegations

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

Disposition of Allegations

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

Status of Investigations

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

Summary of Investigations

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

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

DNFSB Audits Completed

Date	Title	Audit Number
06/21/2021	Audit of the DNFSB's Fiscal Year (FY) 2020 Compliance with Improper Payment Laws	DNFSB-21-A-06
04/29/2021	Office of the Inspector General 2021 DNFSB Safety Culture and Climate Survey	DNFSB-21-A-05

DNFSB Audit Resolution Activities

Table I

OIG Reports Containing Questioned Costs*

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

** The OIG questions costs 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
Subtotal (A + B)	0	0	0
C. For which a management decision was made during the reporting period:			
i. Dollar value of disallowed costs	0	0	0
ii. Dollar value of costs not disallowed	0	0	0
D. For which no management decision had been made by the end of the reporting period	0	0	0

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

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 Safeguards Information (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 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(b): Complete the current inventories of classified information in safes and secure storage areas.

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 Cyber Security Inspections at Nuclear Power Plants (OIG-19-A-13)

1 of 2 recommendations open since June 4, 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 September 5, 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)

1 of 2 recommendations open since September 13, 2019

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.

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 April 29, 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)

5 of 13 recommendations open since June 2, 2020

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

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

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

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 Drug-Free Workplace Program Implementation (OIG-20-A-13)

2 of 4 recommendations open since August 8, 2020

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

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

Audit of NRC's 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 30, 2020

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

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

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 the timely and completely documenting of the status of leasehold improvements in process.

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

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

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

Audit of 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 19, 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)

3 of 4 recommendations open since March 29, 2021

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

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

Recommendation 4: Conduct periodic training regarding RPS data input.

Audit of the NRC's Use of Requests for Additional Information in Licensing Processes for Spent Nuclear Fuel (OIG-21-A-08)

3 of 3 recommendations open since April 09, 2021

Recommendation 1: Update guidance to document strategies or tools to be used for risk-informing requests for additional information.

Recommendation 2: Conduct training across the division on how to risk-inform relative to the request for additional information process, and conduct refresher training on an as needed, periodic basis.

Recommendation 3: Create and implement a formalized process to facilitate effective management transitions in the Division of Fuel Management.

Audit of the NRC's Grants Pre-Award and Award Processes (OIG-21-A-11)

2 of 4 recommendations open since July 08, 2021

Recommendation 1: Revise agency policies to require:
(a) a review of applicants' geographic diversity, diversity in technical disciplines, prior award performance issues, number of prior NRC awards, and current unexpended grant funds, including the NRC staff responsible for the review; and,
(b) a review of the NRC's suspended Automated Standard Application for Payments account list to determine applicants' performance histories, including the NRC staff responsible for the review.

Recommendation 2: Develop agency guidance for when to use additional and specific conditions in grant agreements for awardees that have prior inconsistent application of grant requirements.

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

1 of 1 recommendation open since August 04, 2021

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

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

4 of 4 recommendations open since August 19, 2021

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

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

Recommendation 3: Implement a central tracking mechanism to track the status of the annual DFS report analyses; and,

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

DNFSB

Audit of the DNFSB's Telework Program (DNFSB-17-A-06)

2 of 3 recommendations open since July 20, 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.

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 07, 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 January 27, 2020

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

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

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

7 of 11 recommendations open since March 31, 2020

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

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

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

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

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

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

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

14 of 14 recommendations open since March 25, 2021

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

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

Recommendation 3: Using the results of 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 21.

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 21, 2020

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

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

ABBREVIATIONS AND ACRONYMS

ATF	Accident Tolerant Fuel
CCU	Cyber Crimes Unit
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CFR	Code of Federal Regulations
COVID-19	Coronavirus Disease 2019
DCAA	Defense Contract Audit Agency
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOJ	Department of Justice
DPO	Differing Professional Opinion
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FRDAA	Fraud Reduction and Data Analytics Act
FTR	Federal Travel Regulation
FY	Fiscal Year
GAO	Government Accountability Office
HR	Human Resources
IAM	Issue Area Monitoring
IG	Inspector General
IPERA	Improper Payments Elimination and Recovery Act
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IPIA	Improper Payments Information Act
IT	Information Technology
LAR	License Amendment Request
LTAs	Lead Test Assemblies
MC&A	Material Control and Accounting
MD	Management Directive
NRC	Nuclear Regulatory Commission
OEDO	Office of the Executive Director for Operations
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PHE	Public Health Emergency
PIIA	Payment Integrity Information Act of 2019
RAI	Request for Additional Information
ROP	Reactor Oversight Process
SESCDP	Senior Executive Service Candidate Development Program
TEP	Traditional Enforcement Process

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
Section5(a)(14)(15)(16)	Peer review Information	75
Section 5(a)(17)	Investigations statistical tables	40-50; 55-56
Section 5(a)(18)	Description of metrics	50, 56
Section 5(a)(19)	Investigations of senior government officials where misconduct was substantiated	N/A
Section 5(a)(20)	Whistleblower retaliation	N/A
Section 5(a)(21)	Interference with IG independence	N/A
Section 5(a)(22)	Audit not made public	20
Section 5(a)22(b)	Investigations involving senior government employees where misconduct was not substantiated, and report was not made public	30-35; 36-37; 38-40

APPENDIX

Peer Review Information

Audits

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

Investigations

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

The NRC OIG Hotline

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

What should be reported:

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

Ways To Contact the OIG

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

Submit:
Online Form www.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. 2 October 2021

@NRCgov