OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

SPECIAL REPORT

DOE-OIG-18-09 November 2017

MANAGEMENT CHALLENGES AT THE DEPARTMENT OF ENERGY - FISCAL YEAR 2018

Department of Energy
Washington, DC 20585

November 27, 2017

MEMORANDUM FOR THE SECRETARY

FROM: April Stephenson
Principal Deputy Inspector General

SUBJECT: INFORMATION: Special Report on "Management Challenges at the Department of Energy – Fiscal Year 2018"

INTRODUCTION

The Department of Energy's mission is to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions. The Department's world-leading science and technology enterprise generates the innovations that fulfill its missions. Through 17 national laboratories, the Department engages in cutting-edge research that expands the frontiers of scientific knowledge, generates new technologies to address the country's greatest energy challenges, and strengthens national security by maintaining and modernizing the nuclear stockpile. To execute this diverse portfolio, the Department receives an annual appropriation of approximately $30 billion, employs approximately 111,000 Federal and contractor personnel, and manages assets valued at $185.5 billion. The Office of Inspector General annually identifies what it considers to be the most significant management challenges facing the Department. The Office of Inspector General's goal is to focus attention on significant issues with the objective of working with Department managers to enhance the effectiveness of agency programs and operations.

MANAGEMENT CHALLENGES

While the fiscal year 2018 challenge areas remain largely consistent with those in previous years, based on the results of our work over the last year, we made a few changes. As a result, the fiscal year 2018 management challenges include the following:

- Contract Oversight
  - Contractor Management
  - Subcontract Management
- Cybersecurity
- Environmental Cleanup
- Nuclear Waste Disposal
- Safeguards and Security
- Stockpile Stewardship
- Infrastructure Modernization

The changes to this year's report includes the addition of Subcontract Management as a component of Contract Oversight. Over the past year, the work of the Office of Inspector General has shown Subcontract Management is an increasing challenge for the Department. In one instance, the Justice Department, in conjunction with the Office of Inspector General Office of Investigations, announced one of the Department's subcontractors had agreed to pay $4.6 million to resolve the government's lawsuit filed under the False Claims act alleging that it knowingly failed to perform required quality assurance procedures and supplied defective steel reinforcing bars in connection with a contract to construct a nuclear waste treatment facility at the Department. Given the large volume of contracts awarded by the Department and its management and operating contractors and the need for adequate oversight of subcontractors, we added Subcontract Management as a component of the Contract Oversight challenge.

WATCH LIST

The Office of Inspector General also prepared an annual Watch List, which incorporates other issues that do not meet the threshold of a management challenge, yet in our view, warrant special attention by Department officials. For fiscal year 2018, the Watch List includes the Department's Employee Concerns Program, the Power Marketing Administrations, Human Capital Management, the Loan Guarantee Program, and Worker and Community Safety.

SUMMARY

Attached is a brief synopsis of each management challenge, accompanied by summaries of reports and Department of Justice press releases that informed our decision process. A complete list of reports can be found at: https://energy.gov/ig/calendar-year-reports and press releases may be found at: https://energy.gov/ig/listings/media-releases.

The management challenges process is an important tool that assists us in focusing our finite resources on what we consider to be the Department's most significant risks and vulnerabilities. We look forward to working with you and your leadership team in addressing and resolving these issues.

Attachment

cc: Deputy Secretary
Chief of Staff
Administrator, National Nuclear Security Administration
Under Secretary of Energy
Under Secretary for Science
Chief Information Officer
Acting Chief Financial Officer

Contract Oversight

The Department of Energy is the largest civilian contracting agency in the Federal Government and spends approximately 90% of its annual budget on contracts to operate its scientific laboratories, engineering and production facilities, environmental restoration sites, and large capital asset projects. In fiscal year (FY) 2016, the Department managed 11,311 contracts valued at more than $24 billion. Additionally, according to the Office of Acquisition Management, the Department's management and operating contractors reported over $354 million in subcontracts during FY 2017.

Oversight of the Department's contracts is necessary to ensure that contractors meet the established requirements, from contract award through completion or termination. Contract oversight starts with the development of a clear, concise performance based statement of work and a plan that effectively measures the contractor's performance. The specific nature and extent of oversight varies by contract and can range from simple acceptance of delivery and payment to extensive involvement by program, audit and procurement officials. The goal of effective contract oversight is to ensure that the government receives procured products and services and that the public interest is effectively protected.

The Department has been challenged, both internally and externally, to improve the efficiency and effectiveness of its contract oversight process. Since 1990, the Government Accountability Office has designated the Department's contract management, which included inadequate contract and project oversight, as a high risk area. In addition, our investigative work and referrals to the Office of Inspector General (OIG) Hotline have identified continued vulnerabilities with less than adequate subcontract oversight. Because of these issues and the large number of contracts and subcontracts managed by the Department, this year's management challenges report broadens the area of Contract Oversight to include Contractor Management and Subcontract Management as sub-components.

Contractor Management

In February 2017, the Government Accountability Office reported that the Department did not have the capacity to resolve contract and project management problems, nor did the Department demonstrate progress toward implementing measures to resolve high-risk areas. Further, our FY 2017 audit, inspection and investigative work identified numerous issues related to contractor management. Specifically, we found issues/weaknesses with contractor quality assurance programs and requirements, including contractors' ability to manage quality assurance of procurements.

The Government Accountability Office acknowledged that the Department continued to meet the leadership commitment criteria and partially meet the criteria for having a corrective action plan. The Agency further acknowledged that the Department had improved its monitoring of the effectiveness of corrective measures.

However, given the number of contracts handled by the Department and the complexity and importance of the Department's numerous multimillion dollar projects, the area of Contract Management is a significant management challenge.

The following reports and Department of Justice press releases highlight the need for continued focus by the Department in contract management.

United States Settles Lawsuit Against Energy Department Contractors for Knowingly Mischarging Costs on Contract at Nuclear Waste Treatment Plant
November 23, 2016 Department of Justice Press Release

The Justice Department announced that Bechtel National Inc., Bechtel Corp., URS Corp., (predecessor in interest to AECOM Global II LLC) and URS Energy and Construction Inc. (now known as AECOM Energy and Construction Inc.) have agreed to pay $125 million to resolve allegations under the False Claims Act that they made false statements and claims to the Department by charging the Department for deficient nuclear quality materials, services, and testing that was provided at the Waste Treatment and Immobilization Plant (WTP) at the Department's Hanford Site near Richland, Washington. The settlement also resolves allegations that Bechtel National Inc. and Bechtel Corp. improperly used federal contract funds to pay for a comprehensive, multi-year lobbying campaign of Congress and other federal officials for continued funding at the WTP.

Between 2002 and the present, the Department has paid billions of dollars to the defendants to design and build the WTP, which will be used to treat dangerous radioactive wastes that are currently stored at the Department's Hanford Site. The contract required materials, testing, and services to meet certain nuclear quality standards. The United States alleged that the defendants violated the False Claims Act by charging the government the cost of complying with these standards when they failed to do so. In particular, the United States alleged that the defendants improperly billed the government for materials and services from vendors that did not meet quality control requirements, for piping and waste vessels that did not meet quality standards, and for testing from vendors who did not have compliant quality programs. The United States also alleged that Bechtel National Inc. and Bechtel Corp. improperly claimed and received government funding for lobbying activities in violation of the Byrd Amendment, and applicable contractual and regulatory requirements, all of which prohibit the use of federal funds for lobbying activities. The claims asserted against the defendants are allegations only and there has been no determination of liability.

The full press release is available at: https://energy.gov/sites/prod/files/2016/11/f34/Department of Justice.pdf

Quality Assurance Management at the Waste Isolation Plant
September 2017, DOE-OIG-17-07

The Department's Waste Isolation Pilot Plant (WIPP) in southeastern New Mexico is the nation's only geologic repository for the disposal of radioactive waste materials generated by atomic energy defense activities. WIPP is managed and operated by Nuclear Waste Partnership, LLC with oversight by the Department's Carlsbad Field Office. Its mission is to protect human health and the environment through safe management and disposal of certain transuranic wastes. WIPP is categorized as a Hazard Category 2 Nonreactor Nuclear Facility because it has the potential for significant radiological consequences. To provide protection against such consequences, WIPP utilizes Safety Class/Safety Significant systems and components in its

infrastructure and equipment. These items are designed to provide protection against radioactive exposure to the public and safety to the worker.

WIPP's management and operating contract requires compliance with the Department Order 414.1D, *Quality Assurance*, and that WIPP develop and conduct work in accordance with a Department approved quality assurance plan. In addition, WIPP's contract requires the implementation and maintenance of a quality assurance program in accordance with the provisions of 40 Code of Federal Regulations Part 194. These regulations require WIPP's quality assurance plan to comply with the *American Society of Mechanical Engineers Quality Assurance Program* requirements for Nuclear Facilities, 1989 edition. At WIPP, these requirements, based on a graded approach, apply to all Safety Class/Safety Significant items. The Carlsbad Field Office provides oversight to ensure proper implementation of quality assurance at WIPP.

Our review found that WIPP had not always effectively managed quality assurance requirements. Specifically, we found that WIPP did not always effectively:

- Perform commercial grade dedications of items relied on for safety. We found instances where WIPP did not effectively perform technical evaluations and/or the acceptance process, which are both key parts of an effective commercial grade dedication.
- Evaluate suppliers' abilities to meet quality assurance requirements prior to and after contract award.
- Identify the appropriate quality assurance requirements in contract documents.
- Maintain adequate document control of quality assurance documents.

Ineffective implementation of quality assurance requirements limits WIPP's ability to provide reasonable assurance of safe future operations. Further, problems associated with poor quality assurance can result in increased costs and future operational delays. Given WIPP's integral role in the Department's cleanup mission, it is imperative that quality assurance requirements are met in order to help eliminate future delays and additional costs to taxpayers.

The full report is available at: https://energy.gov/sites/prod/files/2017/09/f36/DOE-OIG-17-07.pdf

Washington River Protection Solutions Agrees to Pay $5.275 Million to Settle False Overtime and Premium Pay Allegations
January 23, 2017 Department of Justice Press Release

Washington River Protection Solutions LLC (WRPS) has agreed to pay the United States $5.275 million to settle allegations that WRPS knowingly submitted false claims to the Department for overtime and premium pay and also failed to comply with the contract's internal audit requirements.

Since 2008, WRPS has received millions of dollars from a prime contract with the Department to perform environmental cleanup and maintenance efforts at an area of the Department's Hanford Nuclear Site known as the Tank Farms. The Tank Farms is a large area of the Hanford Site

consisting of underground storage tanks that contain radioactive and hazardous waste from nuclear weapons production. The government alleged that, upon being awarded the Tank Farms contract in 2008, WRPS was advised by law enforcement of specific concerns about systemic timecard fraud being committed by the previous contract at the Tank Farms, many of whose employees and procedures were retained by WRPS. WRPS allegedly made no actual changes to the timekeeping procedures at the Tank Farms for nearly five years and did not take steps, until after July 2013, to curtail the prior fraudulent practices. As a result, the government alleged that WRPS knowingly charged the Department for overtime for busy work or for work that was not actually performed and premium emergency call-in pay that was not authorized by the Tank Farms Contract.

The government also alleged that WRPS charged the government for auditing work that was not performed. WRPS allegedly installed as the head of the contractually required Internal Audit Department for the first three years of the Tank Farms contract its own general counsel, who allegedly had no auditing experience and failed to provide any meaningful oversight of the Audit Department. The government alleged that this knowing violation of an important safeguard in the contract enabled the extensive timecard fraud.

The claims resolved by the settlement are allegations only; there has been no determination of liability.

The full press release is available at: https://energy.gov/sites/prod/files/2017/01/f34/WRPS FCA Settlement AAG Approved.pdf

Subcontract Management

As previously noted, the Office of Acquisition Management indicated that the Department's management and operating contractors reported $354 million in subcontracts during FY 2017. Many of the contractual provisions that are included in management and operating contracts are required to be flowed down into any subcontracts. However, as discussed under several of the examples in the prior section of this report on Contract Management, the Department and its contractors had not always provided adequate oversight of subcontracts. For example, as detailed below, Washington Closure Hanford, LLC (WCH) was required to flow down quality assurance requirements, specific to the scope of work, in its subcontracts and evaluate the subcontractors' capability of implementing the applied requirements. However, we identified weaknesses in how WCH flowed down quality assurance requirements and in the subsequent evaluations used to determine subcontractors' capability to implement a quality assurance program.

Additionally, during the past year, the OIG has investigated issues of contract fraud, especially in the area of procurement, and has received complaints through the Hotline concerning hiring irregularities and time and attendance issues. Given that these issues extend to subcontractors and the importance of the Department's subcontracts, this area has been identified as a management challenge.

Quality Assurance for River Corridor Closure Contract Procurements
February 2017, OAI-M-17-05

During the Hanford Site's Plutonium production mission, the Department operated nine reactors and a large laboratory complex along the Columbia River. In 2005, the Department's Richland Operations Office awarded WCH a $2.9 billion contract to remediate nearly 220 square miles of the Hanford Site.

To ensure compliance with contract requirements and safe performance of work, the Department's Richland Operations Office included in WCH's contract the Department's order on *Quality Assurance*, which requires the use of an appropriate consensus quality assurance standard consistent with regulatory requirements. WCH adopted the *American Society of Mechanical Engineers - Quality Assurance Requirements for Nuclear Facility Applications (NQA-1)* as its consensus standard for its quality assurance program. Specific to procuring material and services, WCH was required to flow down quality assurance requirements specific to the scope of work in its subcontracts and to evaluate the subcontractor's capability of implementing the applied requirements. If the scope of work could affect nuclear safety or mission, WCH was required to flow down the appropriate requirements of NQA-1 in its subcontracts.

We found instances where WCH did not effectively manage quality assurance in its procurements. Specifically, we identified weaknesses in how WCH flowed down quality assurance requirements in its subcontracts and in the subsequent evaluations used to determine whether subcontractors had the capability to implement an NQA-1 quality assurance program. We also found that WCH did not ensure that staff augmentation contracts contained requirements to perform work under WCH's quality assurance program.

The weaknesses identified in WCH's quality assurance program can increase the risk that contractual requirements are not met and ultimately expose the Department to increased financial risk. Not imposing applicable NQA-1 requirements can result in conditions that require rework. In fact, in discussions with the Office of Standards and Quality Assurance, its review of the Department's Environmental Management Consolidated Business Center identified several contracts that did not have quality assurance requirements included in the procurement documents. The work had to be stopped because contractors were not allowed to execute Environmental Management funded work without an approved quality assurance program. Not identifying the appropriate quality assurance requirement can affect cost and schedule, as well as possibly require the submission of a request for equitable adjustment that includes the omitted requirements. On the other hand, imposing NQA-1 requirements for items and services not important to safety or mission can result in unnecessary expenditure of funds. In addition, inadequate supplier evaluations may increase the risk of awarding contracts to subcontractors that cannot perform to contract requirements.

The full report is available at https://energy.gov/sites/prod/files/2017/02/f34/OAI-M-17-05_0.pdf

Procurement of Parts and Materials for the Waste Treatment and Immobilization Plant at the Hanford Site
November 2015, DOE-OIG-16-03

One of the Department's largest cleanup challenges involves 56 million gallons of hazardous and highly radioactive waste stored in underground tanks at the Hanford Site, located in Southeastern Washington State. The Department's Office of River Protection manages the cleanup project. As part of this effort, Bechtel National Inc. (Bechtel) was contracted by the Department to complete the design and construction of WTP to treat and immobilize the majority of the waste in preparation for permanent disposal. Construction of WTP began in 2001, with the start of operations scheduled to occur in 2019 and with an estimated cost of $12.2 billion. In constructing WTP, Bechtel has done extensive business with a number of vendors and subcontractors, acquiring $4 billion in parts and materials through the end of fiscal year 2014. However, technical issues have led to construction delays for the project.

To support construction of WTP, Bechtel has procured approximately $4 billion in parts and materials through the end of FY 2014 and instituted steps to ensure that procured parts and materials meet specifications and requirements. To help ensure that parts were satisfactory, Bechtel developed several controls to include verification of vendor design submissions, review of the manufacturing or fabrication process, and receipt inspection and testing. Bechtel also developed procedures to identify and resolve the nonconforming items and recover the costs from vendors.

A key function of Bechtel's procurement process is to ensure that vendors and subcontractors deliver items that conform to the specifications in procurement orders. However, the Department and its contractor had not always effectively executed procurements and material management activities at the Department's Office of River Protection. Specifically, Bechtel did not always identify nonconforming items resulting from vendor errors in a timely manner, resolve issues with nonconforming items in a timely manner after they were identified, or recover the costs for resolving non conformances from vendors when the problems were the result of vendor errors.

These problems were caused by weaknesses in Bechtel's quality assurance program. In particular, although Bechtel had procedures in place to prevent or identify nonconforming items, they were not always performed effectively. Contributing to these weaknesses were Bechtel's failure to effectively implement corrective actions, a lack of timeliness for resolving non conformances, and inadequate Federal oversight over Bechtel's cost recovery processes for nonconforming items. Failure to have a time requirement and track the progress for resolving nonconformances reduces Bechtel's opportunity to recoup the costs of fixing these nonconformances from the vendors and subcontractors.

The full report is available at https://energy.gov/sites/prod/files/2015/11/f27/DOE-OIG-16-03.pdf

Energy & Process Corp. Agrees to Pay $4.6 Million for Alleged False Claims Regarding Defective Steel Rebar and Quality control Failures in Nuclear Waste Treatment Facility
April 24, 2017 Department of Justice Press Release

The Justice Department announced that Energy & Process Corporation (E&P) of Tucker, Georgia has agreed to pay $4.6 million to resolve the government's lawsuit filed under the False Claims act alleging that it knowingly failed to perform required quality assurance procedures and supplied defective steel reinforcing bars in connection with a contract to construct a Department nuclear waste treatment facility.

The lawsuit alleged that the Department paid E&P a premium to supply steel reinforcing bars that met stringent regulatory standards for the Mixed Oxide Fuel Fabrication and Reactor Irradiation Services facility in the Department's Savannah River site near Aiken, South Carolina, but that E&P failed to perform most of the necessary quality assurance measures, while falsely certifying that those requirements had been met. The lawsuit further alleged that one-third of the steel reinforcing bars supplied by E&P and used in the construction was found to be defective. E&P subsequently replaced some of the defective steel reinforcing bars. The $4.6 million to be paid by E&P to resolve the government's False Claims Act lawsuit is in addition to the replacement costs incurred by E&P.

The claims asserted against E&P are allegations only, and there has been no determination of liability.

The full press release is available at:
https://energy.gov/sites/prod/files/2017/05/f34/20170505113910088.pdf

Cybersecurity

The use of information technology by Federal agencies continues to evolve, resulting in greater opportunities for accessibility to Government information and resources. Specifically these advancements in technology have led to cybersecurity incidents becoming a prominent threat and are occurring at an increased frequency. According to the Office of Management and Budget (OMB), Federal agencies reported over 30,000 cyber incidents in FY 2016. Sixteen of these incidents met the threshold for a major incident, defined as any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Given the importance and sensitivity of the Department's activities, along with the vast array of data it processes and maintains, protecting cyber assets continues to be a crucial aspect of the Department's overall security posture.

Although the Department made progress in the area of cybersecurity during FY 2017, our annual review of the Unclassified Cybersecurity Program continued to identify deficiencies with the Department's management of the program. For instance, in our FY 2017 review of the Department's Unclassified Cybersecurity Program (DOE-OIG-18-01, October 2017), we noted that the Department had made progress remediating weaknesses identified in our FY 2016 evaluation, which resulted in the closure of 13 of 16 prior year deficiencies. However, issues

related to vulnerability management, system integrity of Web applications, and access controls continued to exist. Further, in March 2017, the OMB concluded that the Department failed to reach the Cybersecurity Cross-Agency Priority goals in the areas of Hardware Asset Management, Software Asset Management, Vulnerability Management, Secure Configuration Management, Unprivileged User Personal Identity Verification (PIV) Implementation, Privileged User PIV Implementation, and Anti-Phishing Defenses. As a result of these inherent risks and the sensitivity of much of the Department's work, Department management must continue to emphasize cybersecurity.

The following reports identified weaknesses in the Department's cybersecurity programs.

The Department of Energy's Unclassified Cybersecurity Program – 2017
October 2017, DOE-OIG-18-01

The *Federal Information Security Modernization Act of 2014* requires Federal agencies to develop, implement, and manage agency-wide information security programs. In addition, Federal agencies are required to provide acceptable levels of security for the information and systems that support their operations and assets. In our 2017 review of the Department of Energy's Unclassified Cybersecurity Program, we found that the Department, including the National Nuclear Security Administration (NNSA), had taken a number of actions over the past year to address previously identified weaknesses related to its cybersecurity program. In particular, programs and sites made progress remediating weaknesses identified in our FY 2016 evaluation, which resulted in the closure of 13 of 16 prior year weaknesses. For instance, the Department reduced the number of vulnerability management findings from nine in FY 2016 to five in FY 2017. While these actions were positive, our current evaluation found that the types of weaknesses identified in prior years, including issues related to vulnerability management, system integrity of Web applications, and access controls continue to exist.

The weaknesses identified occurred in part, because Department officials had not fully developed and/or implemented policies and procedures related to the issues identified in our report. For instance, similar to previous years, we found that current configuration and security patch management processes had not ensured that software remained up-to-date and secure. In addition, the Department had not always implemented effective performance monitoring and risk management programs. For example, we continued to identify concerns with the Department's implementation of plans of action and milestones and the effective use of corrective action plans to address identified weaknesses. We also noted that security testing at several locations reviewed was not fully supportive of an effective continuous monitoring cybersecurity program. The OIG has continuously recognized cybersecurity as a management challenge area for the Department, emphasizing the critical need to enhance the Department's overall security posture.

The full report is available at: https://energy.gov/sites/prod/files/2017/10/f37/DOE-OIG-18-01.pdf

The Office of Enterprise Assessments Testing Incident at the 2016 Department of Energy Cyber Conference
June 2017, OIG-SR-17-05

The Department's Office of Enterprise Assessments is responsible for conducting independent assessments on behalf of the Secretary and Deputy Secretary in the areas of nuclear and industrial safety and cyber and physical security. Within the Office of Enterprise Assessments, the Office of Cyber Assessments evaluates the effectiveness of cybersecurity policy throughout the Department, as well as program and site office performance as it relates to implementation of cybersecurity programs. Assessments can be announced or unannounced and typically include a programmatic cybersecurity policy review in conjunction with technical performance testing. Announced testing is coordinated with the organization being tested and conducted as part of a scheduled appraisal activity. Unannounced tests, also known as red team exercises, are conducted without informing the site but are required to include coordination with a trusted agent. Due to the potential operational impacts, assessments must be carefully and thoroughly conducted and coordinated.

The Office of the Chief Information Officer (OCIO) recently sponsored the Department's 2016 Cyber Conference, held at a non-Federal facility located in Atlanta, Georgia. During the conference, the Office of Cyber Assessments conducted an unannounced assessment related to the use of mobile device charging stations. Officials indicated that the purpose was to determine whether conference participants would connect government and/or personal devices to a charging station. Due to concerns raised by various Department officials related to the Office of Cyber Assessments' lack of coordination with the OCIO prior to the assessment, the OIG initiated a special inquiry to determine the facts and circumstances surrounding the assessment.

Our review of the cyber conference testing incident substantiated concerns that the assessment had not been appropriately coordinated with the OCIO. We also identified issues related to the resulting response by OCIO officials. Although they participated in planning the conference, we found that the Office of Cyber Assessments had not taken appropriate planning and coordination steps when conducting its security assessment during the Department's 2016 Cyber Conference. Specifically, we found that Office of Cyber Assessments officials placed two data collection devices disguised as charging stations outside the conference exhibit hall just prior to commencement of the conference, without coordination with any individual responsible for planning or hosting the conference. In addition, once discovered, OCIO officials may not have taken the appropriate steps in responding to the identification of the uncoordinated devices. While it was ultimately determined that the devices were not malicious, did not pose a risk to the conference attendees, and no data was collected during the conference, we are concerned about the lack of coordination among Department elements and the related OCIO response to the potential threat that such devices could have posed.

The full report is available at: https://energy.gov/ig/downloads/special-report-oig-sr-17-05

Management of Brookhaven National Laboratory's Cybersecurity Program
November 2016, DOE-OIG-17-02

Brookhaven National Laboratory (Brookhaven) is a multipurpose research institution funded primarily by the Department and operated by Brookhaven Science Associates. To support its research mission, Brookhaven makes extensive use of information technology resources for scientific and business computing related to high-speed network infrastructure, data management, and Web applications. As a management and operating contractor, Brookhaven is responsible for meeting various Federal cybersecurity requirements.

We found that Brookhaven had not implemented a fully effective cybersecurity program. We identified weaknesses related to vulnerability and configuration management, physical and logical access controls, security planning and assessments, and contingency planning and data retention. Specifically, we found that Brookhaven:

- Was not fully effective at implementing vulnerability and configuration management controls and processes.
- Had not always maintained adequate physical or logical access controls over its information and systems.
- Had not conducted security planning and assessment activities in accordance with Federal requirements.
- Had not developed adequate contingency planning procedures to ensure that it could recover essential functions in the event of a significant disruption.

The identified weaknesses occurred, in part, because Brookhaven officials had not fully implemented applicable requirements related to cybersecurity. Without improvements that fully implement cybersecurity policies and procedures, Brookhaven's information and systems will continue to be at a higher-than-necessary risk of compromise, loss, or modification. For instance, without an effective vulnerability management program and sufficient controls over its network traffic, Brookhaven increases its risk of malicious attacks that could allow attackers the ability to compromise systems and information. In addition, the lack of enforcement of logical and physical access controls increases the risk of unauthorized access to systems and information. Further, the weaknesses identified related to contingency planning may hinder Brookhaven's ability to complete essential mission functions in the event of a significant disruption.

The full report is available at https://www.energy.gov/sites/prod/files/2016/11/f34/DOE-OIG-17-02.pdf

Followup on Bonneville Power Administration's Cybersecurity Program
August 2017, DOE-OIG-17-06

The Bonneville Power Administration (Bonneville) was established in 1937 as a Federal nonprofit power marketing administration and provides approximately 28 percent of the electric power used across 300,000 square miles in the Pacific Northwest. With an overall budget of $4.3 billion, Bonneville utilizes numerous information systems to conduct business and

electricity-related operations, including financial and administrative systems. Prior reviews have identified weaknesses related to Bonneville's cybersecurity program. More recently, the OIG received two allegations – one that alleged Bonneville officials had required nearly all teams to stop patching its systems and another that officials did not ensure systems stayed up-to-date on security controls.

While we did not substantiate all information included in the allegations, we did identify various weaknesses related to vulnerability management similar to those included in the allegations. We did note that officials had not ensured all systems contained up-to-date security controls. While Bonneville made efforts to improve its cybersecurity program, we found that they had not implemented a fully effective cybersecurity program and continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. We also noted weaknesses related to risk management. In particular, Bonneville had not implemented effective risk management practices as part of its security planning process and had not fully implemented effective logical access controls. Further, a number of configuration management vulnerabilities existed on systems reviewed that weakened Bonneville's security posture and contingency planning and testing issues continued to exist.

The issues identified occurred, at least in part, because officials had not ensured that Federal and Bonneville requirements were updated and/or fully implemented. For instance, officials had not incorporated the most recent Federal requirements issued by the National Institute of Standards and Technology into policies and system security plans even though the requirements were issued more than three years prior to our review. In addition, even when policies existed related to access control, configuration management, and vulnerability management, Bonneville officials had not taken appropriate actions to ensure that the policies were fully implemented. Without improvements to its cybersecurity program, Bonneville's systems may continue to operate at a higher than necessary risk of compromise, loss, modification, and non-availability. For instance, the lack of remediation of certain vulnerabilities identified could have permitted an attacker or malicious user access to systems supporting business operations and other general support systems.

The full report is available at https://www.energy.gov/sites/prod/files/2017/08/f36/DOE-OIG-17-06_3.pdf

The Department of Energy's Implementation of Multifactor Authentication Capabilities
September 2017, DOE-OIG-17-08

The Department operates many types of information systems supporting mission related activities such as nuclear security, scientific research and development, and environmental management. Strengthening cybersecurity over its information technology environment is a significant challenge facing the Department. Federal requirements and industry best practices indicate that multifactor authentication is one of the most effective methods of safeguarding information systems. In its most basic form, authentication is the process of verifying the identity of a user prior to allowing access to an information system. While the most common method of authentication is username and password, multifactor authentication adds rigor to the

authentication process using two or more different authenticators such as hardware security tokens and PIV cards.

Federal requirements concerning multifactor authentication on Federal information systems, including those operated by contractors, have existed for many years. For instance, the OMB issued M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, in August 2005 which required Federal agencies to implement multifactor authentication, in the form of PIV cards, for logical and physical access to Federal facilities and information systems. More recently, in June 2015, OMB initiated a 30-day Cybersecurity Sprint initiative to further emphasize access controls over Federal information systems by directing that all privileged users and most standard users utilize PIV card credentials to access information systems by September 30, 2016.

The Department made progress towards fully implementing multifactor authentication in accordance with Federal requirements. Specifically, the Department recently invigorated its efforts to meet the demands of the OMB Cybersecurity Sprint; however, we found that additional effort was needed for access to technology resources to ensure that multifactor authentication, including the use of PIV cards, was fully implemented across the Department. Specifically, our review of 18 Federal information systems, including those systems operated by contractors, identified weaknesses related to ensuring adequate protections over access to network and application resources, and noted that information reported to OMB related to the Cybersecurity Sprint was not always consistent. Specifically, we found:

- Although requirements existed for more than 10 years, none of the locations reviewed had fully implemented multifactor authentication for secure access to information systems and resources.
- Federal and contractor locations tested had not always considered the applicability of multifactor authentication for software applications, including those that contained sensitive information such as personally identifiable information and personal health information.
- Information reported to OMB by the Department related to progress implementing the Cybersecurity Sprint was not consistent and did not portray an accurate accounting of its use of multifactor authentication.

The weaknesses identified occurred, in part, because officials had not fully planned for implementation of multifactor authentication on information systems. Department guidance and requirements related to multifactor authentication technologies also were not always communicated effectively. In particular, even though Federal requirements related to the use of multifactor authentication, including PIV cards, had existed for many years, we noted that the Department had not fully deployed its enterprise-wide identity, credential, and access management program to address multifactor authentication. Furthermore, the Department had yet to officially approve its multifactor authentication implementation plan in response to the OMB Cybersecurity Sprint.

The full report is available at https://energy.gov/sites/prod/files/2017/09/f37/DOE-OIG-17-08.pdf

Environmental Cleanup

The Department is responsible for addressing the nation's Cold War environmental legacy resulting from five decades of nuclear weapons production and government-sponsored nuclear energy research. The cleanup operation is the largest in the world and includes 107 sites across the country encompassing an area equal to the combined size of Rhode Island and Delaware. Fifty years of activities has produced unique and technically complex problems. Specifically, this legacy includes some of the world's most dangerous sites with large amounts of radioactive wastes, spent nuclear fuel, excess plutonium and uranium, thousands of contaminated facilities, and contaminated soil and groundwater.

Since 1989, the Department has spent over $164 billion to retrieve, treat, and dispose of nuclear and hazardous waste and has completed cleanup at 91 of the 107 sites. In the last 6 years alone, the Department has spent $35 billion, primarily to treat and dispose of nuclear and hazardous waste and construct capital asset projects to treat waste. Cleanup activities can last for decades and often require first-of-a-kind solutions. Characterization of legacy waste sites is performed in conjunction with planning and executing cleanup activities, such as deactivating and decommissioning facilities, removing hazardous materials, stabilizing waste streams to prevent additional environmental damage, and restoring the sites to conditions required by legal agreements.

Despite billions spent on environmental cleanup, the Department's environmental liability has roughly doubled from a low of $176 billion in FY 1997 to the FY 2016 estimate of $372 billion. The Department is responsible for 83%, of the Federal government's $447 billion FY 2016 reported environmental liability which is mostly related to nuclear waste cleanup. Half of the Department's environmental liability resides at the Hanford Site in Washington State and the Savannah River Site in South Carolina.

Our recent report on the management of the Department's West Valley Demonstration Project highlights some of the challenges faced by the Department in this area.

Department of Energy's West Valley Demonstration Project
April 2017, DOE-OIG-17-05

From 1966 to 1972, Nuclear Fuel Service, Inc. operated a commercial nuclear fuel reprocessing plant at the Western New York Nuclear Services Center near West Valley, New York. The plant was the first and only U.S. plant in history to commercially reprocess uranium and plutonium from spent nuclear fuel. Operations at the plant generated more than 600,000 gallons of liquid high-level waste, which was stored on-site in underground tanks. In 1980, Congress passed the *West Valley Demonstration Project Act*, which required the Department, in cooperation with the State of New York, to solidify high-level waste, develop containers suitable for permanent disposal of the high-level waste, transport the waste to a permanent Federal repository, dispose of low-level transuranic waste, and decontaminate and decommission the associated facilities and tanks.

The Department reported that it had developed suitable containers and solidified the high-level waste via vitrification by 2002, fulfilling its first two responsibilities under the *West Valley*

Demonstration Project Act. The Department then commenced interim activities for decontaminating and decommissioning the facilities and managing wastes until it issued its Record of Decision in 2010. In this Record of Decision, the Department settled on a phased approach to complete the remainder of cleanup actions at the site. Phase I decommissioning actions included near-term removal of some facilities. During Phase I, further characterization of site contamination and additional scientific studies would be completed to support Phase II decommissioning decisions. In June 2011, the Department awarded a $333 million, 6-year contract to CH2M Hill B&W West Valley LLC for the facility disposition portion of the Phase I work.

We identified several significant issues with the management of the West Valley cleanup effort. In particular, we found substantial weaknesses related to the Department's project and contract management that contributed to the inability to meet the major milestones established in the Phase -I Facility Disposition contract. Specifically, we found that:

- Although the West Valley Phase I activities had been underway since 2011 and had incurred costs of $264 million by October 2015, the project was not administered using basic project management principles.
- The Department had omitted or had not explicitly described critical activities from the Phase - I contractor's original scope. As of November 2015, the contract value had increased by $196 million as a result of differing site conditions and inaccurate scope.

These conditions occurred, in part, because the Department had not ensured that project management policies and procedures were followed. Despite the requirements established in OMB's *Capital Programming Guide*, Department Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, and *Environmental Management's Portfolio Management Framework*, the site did not manage the West Valley decontamination and decommissioning work as a capital project. Additionally, Environmental Management had not ensured that site personnel had the appropriate skill level to manage the complex characterization and remediation work at West Valley or that its streamlined procurement efforts captured the scope of work to be performed when it solicited the contract.

After the Department fulfils its requirements at West Valley, it plans to return the site to its owner, the State of New York. However, with no baseline and no effective strategy for managing the work, neither the Office of Environmental Management nor the Department can realistically estimate resource needs or inform Congress of the true project cost to complete the West Valley cleanup effort. As a result, the West Valley cleanup project will likely continue to experience escalating costs and schedule delays, particularly in light of project risks involving radioactive contamination at the site, waste uncertainties, and deteriorating facility infrastructure.

The full report is available at: https://energy.gov/sites/prod/files/2017/04/f34/DOE-OIG-17-05.pdf

Nuclear Waste Disposal

The Department is responsible for safely disposing of nuclear waste and seeks cost effective and environmentally responsible project execution methods. The Department's waste management mission involves planning and optimizing tank waste processing and nuclear materials, including spent nuclear fuel. Overall, the Department has approximately 88 million gallons of liquid waste stored in underground tanks and approximately 4,000 cubic meters of solid waste derived from the liquids stored in bins. The Department's current estimated cost for retrieval, treatment, and disposal of this waste exceeds $50 billion. The highly radioactive portion of this waste, located at the Hanford Site, Idaho National Laboratory, and Savannah River sites, must be treated and immobilized, and prepared for shipment to a waste repository.

To accomplish its mission, the Department operates several waste processing and storage facilities. One such facility is the WIPP located near Carlsbad, New Mexico. The Department suspended operations at WIPP in February 2014 as a result of an accidental radiological release. As the Nation's sole repository for the disposal of transuranic waste generated by atomic energy defense activities, the closure of WIPP affected transuranic waste operations across the Nation. While the Department's initial Recovery Plan slated operations to resume in the first quarter of calendar year 2016, this date was pushed back several times, and WIPP did not resume operations until January 2017.

In addition, the Department is currently in the process of designing and building WTP. When complete, WTP will be the world's largest radioactive waste treatment plant. Its mission is to process and stabilize 56 million gallons of radioactive and chemical waste currently stored at the Hanford Site. However, the Department has faced significant technical challenges in successfully constructing and operating WTP. In December 2016, the Department increased the cost estimate for WTP by approximately $4.5 billion and extended the completion date.

As noted in our report regarding WTP and WIPP, the Department continues to face challenges with disposing of nuclear waste.

Corrective Action Program at the Waste Treatment and Immobilization Plant
February 2016, OAI-M-16-06

Bechtel, the contractor responsible for the design, construction, and commission of the WTP, is responsible for establishing and implementing effective programs for reporting and resolving safety and quality problems. These are essential elements in creating a safety conscious work environment. According to Bechtel's Corrective Action Management Program, the *Integrated Issues Management Policy* establishes the Corrective Action Management Program as the primary issues management program for documenting and resolving conditions adverse to quality identified at the WTP. The program is used to manage adverse conditions, technical issues, as well as other issues, recommendations, and suggestions for improvement. The program also provides a mechanism to document issues and initiate the process for evaluating, correcting, and verifying resolution of issues. A condition report is generated to document issues in the corrective action program, which is managed through a graded process based on the

significance of the issue. An effective corrective action program promotes prompt identification of issues and appropriate evaluation, tracking, trending, and correction in a timely manner.

Our audit found that the WTP corrective action program was not fully effective in managing and resolving issues. Specifically, we discovered that in some instances, issues were not managed and tracked in the corrective action program, as required. For example, several significant technical issues related to Inadequate Design of Mixing System were managed outside of the corrective action program and were closed before the overall issue was resolved. Inadequate performance of mixing systems at WTP could lead to nuclear criticality accidents, explosions of flammable gases, and mechanical failures of process vessel components. We also noted that corrective actions had not been implemented in a timely manner and that Bechtel failed to follow through on implementing prior corrective action program improvement initiatives.

Weaknesses with Bechtel's corrective action program have been reported for years. Although Bechtel has acknowledged these weaknesses and developed multiple improvement plans, in several cases initiatives were not fully implemented or sustained. Construction of the $12.3 billion WTP is an extremely complex project posing numerous technical challenges. Accordingly, an effective corrective action program is essential to ensure that important quality and safety issues are resolved in a timely manner.

The full report is available at: https://www.energy.gov/sites/prod/files/2016/02/f29/OAI-M-16-06.pdf

Safeguards and Security

Safeguards and Security programs are an essential part of the Department's ability to efficiently and effectively meet all its obligations to protect Special Nuclear Material, other nuclear materials, classified matter, sensitive information, government property, and ensure the safety and security of employees, contractors, and the general public. Safeguards and Security Programs are required to incorporate a risk-based approach to protect assets and activities against the consequences of attempted theft, diversion, terrorist attack, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security or the environment. In addition, these programs are designed to protect against activities that may pose significant danger to the health and safety of Department Federal and contractor employees or the public.

In addition to the reports summarized below, entities within and outside the Department have identified challenges associated with Safeguards and Security. For example, the Defense Nuclear Facilities Safety Board and the NNSA Office of Safety and Health identified management weaknesses in the Pantex Plant Emergency Management Program. These weaknesses included, but were not limited to training, drills, and exercises that had not always been adequately planned, conducted, or completed timely. Further, program self-assessments had not always identified program weaknesses. In addition, the Office of Enterprise Assessments issued its *2016 Best Practices and Lessons Learned* report in June 2017, which found weaknesses in Emergency Response Performance and Emergency Preparedness. Some of the issues identified by the Office of Enterprise Assessments included:

- Inability to demonstrate situational awareness due to poor communications;
- Inadequate use of information management tools;
- Responders not referring to procedures;
- Response procedures not available, accurate, or complete, at all times; and
- Inadequate corrective action implementation which resulted in recurring issues and delays in program improvement.

In a separate report, *Assessment of Work Planning and Control at the Lawrence Livermore National Laboratory*, the Office of Enterprise Assessments found instances in which hazard controls of a Hazard Control Plan were confusing or conflicting, or could not be followed as documented in the Plan.

Safeguards and Security remains an area of focus for the Department, as evidenced by our recent reviews on Tesa Access Issues at Lawrence Livermore National Laboratory (Livermore) and Security and Safety Concerns at Oak Ridge National Laboratory (ORNL).

Alleged Tesa Access Issues at Lawrence Livermore National Laboratory
July 2017, OAI-M-17-09

The OIG received an allegation that Livermore's Tesa database contained outdated and incorrect data and that this constituted a serious security issue. Specifically, it was alleged that an employee's Tesa locking plan included numerous Tesa locks for which the employee did not have a current need, could not access, or could not locate. Tesa locks are electro-mechanical locks that are accessed by inserting a Tesa-encoded card into the lock. Tesa locks can be attached to internal and external doors, or lockboxes to a classified network. A personalized pin may also be required to access certain Tesa locks.

We substantiated the allegation that Livermore's Tesa database contained incorrect data. Of the 63 locks on the employee's locking plan, we found that 44 of the Tesa locks had no current mission-related need, 5 Tesa locks were erroneously given to the employee, and 1 Tesa lock that had been removed from service. Additionally, 13 locks on the employee's locking plan for Tesa lockbox's related to a classified network account. Further, we found that for 23 of the 85 Livermore employees included in a judgmental sample, information stored in the Tesa database had not been updated in a timely manner or in accordance with Livermore's *Locks, Keys, and Tesa Policy and Procedures*.

The Tesa database contained outdated and incorrect data because Livermore did not always accurately maintain its employee's Tesa locking plans within its area of responsibility. The non-mission-related Tesa locks on the employee's locking plan, and the additional Tesa databased issues existed because Livermore did not always have adequate controls in place to ensure that Tesa locks were removed from the employee's locking plans when the mission-related need ceased. By not adhering to Livermore's *Locks, Keys, and Tesa Policy and Procedures*,

Livermore may not be able to provide reasonable assurance that sensitive information and other valuable assets are fully protected.

The full report is available at https://www.energy.gov/sites/prod/files/2017/07/f35/OAI-M-17-09.pdf

Alleged Security and Safety Concerns at the Oak Ridge National Laboratory
April 2017, OAI-L-17-05

ORNL is the Department's largest science and energy laboratory and operates in an open campus environment to encourage collaboration and the sharing of knowledge. ORNL is also subject to additional security requirements because it is home to Building 3019, a facility that stores Special Nuclear Material. The OIG received a complaint involving perceived security concerns at Building 3019 and safety and security concerns at a vehicle entry portal on the ORNL site.

We substantiated that some of the situations described by the complainant did exist, as alleged. We noted however, that these situations were aligned with procedures and strategies approved by cognizant managers, and Federal officials were aware of the practices employed at the site. During our review, we also identified other concerns related to vehicle searches at the site's entry portals and the secondary response force.

While observing search procedures at ORNL's entry portal, we identified two instances where the search was not conducted in accordance with established requirements. In both cases, the protective force's security officer was unable to access the interior of sealed shipping containers, and failed to compare numbered seals on the containers to previously approved lists of seals from authorized shipments. Instead, we observed that the officer instructed the driver to continue onto the site without fully completing the search. These numbered seals, when properly affixed to the containers before shipping, provide reasonable assurance that cargo has not been tampered with in transit. A senior protective force official concurred with our conclusions after viewing the related security video, and promptly issued clarification of procedures to be followed in such cases, including verifying seal numbers against approved lists. Further, site officials developed official policy on this matter and agreed to coordinate with protective force management to prevent future occurrences.

The full report is available at https://www.energy.gov/sites/prod/files/2017/04/f34/OAI-L-17-05.pdf

Stockpile Stewardship

The Department and NNSA are responsible for enhancing national security through the military application of nuclear science. NNSA maintains and enhances the safety, security, and effectiveness of the Nation's nuclear weapons stockpile without nuclear testing. NNSA's stockpile surveillance program continuously assess and evaluates each nuclear weapon system to detect or anticipate any potential problems. NNSA's mission is supported by three crosscutting capabilities: science, technology, and engineering; people and infrastructure; and management and operations. These capabilities are spread across the NNSA nuclear security enterprise at

Headquarters, the field offices, production facilities, national security laboratories, and a national security site. These locations consist of more than 1,500 Federal employees and 35,000 contractor personnel, as well as assigned members of the military.

While the Department indicated that substantial progress on priorities, including life extension programs, had been made, continued investment is required to ensure the stockpile remains safe, secure, and effective. The nuclear weapons stockpile is aging and contains many obsolete technologies that must be replaced as the service lives of the weapons are extended. Further, NNSA's mission depends on the facilities, infrastructure, and equipment for success. Yet the current demands of the stockpile stewardship program have placed increasing loads on an aging NNSA infrastructure.

As noted in our reports on the Department's Heavy Water Inventory and NNSA's Weapons Evaluation Test Laboratory (WETL), stockpile stewardship remains an area of emphasis for the Department.

Followup Audit of the Department's Heavy Water Inventory
December 2016, OAI-M-17-03

The Department and NNSA's inventory of heavy water is a vital national security asset. Heavy water, primarily managed and stored at the Y-12 National Security Complex (Y-12), is used in NNSA Weapons Activities to produce parts for weapons system life extension programs and to support National Ignition Facility nuclear weapon design and simulation missions. Additional heavy water inventories are located at ORNL, used primarily for non-Weapons Activities such as Spallation Neutron Source research and development, and at the Savannah River Site, which maintains an inventory unusable for current programs and planned for future disposal.

We determined that, while the Department had taken several actions to address heavy water requirements to meet mission needs through FY 2031, management of the heavy water inventory may not ensure a sufficient supply for Weapons Activities beyond that time. Specifically, we found that the Department's current inventory of usable heavy water is its only source of material for Weapons Activities. The United States has not had a heavy water production capability since 1996, and there are no current plans to construct a capability. According to Y-12 documentation, the establishment of a new production capability would require a rough estimated lead time of 10-15 years.

According to Department officials, actions to address Weapons Activities heavy water requirements after FY 2031 were not taken because, based on Nuclear Materials Management forecasts developed in 2012, when Y-12 fully implemented the Direct Materials Manufacturing process, the Department determined that the heavy water inventory was adequate to meet program requirements through FY 2031 and beyond, which would afford sufficient time to prepare plans to meet needs beyond that date. Thus, the Department did not have any concerns regarding the long-term availability of heavy water. As such, the Department had not established a point, such as an inventory level or other trigger point, when it would begin to pursue other options for acquiring heavy water for Weapons Activities. However, given the uncertainty of heavy water requirements beyond 2031, the long lead time to establish a production capability, and the estimated lead time to develop recycle or re-enrichment capabilities, the Department may

be at risk of being unable to meet all of its Weapons Activities heavy water requirements in the long term.

The full report is available at: https://energy.gov/sites/prod/files/2016/12/f34/Audit Report OAI-M-17-03.pdf

The National Nuclear Security Administration's Weapons Evaluation Test Laboratory
January 2017, OAI-M-17-04

The primary mission of the Department's NNSA is to ensure the safety, reliability, and performance of the Nation's nuclear weapons stockpile. NNSA's stockpile surveillance program continuously assess and evaluates each nuclear weapon system to detect or anticipate any potential problems. Sandia National Laboratories' (Sandia) WETL, located at the Pantex Plant in Amarillo, Texas supports the execution of the stockpile surveillance program by testing weapon functionality and providing quality data to support NNSA's annual stockpile assessments. Specifically, WETL performs laboratory testing using centrifuges and other test equipment. The non-nuclear components are mounted on a centrifuge and exposed to environments that simulate the launch and reentry conditions.

In December 2013, the OIG received an anonymous complaint regarding the management of Sandia's Integrated Stockpile Evaluation Group. The complaint alleged that Sandia diverted equipment to other programs and failed to fund preventative maintenance for WETL. While we did not substantiate the allegation that Sandia diverted equipment to other programs, we did find that Sandia had not met NNSA's expectations for laboratory testing at WETL. Our review disclosed that Sandia experienced delays in executing baselined laboratory tests. In particular, we determined that Sandia had not completed all baselined tests for four of the eight weapons systems. The testing delays were due primarily to significant unplanned downtime of WETL testing equipment in FYs 2014 and 2015. Specifically, one of WETL's large centrifuges was inoperable due to noise and vibration issues, followed by an unrelated fire in the drive system. This large centrifuge was not used for testing for nearly 2 years.

The efficient execution of WETL laboratory tests is critical to identifying stockpile defects in a timely manner to maintain a safe, secure, and reliable nuclear weapons stockpile. Although Sandia anticipates that it will eliminate the WETL test backlog by April 2017, because of the age and uniqueness of the centrifuges, we believe there is an increased risk of further operational delays and unplanned equipment outages.

The full report is available at: https://energy.gov/sites/prod/files/2017/01/f34/OAI-M-17-04.pdf

Infrastructure Modernization

The Department is responsible for a vast portfolio of infrastructure that consists of world-leading scientific and production tools, as well as the general purpose infrastructure needed to enable the use of those tools. As of November 2016, the Department had the fourth largest inventory of real property in the Federal government by square footage, including 10,095 buildings totaling 119 million square feet (owned and leased) with approximately $2 billion in annual operating

and maintenance costs. Modern and reliable infrastructure is critical to support the Department in successfully and efficiently executing its missions both today and in the years ahead. According to the Department of Defense's April 2010 Nuclear Posture Review Report, in order to remain safe, secure, and effective, the U.S. nuclear stockpile must be supported by a modern physical infrastructure comprised of the national security laboratories and a complex of supporting facilities. However, the average age of the Department's facilities is 36 years and its utilities is 39 years.

Specifically, while the Department made significant investments in world class experimental facilities, much of the supporting infrastructure that enables the mission and forms the backbone of the Department enterprise is in need of greater attention. Facilities and infrastructure can have a substantial impact on laboratory research and operations in a variety of ways. Laboratory facilities and infrastructure in poor condition can have inadequate functionality on mission performance; negative effects on the environment, safety, and health of the site; higher maintenance costs; and problems with recruiting and retaining high-quality scientists and engineers. Based on Department-wide facility assessments and data analyses, the Department is facing a systemic challenge of degrading infrastructure and levels of deferred maintenance that have been increasing. In fact, the November 2016 *The State of General Purpose Infrastructure at the Department of Energy* report indicated that 50% of the Department's assessed, owned and active buildings, trailers, and other structures and facilities were considered functionally adequate to meet the mission, while 33% were considered substandard and 17% were considered inadequate.

Our audit report summarized below illustrates the tremendous challenge facing the Department in the area of infrastructure modernization.

Enriched Uranium Operations at the Y-12 National Security Complex
July 2016, DOE-OIG-16-13

Y-12 performs critical elements of NNSA's mission to ensure the safety, reliability, and performance of the Nation's nuclear weapons deterrent. Specifically, Y-12 processes enriched uranium for NNSA's Defense Programs, such as weapons life extension programs and maintains the Nation's strategic reserve of enriched uranium. Y-12's enriched uranium processing capability is housed in multiple facilities: building 9212 and its related facilities, collectively known as the 9212 complex, and building 9215 and its associated facilities, known as the 9215 complex. The structures were built decades ago and do not meet modern nuclear facility design requirements. Production equipment has also aged and experienced maintenance and reliability issues.

Due to the condition of the buildings and equipment, serious concerns about the future reliability of the facilities have been raised by NNSA and the Defense Nuclear Facilities Safety Board. As a result, NNSA originally planned to construct the Uranium Processing Facility to house all enriched uranium operations at Y-12. The Uranium Processing Facility was planned to be operational in 2018; however, Y-12 reported that full operations are now not likely to occur until 2025, and the Uranium Processing Facility will not replace all of the capabilities currently housed in the 9212 complex. The remaining needed operational capability is planned to be located in existing facilities designated as bridging or enduring facilities. We performed this

audit to determine whether current enriched uranium operations facilities at Y-12 will meet NNSA mission needs until new facilities are available. In particular, we focused our audit on the 9212 and 9215 facilities.

During our audit, we found that Y-12 may not be able to continue to meet NNSA mission needs in its existing, aging facilities. We found that at 70 years old, the 9212 complex has reached the end of its life. Although Y-12 recently completed critical upgrades to the 9212 complex to reduce risk through 2021, critical operations at the facility are now projected to continue through 2025. Additionally, Y-12 plans to move some 9212 complex operations into the 9215 complex, which is also old and in need of upgrades. Y-12 initially planned to conduct enriched uranium operations in the 9215 complex through 2030, but a recent long-term strategy identified continued operations into the 2030s; however, this strategy has not been planned or funded. Regarding maintenance, both the 9212 and 9515 complexes have significant and steadily increasing deferred maintenance. Deferred amounts continued to increase due to competing budget priorities and because Y-12 did not request funding for all identified maintenance work.

We noted that not all potential significant risks were fully addressed by NNSA and Y-12. In particular, if the gap between Y-12's mitigating actions and transition of operations from the 9212 complex to the Uranium Processing Facility is not addressed, there is a potential risk that a maintenance event may significantly affect production or that a safety event could endanger personnel. Further, these risks also exist while operations continue in the 9215 complex. Thus, failure to take action could affect Y-12's ability to meet mission requirements.

The full report is available at https://www.energy.gov/sites/prod/files/2016/07/f33/DOE-OIG-16-13.pdf

Watch List Items

Annually, the OIG also prepares a Watch List to accompany the Management Challenges listing. These areas identified incorporate issues that at the current time do not meet the threshold of a management challenge; however in our view, warrant special attention by Department officials.

Department's Employee Concerns Program

The Department's Employee Concerns program provides Department federal, contractor, and subcontractor employees with an independent avenue to raise any concern related, but not limited, to the environment, safety, health, and management. The Employee Concerns Program is designed to encourage open communication and ensure employees can raise issues without fear of reprisal. Free and open expression of employee concerns is essential to safe and efficient accomplishment of the Department's mission. However, the OIG is concerned about the rigor of the Employee Concerns Program. Specifically, the OIG has become concerned that contractors are not adequately addressing employee's concerns and may be suppressing complaints. Citing an investigation report issued by the OIG in 2017, the Department found that a contractor, Savannah River Nuclear Solutions, retaliated against the complainant when it fired that person following that person's disclosure of information to the Government Accountability Office. The Department ordered Savannah River Nuclear Solutions to reinstate the complainant, pay the complainant back pay, and reimburse the complainant for their expenses. For these reasons, the Department's Employee Concerns Program has been added to the management challenges watch list.

Power Marketing Administrations

The Department's four Power Marketing Administrations sell electricity primarily generated by federally owned hydropower projects. Preference in the sale of power is given to public entities and electric cooperatives. Revenues from the sale of Federal power and transmission services are used to repay all related power costs. However, the Department has experienced challenges in overseeing the Power Marketing Administrations. Based on our in-process work at the Power Marketing Administrations, there have been indicators of potential fraud, waste, and abuse in certain circumstances. For these reasons, the Power Marketing Administrations have been added to the management challenges watch list.

Human Capital Management

Human Capital Management is responsible for the attraction, selection, training, assessment, and rewarding of employees. Human Capital Management impacts almost every aspect of an organization's activities and its effective implementation is critical to the organization's success. According to the 2016-2020 *Strategic Human Capital Plan*, over 35% of the Department's federal employees will be eligible to retire by 2020, including many of its most experienced and highly skilled professionals. Current budget uncertainties and long-term fiscal pressures, coupled with a potential wave of employee retirements could produce gaps in leadership and institutional knowledge that would threaten the Department's ability to meet its mission. Further, Department officials from the Office of Nuclear Energy, NNSA, and Office of the Chief

Human Capital Officer have all indicated that Human Capital Management is a workforce challenge. For these reasons, Human Capital Management is on this year's management challenges watch list.

Loan Guarantee Program

The Department's Loan Programs Office manages a portfolio comprising more than $30 billion of loans, loan guarantees and conditional commitments covering more than 30 projects. The Department operates two direct loan and loan guarantee programs; the Advanced Technology Vehicles Manufacturing Loan Program and the Title XVII Guarantee Program for Innovative Technologies. The Advanced Technology Vehicles Manufacturing Loan Program authorizes direct loans to support the development of advanced technology vehicles and associated components. The Title XVII Guarantee Program for Innovative Technologies Loan Program authorizes the Department to issue loan guarantees to eligible projects that avoid, reduce, or sequester air pollutants or anthropogenic emissions of greenhouse gases and employ new or significantly improved technologies. However, the Department has not always managed these loan guarantee programs effectively. For example, in FY 2016, the Department wrote off two loans worth over $74 million. In addition, in September 2017, the Department announced additional conditional commitments of up to $3.7 billion in loan guarantees for the construction of two reactors at the Vogtle Electric Generating Plant on top of the $8.3 billion in loan guarantees already provided for the construction. Construction of the reactors at the Vogtle Electric Generating Plant could be at risk due to the filing of Chapter 11 bankruptcy of one of the original construction contractors, Westinghouse, in March 2017. For these reasons, the Loan Guarantee Program is on this year's management challenges watch list.

Worker and Community Safety

The Department's worker and health and safety requirements, and expectations ensure protection of workers from the hazards associated with Department operations. The Department implements medical surveillance and screening programs for current and former workers and supports the Department of Labor in the implementation of the Energy Employees Occupational Illness Compensation Program Act. Health studies are conducted to determine worker and public health effects from exposure to hazardous materials associated with Department operations and supports international health studies and programs. Departmental worker health and safety programs and activities also serve to assist Department headquarters and field elements in implementation of policy and resolve worker safety and health issues. Because of the importance of Department employees, worker and community safety continues to be on the management challenges watch list.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.