OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

SPECIAL REPORT

OIG-SR-17-02 November 2016

MANAGEMENT CHALLENGES AT THE DEPARTMENT OF ENERGY – FISCAL YEAR 2017

Department of Energy
Washington, DC 20585

November 16, 2016

MEMORANDUM FOR THE SECRETARY

FROM: Rickey Hass
Acting Inspector General

SUBJECT: INFORMATION: Special Report on "Management Challenges at the Department of Energy – Fiscal Year 2017"

INTRODUCTION

The Department of Energy is responsible for some of the Nation's most complex and technologically advanced missions. These include cutting edge work in basic and applied sciences, clean energy innovation, energy efficiency and conservation, environmental cleanup, nuclear weapons stewardship, and efforts to enhance national security. To execute this diverse portfolio, the Department receives an annual appropriation of approximately $30 billion, employs approximately 108,000 Federal and contractor personnel, and manages assets valued at $182.8 billion, including 17 national research and development laboratories. The Office of Inspector General (OIG) annually identifies what it considers to be the most significant management challenges facing the Department. The OIG'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 (FY) 2017 challenge areas remain largely consistent with those in previous years, based on the results of our work over the last year, we have made one notable change. As a result, the FY 2017 management challenges include the following:

- Financial Assistance and Contract Management
- Cybersecurity
- Environmental Cleanup
- Nuclear Waste Disposal
- Safeguards and Security
- Stockpile Stewardship
- Infrastructure Modernization

The change to this year's report involves the addition of Financial Assistance Management to the management challenges list. Our recent reviews revealed Financial Assistance Management as a challenge for the Department. In one notable instance, we found that the Department had taken actions that increased its financial risk in the estimated $1.9 billion Texas Clean Energy Project, of which the Department's share of the project was $450 million. Given the large volume of financial assistance awards managed by the Department and the need for adequate oversight to protect the Department's investments, we have added Financial Assistance Management as a management challenge.

WATCH LIST

The OIG also prepares 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 FY 2017, the Watch List includes 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 OIG reports that informed our decision process. A complete list of reports can be found at http://energy.gov/ig/calendar-year-reports.

The management challenge 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
Administrator for the National Nuclear Security Administration
Under Secretary for Science and Energy
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Financial Officer
Chief Information Officer

Financial Assistance and Contract Management

The Department of Energy is the largest civilian contracting agency in the Federal Government and awards contracts, grants, and other financial assistance instruments to industrial companies, small businesses, academic institutions, and nonprofit organizations. Approximately 90 percent of the Department's budget is spent on contracts and large capital asset projects. In fiscal year (FY) 2015, the Department managed 11,337 contracts valued at more than $27 billion. Additionally, the Department reported more than $2.7 billion in financial assistance direct payments, including almost $1.5 billion in grants. The challenges associated with managing the Department's sizeable contracting portfolio have been recognized internally by the agency and the Office of Inspector General (OIG), as well as externally by the Government Accountability Office, which has included inadequate contract and project oversight on its High Risk List since 1990.

Acknowledging the Department's progress in this area, as of February 2013, the Government Accountability Office had narrowed the focus of the high risk designation to the Office of Environmental Management and National Nuclear Security Administration (NNSA) major contracts and projects that have an estimated cost of $750 million or more. Together, these two programs accounted for more than 60 percent of the Department's FY 2016 discretionary funding of nearly $30 billion. As recently as 2015, the Government Accountability Office found continuing cost and schedule problems with the Office of Environmental Management and NNSA major projects but noted that the Department's top leadership continued to be engaged and take action to address this high-risk area. 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 Financial Assistance and Contract Management is a significant management challenge.

The following OIG reports highlight the need for continued focus by the Department in financial assistance and contract management.

Management and Oversight of Information Technology Contracts at the Department of Energy's Hanford Site
April 2016, DOE-OIG-16-10

The Department's Hanford Site (Hanford) supported the Manhattan Project and Cold War through the production of plutonium. The weapons production processes resulted in the creation of solid and liquid wastes that posed a risk to the local environment. To help remediate the environmental risks, the Richland Operations Office and the Office of River Protection oversee the cleanup work completed by seven prime contractors. The Richland Operations Office designed Hanford's Mission Support Contract to provide integrated infrastructure services to the prime contractors performing the cleanup mission. A portion of the contract's scope included information technology (IT) support services related to application hosting services, support for hardware and software, network management, and desktop/user services.

The Office of Inspector General received a complaint expressing concerns with the Department's oversight of IT functions at Hanford. The complaint alleged, among other things, that Mission

Support Alliance, LLC's (MSA) request to subcontract to Lockheed Martin Services, Inc. (LMSI) had not been formally approved and that LMSI had refused to provide a breakdown of costs. The complainant further alleged that LMSI was likely receiving unallowable affiliate profit. Shortly after the audit began, Richland Operations Office officials stated that they had similar concerns regarding unallowable fee or profit and had made attempts to resolve the issue. The complaint also alleged a potential conflict of interest between MSA and LMSI. To that end, we initiated this audit to determine whether IT contracts and activities at Hanford were effectively managed.

Our review largely substantiated that there were a number of problems related to the management and oversight of the IT contracts at Hanford. While we did not substantiate the allegation regarding a conflict of interest, we determined that several MSA executives also held senior executive positions within Lockheed Martin Corporation and, as such, had inappropriately taken actions on excluded activities that resulted in the appearance of a conflict of interest. We identified weaknesses related to contract awards and work scope, time and material task orders, and affiliate fee or profit.

The identified weaknesses occurred, at least in part, because MSA had not fully executed the Mission Support Contract in accordance with its terms. We also observed that Richland Operations Office and MSA officials had not ensured that incurred cost audits were conducted in accordance with Federal requirements, a key component of an effective monitoring and oversight program.

In light of the issues identified, the Department may have awarded a contract that was not in the best interest of the Government. Specifically, the Department may have inappropriately paid up to $63.5 million in affiliate fee or profit. In addition, we questioned $120 million in time and materials costs pending resolution through incurred cost audits.

The full report is available at http://energy.gov/sites/prod/files/2016/04/f30/DOE-OIG-16-10.pdf

The Department of Energy's Continued Support of the Texas Clean Energy Project Under the Clean Coal Power Initiative
April 2016, OIG-SR-16-02

The Department's Clean Coal Power Initiative is a partnership with industry to demonstrate advanced coal-based technologies, with the goal of accelerating commercial deployment of promising technologies to ensure the nation has clean, reliable, and affordable electricity. In January 2010, the Department awarded a $1.7 billion cooperative agreement under the Initiative for the Texas Clean Energy Project (Project), which was estimated to cost $1.9 billion. The Department's share of the Project cost was $350 million, including approximately $216 million in *American Recovery and Reinvestment Act of 2009* (Recovery Act) funding. The Department later increased its commitment to $450 million. The remaining costs were to be provided by the awardee, Summit Texas Clean Energy LLC (Summit). The Project objective was to demonstrate the integration of a commercial power generation plant with carbon dioxide capture, transport, and geologic sequestration. The first phase of the Project was originally scheduled for

completion in December 2010, and would move into later phases of design and construction and operations upon Summit securing additional financing. We initiated this audit to determine whether the Department managed projects under the Initiative effectively and efficiently.

During our audit, we found that due to Summit's inability to obtain the required commercial debt and equity project financing and the adverse effect of changing energy markets on the demand for coal-based power plants, the viability of the Project and the Department's continued involvement is a concern. Without commercial debt and equity financing, Summit will be unable to contribute its share of costs and move forward with the Project. We also found that the Department had taken actions that increased its financial risk in the Project. Specifically, it accelerated disbursements of Recovery Act funds and allowed Summit to shift Project costs from the phase 2 design; resulting in higher reimbursements than were originally intended during the first phase. As of February 2016, the Project remained in the first phase and the Department had invested about $116 million in the Project without assurances that it would succeed.

The full report is available at http://energy.gov/sites/prod/files/2016/04/f30/OIG-SR-16-02.pdf

Cybersecurity

The use of IT by Federal agencies continues to evolve, resulting in greater opportunities for accessibility to Government information and resources. Given the importance and sensitivity of the Department's activities, along with the vast array of data it processes and maintains, cybersecurity is a crucial aspect of the Department's overall security posture. According to the Office of Management and Budget, Federal agencies reported more than 77,000 information security incidents in FY 2015, up 10 percent from FY 2014. The increasing number and impact of these incidents demonstrates that continuously confronting cyber threats must remain a strategic priority. While the usual attacks by hackers and criminals remain persistent challenges, threats are increasingly coming from state-sponsored military and intelligence organizations, terrorists groups, and international crime organizations. These evolving security concerns could lead to devastating consequences in the event of a cyber breach.

Although the Department has made progress, our annual reviews of the Department's Unclassified Cybersecurity Program continue to find deficiencies with the Department's management of the program. In our FY 2015 review, we noted that the Department had made significant progress in remediating weaknesses identified in our FY 2014 evaluation, which resulted in the closure of 22 of 26 reported deficiencies. However, we found that issues related to security reporting, vulnerability management, system integrity of Web applications, and account management continued to persist. Further, in March 2016, the Office of Management and Budget concluded that the Department failed to reach the Cybersecurity Cross-Agency Priority Goals in the areas of Information Security Continuous Monitoring, Strong Authentication, and Anti-Phishing and Malware Defense. As a result of the identification of continuing cybersecurity weaknesses 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 – 2015
November 2015, DOE-OIG-16-01

The *Federal Information Security Management Act of 2002* established the requirement for Federal agencies to develop, implement, and manage agency-wide information security programs. Federal agencies are also required to provide acceptable levels of security for the information and systems that support their operations and assets. The *Federal Information Security Modernization Act of 2014* modified the scope of agency reporting requirements to include specific information about security threats, incident reporting, and cyber breach notifications. In our 2015 review of the Department of Energy's Unclassified Cybersecurity Program, we found that the Department, including the NNSA, had taken a number of positive steps over the past year to address previously identified cybersecurity weaknesses related to the program. We noted that the Department had made significant progress in remediating weaknesses from the previous year, which resulted in the closure of 22 of 26 deficiencies. While these actions were positive, we also found that the types of deficiencies identified in prior years, such as issues related to security reporting, vulnerability management, systems integrity of Web applications, and account management continued to persist.

The weaknesses identified in our evaluation occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements. In addition, the Department had not always implemented an effective performance monitoring and risk management program. Without improvement to its cybersecurity program, such as adherence to policies and processes to ensure security controls are fully implemented, the systems with vulnerabilities identified will continue to be at a higher-than-necessary risk of compromise, loss, and/or modification. Furthermore, absent an effective process for tracking and implementing corrective actions, the Department may not adequately address cybersecurity risks or prioritize investments to ensure protection of data and information systems.

The full report is available at http://energy.gov/sites/prod/files/2016/02/f29/DOE-OIG-16-01_version2.pdf

The Department of Energy's Cybersecurity Risk Management Framework
November 2015, DOE-OIG-16-02

Cyber attacks on information systems have become aggressive, disciplined, well-organized, and very sophisticated. The threat environment also continues to change and become more complex. In response, the Department began transitioning several years ago from a compliance based information system certification and accreditation process to a cybersecurity risk management framework. This change was designed to allow the Department to more effectively manage the risks to its information systems and retain assurance that new risks are identified and mitigated in a timely manner. In FY 2015, the Department planned to spend at least $300 million on

cybersecurity activities designed to protect IT resources supporting its national security, energy, science, and environmental missions. We initiated this audit to determine whether the Department had effectively implemented its cybersecurity risk management framework.

During our audit, we found that the Department had made progress toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data. However, we found that additional effort is needed to ensure that operating system risks are identified and systems and information are adequately secured. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure they were effective. Further, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risk, weakness, and vulnerabilities to the information systems under their purview. The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented and the Department had not established sufficient oversight and communication to support its cybersecurity risk management program. While positive actions had been taken, without improvements to its cybersecurity risk management program, the Department cannot ensure that it has an ongoing understanding of the risks to its systems and to what extent those risks have been or can be mitigated. As a result, risk acceptance decisions may be based on inaccurate information and the Department's systems and information may be placed at an increased risk of compromise.

The full report is available at http://energy.gov/sites/prod/files/2015/11/f27/DOE-OIG-16-02.pdf

Environmental Cleanup

The Department is responsible for one of the most complex nuclear remediation efforts in the world. To meet this challenge, the Department is faced with developing unique solutions to address often unknown obstacles. As part of this mission, the Department is tasked with safely and cost-effectively transporting and disposing of low-level wastes, decommissioning and decontaminating old facilities, remediating contaminated soil and groundwater, and securing and storing nuclear material in stable, secure locations to protect national security. This includes disposing of multiple waste streams generated during more than 50 years of nuclear defense and energy research work.

For example, the Department has 177 large underground tanks at the Hanford Site in southeastern Washington containing 56 million gallons of radioactive and chemical waste. Of these, more than one-third have already leaked, contaminating the subsurface and threatening the nearby Columbia River. The Hanford Tank Waste Treatment and Immobilization Plant is currently being constructed to process and stabilize the waste stored at the site. However, the Department faces significant technical challenges in successfully constructing and operating the Waste Treatment and Immobilization Plant, and the estimated cost of the project has tripled, while the scheduled completion date has slipped by nearly a decade. In another example, we found that the Department had delayed the planned start of operations at the recently constructed Integrated Waste Treatment Unit, the Sodium-Bearing Waste Treatment Facility (SBWTF) at the Idaho National Laboratory, a number of times due to cost and schedule issues. In September 2016, the Department announced that it was unlikely to meet the deadline for the start of waste

treatment at the Integrated Waste Treatment Unit. The Department's Environmental Cleanup efforts are projected to cost at least $340 billion and will continue well into the foreseeable future. As such, this remains a management challenge that warrants attention on the part of Department management.

Our recent report on the management of the startup of the SBWTF highlighted some of the challenges faced by the Department in this area.

Management of the Startup of the Sodium-Bearing Waste Treatment Facility
March 2016, DOE-OIG-16-09

Under its contract for the Idaho Cleanup Project, CH2M-WG Idaho LLC was to design, construct, and operate the SBWTF to treat 900,000 gallons of radioactive liquid waste that is currently stored in underground waste tanks at the Idaho National Laboratory. The 1995 Settlement Agreement required the Department to complete processing of the sodium-bearing waste by December 31, 2012. Following treatment, as required by the *Resource Conservation and Recovery Act*, the waste tanks were to be removed from service by December 2014. However, the project had cost and schedule issues, leading the Department's Idaho Operations Office to delay the planned start of operations a number of times. In December 2010, to address cost overruns, the Department implemented a contract modification where it placed a cost cap of $571 million for the construction of the facility. Any construction costs above that amount were to be borne by the contractor. Operating costs are fully reimbursable, are not subject to the cost cap, and begin after construction is complete.

In April 2012, the Department declared construction complete, beginning the project's operation phase, and in June 2012, CH2M-WG Idaho LLC initiated comprehensive performance testing, which involved operating the plant at high temperature with a nonradioactive simulant to prove full performance of the facility. On June 16, 2012, during testing, the facility experienced a "system pressure event" which led to the shutdown of the facility. The Department's investigation into the event revealed both operational and design deficiencies and the facility has been shut down since the event for modifications and repairs to the facility and process. We initiated this audit to determine whether the Department effectively managed the startup of the SBWTF.

Our audit revealed significant problems with the Department's management of the startup of the SBWTF. In particular, we found that the Department moved the work associated with the comprehensive performance test, which demonstrates that the facility would perform its mission as designed, from the construction phase of the project to the operations phase of the project. Additionally, we identified a weakness in Department Order 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, which does not specifically require that comprehensive performance testing occur during the construction phase. Finally, the Department based its declaration of project completeness on Operational Readiness Reviews

without the benefit of robust design reviews and thorough acceptance and startup testing using materials that simulate, to the greatest extent possible, the waste or other materials to be processed in the actual facility prior to the readiness reviews.

In light of the issues we identified, we concluded that the Department's cost cap did not successfully limit the construction costs borne by the taxpayers and the total actual construction cost for this facility is likely understated by about $181 million thus far. Based on expenditures of $4 million per month, the future costs could exceed $40 million by the planned startup date of September 2016. Recasting these "operations costs" as construction costs would breach the approved limit of $571 million.

The full report is available at http://energy.gov/sites/prod/files/2016/04/f30/DOE-OIG-16-09.pdf

Nuclear Waste Disposal

The Department is responsible for the management and safe disposal of nuclear waste. 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 highly radioactive portion of this waste, located at the Hanford Site, Idaho National Laboratory, and Savannah River Site, must be treated and immobilized. The Department estimates that retrieval, treatment, and disposal of this waste will exceed $50 billion over several decades.

The Department operates several waste processing and storage facilities. In addition to the challenges noted above at the Waste Treatment and Immobilization Plant and the SBWTF, the Department continues to experience delays in re-opening the Waste Isolation Pilot Plant, located near Carlsbad, New Mexico. The Department suspended operations at the Waste Isolation Pilot Plant 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 the Waste Isolation Pilot Plant has affected transuranic waste operations across the Nation. For example, in September 2016, the Department notified the State of South Carolina, where the Savannah River Site is located, that there is no plan for shipping transuranic waste out of South Carolina through the end of July 2017. Legacy transuranic waste inventory is located at 4 large-quantity sites and more than 20 small-quantity sites across the United States.

While the Department's initial Recovery Plan slated operations to resume in the first quarter of calendar year 2016, this date has been pushed back several times, and the Waste Isolation Pilot Plant is not expected to resume operations until at least December 2016. Often part of cleanup agreements, nuclear waste disposition is of interest to stakeholders and requires the oversight of regulators. Given the importance of a coherent strategy on nuclear waste disposal that protects public health, safety, and the environment, the area of Nuclear Waste Disposal remains a significant challenge facing the Department.

As noted in our report regarding allegations at Sandia National Laboratories (SNL), the Department continued to face obstacles disposing of nuclear waste.

Allegations Regarding the Sandia National Laboratories Mixed Waste Landfill
February 2016, OAI-SR-16-01

The Department's SNL is a Government-owned, contractor-operated laboratory that is part of NNSA nuclear weapons complex. As part of its mission, SNL operated a 2.6-acre mixed waste landfill (MWL) at its Albuquerque, New Mexico, location on Kirtland Air Force Base and disposed of classified and unclassified waste in the unlined MWL from 1959 through 1988. The MWL is regulated by the New Mexico Environment Department as a solid waste management unit. In 2005, the New Mexico Environment Department ordered SNL and the Department to leave the waste in place, cover the MWL, and periodically monitor the MWL site, including the surrounding groundwater, to ensure that the MWL was not contaminating the local aquifer.

Since December 2014, the OIG has received multiple allegations and information regarding human health and environmental protection issues due to the waste stored in the MWL. For example, it was alleged that the inventory of the MWL was not complete and that contaminants from the MWL had reached the Albuquerque, New Mexico, aquifer. In response, we initiated a special review to examine the facts surrounding the allegations.

Our review substantiated one of six allegations regarding the SNL MWL. Specifically, we substantiated that since the MWL's inception in 1959, SNL and the Department had not maintained a complete inventory of the types and amounts of waste disposed in the MWL. We found examples of waste disposed in the MWL that were not documented in the inventory. Specifically, we found records of contaminated rods and of 204,000 gallons of reactor coolant water. Although the existence of reactor coolant water contained in the MWL was widely known through multiple reports, the item was not listed in the MWL inventory. After the inventory was developed for a 2002 report titled *Report of the Mixed Waste Landfill Phase 2 Resource Conservation and Recovery Act Facility Investigation, Sandia National Laboratories, Albuquerque, New Mexico,* the official MWL inventory was never updated.

Upon acknowledging known items missing from the official MWL inventory, NNSA determined that there would be no value in updating the inventory. Instead, according to NNSA and SNL, to mitigate uncertainty in the inventory, they are in the process of addressing the New Mexico Environment Department's 2005 Final Order. Specifically, they completed construction of the evapotranspirative cover and are fulfilling the requirement for continued monitoring. To SNL's credit, they perform various monitoring activities of the MWL, including monitoring of radon, tritium surface soil, soil vapor, soil moisture, groundwater, and plant and animal life. They are also required to analyze the continued effectiveness of the evapotranspirative cover and reevaluate the feasibility of excavation in a report every 5 years. This report will include an update to the "fate and transport model" with current monitoring data and reevaluate any likelihood of contaminants reaching groundwater. The fate and transport model is used to study and predict future movement of contaminants in the MWL and determine whether the contaminants will eventually reach the groundwater level.

The full report is available at http://energy.gov/sites/prod/files/2016/02/f29/OAI-SR-16-01.pdf

Safeguards and Security

The Department enhances the security and safety of the Nation through its national security endeavors. As a result of the expertise developed to support its nuclear security missions, the national laboratories also serve as strategic assets in support of broader national security. The Department is responsible for the physical security and protection of electric substations and power system control centers identified as critical assets. Additionally, the Department is responsible for preventing nuclear weapons materials and technologies from falling into the hands of adversaries seeking to develop weapons of mass destruction. To faithfully execute its mission, the Department employs numerous security personnel, protects various classified materials and other sensitive property, and develops policies designed to safeguard national security and other critical assets.

In 2013, Safeguards and Security was elevated to the management challenges list primarily as a result of the events at the Y-12 National Security Complex (Y-12), which highlighted the need for a robust security apparatus with effective Federal oversight. In 2016, the Government Accountability Office found that although NNSA had initiated several efforts, it had not completed a Security Infrastructure Plan as required by law. The Security Infrastructure Plan is designed to address physical security threats during the upcoming 5-year fiscal period. Additionally, the Department's management has continually identified issues in this area in its annual memorandums on Assurances of Internal Control. In fact, in its FY 2016 memorandum, one site noted that the aging security alarm system does not provide sufficient functionality to ensure protection. Given the Department's unique mission and the potential catastrophic consequences of a security failure, Department management must ensure the safety and security of the Department's operations.

As evidenced by our recent review on the security and protection of critical assets at Western Area Power Administration, safeguards and security remained an area of focus for the Department.

Followup on Western Area Power Administration's Critical Asset Protection
April 2016, DOE-OIG-16-11

The Department's Western Area Power Administration (Western) markets and transmits electrical power across 15 states to wholesale customers. It maintains an extensive infrastructure, including electrical substations, high-voltage transmission lines and towers, and power system control centers. Western is subject to security requirements established by the Department, the North American Electric Reliability Corporation, and the Department of Homeland Security. As of November 2014, Western officials identified a number of electric substations and power system control centers as critical assets based on existing and draft North American Electric Reliability Corporation requirements. Critical assets are those facilities, systems, and equipment that, if rendered inoperable or damaged, would affect the reliability or operability of the electric system. Western protects its critical assets by conducting risk

assessments of security systems; analyzing threat information, identifying and implementing physical security measures to reduce risk; and documenting the level of risk that management is willing to accept for each asset.

In 2003, we found that Western's risk assessments were inadequate. In 2010, we found that Western had not completed required risk assessments and security measure performance testing and had not implemented physical security enhancements recommended in completed risk assessments. We initiated this followup audit to determine whether Western had effectively and efficiently managed the protection of its critical assets.

Our 2016 audit found that although Western had initiated efforts to improve physical security and protection of its critical assets, significant issues still existed and issues identified in our 2010 report remained unaddressed. Specifically, we found that Western had not always established adequate physical security measures and practices for its critical assets; addressed physical security measures recommended in prior risk assessments; and conducted performance testing to ensure that security measures for physical assets were performing as designed. The issues we identified occurred in large part because Western had not placed sufficient emphasis on physical security. We also found that Western lacked specific policies and procedures for maintaining security equipment, controlling access keys, implementing risk assessment recommendations, and conducting performance tests.

The consequence of tampering with or destroying equipment in substation yards and control buildings could cause significant disruption in the functioning of Government and business, potentially producing a cascading effect far beyond the physical location of the incident. Western had experienced instances where its critical assets had been penetrated and, in some cases, Western did not have the physical security capabilities to promptly detect the intrusions. One of the intrusions resulted in damage to the perimeter fence and control building door and the theft of a security camera and tools. Although not a Western-owned asset, the impact of malicious activity is well demonstrated by a 2013 physical attack on the substation of a utility located in California, which resulted in $15.4 million in damages to 17 transformers and 6 circuit breakers.

The full report is available at http://energy.gov/sites/prod/files/2016/04/f30/DOE-OIG-16-11.pdf

Stockpile Stewardship

The Department is responsible for enhancing the safety, security, and effectiveness of the Nation's nuclear weapons stockpile without nuclear testing. In an increasingly unpredictable world, state and non-state actors continue to pursue nuclear and radiological capabilities. The Administration has pledged that as long as nuclear weapons exist, the United States will sustain safe, secure, and effective nuclear forces to both deter adversaries and reassure allies. To maintain a safe, secure, and effective stockpile without nuclear explosive testing, NNSA extends the lifespan of weapons that have reached the end of their original design life. To accomplish this mission, programs are conducted primarily at 8 sites by a contractor workforce of approximately 30,000 people managed by a Federal workforce comprised of civilian and military staff. For FY 2017, NNSA increased the budget request for weapons activities by $396 million.

A major element of the budget request is the execution of the Nuclear Weapons Council–approved life extension programs (LEPs), including the B61-12. This LEP will improve both the safety and security of the oldest weapon system in the Nation's arsenal. The current total estimated cost for the B61-12 LEP is $8.1 billion, with a First Production Unit by March 2020. While our 2016 report on the management of the B61-12 LEP found that significant challenges had been overcome, we identified issues within the program that, if not corrected, could make it more difficult for the LEP to proactively ensure that its mission and functions are properly executed. Maintaining a credible deterrent is a central component of national security and, as such, management should remain vigilant in ensuring the safety, security, and effectiveness of the nuclear arsenal.

As noted in our report on the B61-12 LEP, stockpile stewardship remained an area of emphasis for the Department.

National Nuclear Security Administration's Management of the B61-12 Life Extension Program August 2016, DOE-OIG-16-15

The primary mission of NNSA's Defense Programs is to ensure the safety, reliability, and performance of the Nation's nuclear weapons stockpile. One of the oldest nuclear weapon systems in the stockpile is the B61. NNSA has raised serious concerns regarding its future reliability. To address these concerns, in 2012, the Nuclear Weapons Council approved the refurbishment of the B61 through an LEP, which extends the bomb's life 20 years and consolidates several existing modifications of the B61 into one modification. The current total estimated cost for the B61-12 LEP is $8.1 billion, with a First Production Unit by March 2020. To help ensure delivery of the updated weapon within cost and schedule, NNSA Defense Programs identified the B61-12 LEP as a pilot program through which it sought to change its approach to LEP management. We initiated this audit to determine whether NNSA was effectively managing the B61-12 LEP.

We found that the B61-12 LEP has overcome significant challenges in implementing several enhanced project management tools. Some of these challenges include developing eight resource-loaded site schedules for development and production activities occurring across NNSA sites, all with different management systems, processes, and cultures. In addition, the B61-12 LEP team had to develop a new system of control accounts and a process not only to integrate earned value data, but also to integrate the different site resource-loaded schedules into an NNSA Integrated Master Schedule. While these accomplishments are noteworthy, we also identified issues within the tools that, in our view, if not corrected, could make it more difficult for the B61-12 LEP to proactively ensure that its mission and functions are properly executed. Specifically, we found that B61-12 LEP master and site schedules contained multiple scheduling issues that limited the full potential of the program's earned value management system to provide program management with the ability to confidently validate the B61-12 LEP's critical path and earned value calculations. Additionally, although the B61-12 LEP implemented a risk management system, we determined that risk mitigation activities could be improved to minimize risk exposure to the B61-12 LEP. We also found that quality assurance activities, in some cases, did not provide documented assurance that redesigned B61-12 LEP components

would fully address prior safety and reliability concerns. Finally, we found that site management reserve estimates were not technically justifiable, potentially constraining the B61-12 LEP's ability to absorb cost impacts of realized risks.

We recognize that the B61-12 LEP master and site schedule improvements have given the program the ability to correct site-to-site schedule alignment problems that were not available to past weapon programs. In addition, our review was performed 4 months after the program completed the new integrated baseline schedule. According to industry standards, the average time to implement an earned value management system is 12 to 18 months, so we are encouraged by the improvements the program had made. However, we believe without further improvement to its project management tools, it will be difficult for the program to proactively manage the costs, schedule, and risks of the B61-12 LEP to ensure it can deliver the First Production Unit within cost and meet its critical national security schedule. In addition, there is uncertainty whether the original cost estimate for the B61-12 LEP contains sufficient management reserve to allow the program to respond to the numerous risks identified in the program.

The full report is available at http://energy.gov/sites/prod/files/2016/08/f33/DOE-OIG-16-15.pdf

Infrastructure Modernization

The Department manages the Federal Government's fifth-largest inventory of real property with an annual operating cost of more than $2 billion. This real property portfolio comprises diverse facilities, including unique fission reactors, accelerators, and high-performance lasers. However, much of the Department's property portfolio reflects an aging infrastructure originating in the 1940s as part of the Manhattan Project. For example, more than 50 percent of NNSA's facilities are more than 40 years old, and almost 30 percent date to the Manhattan Project. To remain safe, secure, and effective, the Nation's nuclear stockpile must be supported by a modern physical infrastructure. In July 2016, the Administrator of NNSA noted that NNSA is long overdue to build a modern, smaller, and safer complex that will meet military requirements; keep the deterrent safe, secure, and effective; and improve worker and public safety.

As the United States reduces the number of nuclear weapons, the reliability of the remaining weapons in the stockpile, including the quality of the facilities needed to sustain it, becomes more important. Our reviews continue to identify concerns with aging infrastructure. For example, we found that Y-12's aging facilities pose risk to Y-12 meeting NNSA's mission. Additionally, infrastructure was continually noted as a concern in the executive management's FY 2016 annual memorandums on Assurances of Internal Control. One Office of Environmental Management site noted facility and systems degradation, deferred maintenance, parts obsolescence, and outdated and inefficient equipment as concerns. Given the Department's aging infrastructure and unique mission requirements, the Department must sustain, modernize, and effectively align real property assets with current and future mission requirements.

Our audit reports summarized below illustrate 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 LEPs, 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 is also aged and has 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 UPS 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. Also, if maintenance needs are not accurately reported, NNSA's decision regarding prioritization of tasks and allocation of resources will be based on inaccurate assumptions.

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

Management of Infrastructure at the Pantex Plant
June 2016, OAI-M-16-12

NNSA's Pantex Plant (Pantex) mission includes the manufacture of specialty explosives, fabrication, and testing of high explosive components, pit requalification and surveillance, and other activities. The NNSA Production Office has the oversight responsibility for the work performed by Consolidated Nuclear Security LLC, the management and operating contractor at Pantex and Y-12. Pantex maintains 608 facilities, including 53 mission-critical facilities, which are primarily used to perform scientific, production, environmental restoration, or stockpile stewardship, and without which, operations would be disrupted or placed at risk. According to Pantex officials, reduced maintenance budgets have created a large backlog of repairs needed to sustain the facilities and infrastructure. In addition, FY 2015 and out-year budgets continue to underfund Pantex requirements for infrastructure management. We initiated this audit to determine whether NNSA had effectively managed infrastructure at Pantex.

Our audit found that although Pantex identified and determined the condition of its infrastructure, systems, and structures that were in need of repair, replacement, or demolition/disposal, its maintenance backlog reporting was inconsistent with Department Guide 433.1-1A, *Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433.1B.* This resulted in a significant underreporting of its maintenance backlog. Department Guide 433.1-1A defines backlogged maintenance as "work that is requested, but not complete (including periodic maintenance past its dude date)." However, we determined that the majority of the requested maintenance tasks at Pantex, although captured in the maintenance system, were not reported to NNSA management via performance metric reporting. In the absence of complete backlog information, NNSA management does not have a true indicator of the site infrastructure's overall condition.

The full report is available at http://energy.gov/sites/prod/files/2016/06/f33/OAI-M-16-12.pdf

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.