U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

SPECIAL REPORT

Management Challenges at the Department of Energy – Fiscal Year 2015

DOE/IG-0924

October 2014

Department of Energy
Washington, DC 20585

October 7, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: "Management Challenges at the Department of Energy – Fiscal Year 2015"

INTRODUCTION

The Department of Energy is responsible for executing some of the Nation's most complex and technologically advanced missions. These include vital work in energy innovation, scientific research, environmental cleanup, nuclear weapons stewardship, and nuclear nonproliferation. To execute this diverse portfolio, the Department receives an annual appropriation approaching $25 billion, employs more than 115,000 Federal and contractor personnel, and manages assets valued at $180 billion, including an extraordinary complex of 17 national research and development laboratories. Considering this set of agency objectives, the Office of Inspector General (OIG) annually identifies what it considers to be the most significant Management Challenges facing the Department. The overall 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) 2015 challenge areas remain largely consistent with those in previous years, based on the results of our work over the last year, a few notable changes in emphasis have been made. As a result, the FY 2015 Management Challenges include the following:

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

A significant change in this year's report involves the removal of Operational Efficiency and Cost Savings from the formal list. Originally introduced in the wake of the Nation's financial crisis, the Department, like other Federal agencies, faced the potential of significant budgetary reductions. While cost savings and increased efficiencies should be a primary agency objective at all times, the atmosphere surrounding the financial crisis provided the Department with, what we thought to be, a unique opportunity to focus on significant operations where reduced costs and increased efficiencies were possible. With this in mind, our FY 2012 Management Challenge report, and those of subsequent years, included a series of measures for management's consideration. The topics included:

- Extending the reach of the Quadrennial Technology Review concept by applying it to the Department's entire science and technology portfolio;

- Eliminating duplicative National Nuclear Security Administration (NNSA) functions;

- Establishing a Base Realignment and Closure (BRAC)-style commission to analyze the Department's laboratory and technology complex;

- Reprioritizing the Department's environmental remediation efforts; and

- Re-evaluating the current structure of the Department's physical security apparatus.

We have been encouraged to find that steps have been taken to further explore these suggestions. For example, in May 2014, the Secretary announced the formation of the congressionally mandated Commission to Review the Effectiveness of the National Laboratories. Further, the Congressional Advisory Panel on the Governance Structure of NNSA is currently examining the roles, responsibilities, and authorities of NNSA's current organizational structure, including the Department's defense laboratories.

Separately, we have changed the designation of Human Capital Management, downgrading the topic from a management challenge to the OIG's Watch List. As noted in previous reports, for a number of years strategic management of human capital has been recognized by oversight organizations as one of the Government's most significant challenges. While concerns remain, the Department has worked aggressively in this arena. For example, it has instituted a program to close critical skills gaps, and the Department's Office of the Chief Human Capital Officer has initiated efforts to improve senior executive recruitment and orientation. The Department also has begun an implementation process to improve human resource delivery models. One aspect of this new approach will be the establishment of shared service centers to support the Department's management structure. There is more to be done, but these important steps form the basis of our actions in this regard.

WATCH LIST

As previously referenced, the OIG also prepares a 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 2015, in addition to the newly added Human Capital

Management topic, the Watch List includes Infrastructure Modernization, Loan Guarantee Program, and Worker and Community Safety.

Infrastructure Modernization, which includes efforts to revitalize the Department's aging weapons complex, is a matter of special concern to the OIG at this time. In specific terms, as the entity ultimately responsible for auditing the Department's annual financial statement, we have noted a significant upward trend in the Department's Deferred Maintenance Account. In FY 2009, deferred maintenance on the Department balance sheet was $3.9 billion. For FY 2013, that figure had grown to more than $5 billion. Given this trend, we are concerned that important functions could be curtailed if maintenance is not sustained on a current basis.

Attached is a brief synopsis of each management challenge, accompanied by summaries of examples of OIG reports that inform the 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, National Nuclear Security Administration
Acting Under Secretary for Science and Energy
Acting Under Secretary for Management and Performance
Chief of Staff
Chief Financial Officer

Contract and Financial Assistance Award Management

The Department of Energy (Department) is the most contractor-dependent civilian agency in the Federal government. The Department awards contracts, grants, and other financial assistance instruments to industrial companies, small businesses, academic institutions, and nonprofit organizations. In fact, approximately 90 percent of the Department's budget is spent through such instruments. The challenges associated with managing the Department's sizeable contracting portfolio have been recognized internally by the agency, as well as externally by the Government Accountability Office, which has included inadequate contract and project oversight on its High-Risk List since 1990. Given the number of contracts handled by the Department and the complexity and importance of the Department's numerous multi-million dollar projects, we consider that the area of Contract and Financial Assistance Award Management remains a significant management challenge.

NNSA's Management of the $245 Million Nuclear Materials Safeguards and Security Upgrades Project Phase II at Los Alamos National Laboratory
January 2014, DOE/IG-0901

To address aging security infrastructure, the National Nuclear Security Administration (NNSA) is now in the final phase of a project to upgrade security at the Los Alamos National Laboratory's (LANL) Technical Area-55. These upgrades, known collectively as the Nuclear Materials Safeguards and Security Upgrades Project - Phase II (NMSSUP), began in 2009. LANL divided the bulk of the project into five firm-fixed price subcontracts that were awarded to one design company and three construction contractors. Due to favorable contract bids in April 2011, NNSA reduced the estimated total project cost from $245 million to $213 million. The project consisted of more than 2,200 scheduled activities and was expected to be completed in January 2013. Los Alamos National Security, LLC (LANS) is the management and operating contractor for LANL.

Our review revealed that the NMSSUP suffered from a number of project management weaknesses. These issues ultimately resulted in cost increases of as much as $41 million and delayed completion of the project by nearly a year. In addition, management information systems failed to provide accurate and complete information about the funds available to complete the remaining work scope. These project management issues created a series of problems that collectively resulted in significant unanticipated cost and schedule impacts. Although it failed to take effective action to address project management weaknesses in NMSSUP, the Department implemented detective controls that identified many of the issues in this report and are key tools for holding Department contractors accountable for their performance. NNSA had taken a number of positive actions to hold LANS accountable for lack of performance; however, project management concerns remain despite these actions.

The full report is available at: http://energy.gov/sites/prod/files/2014/01/f6/IG-0901_1.pdf.

Cost and Schedule of the Mixed Oxide Fuel Fabrication Facility at the Savannah River Site
May 2014, DOE/IG-0911

In September 2000, the United States and Russia signed a Plutonium Management and Disposition Agreement for the disposal of surplus weapons-grade plutonium. This agreement called for each country to dispose of at least 34 metric tons of plutonium by converting it into mixed oxide fuel that can be used in commercial nuclear power reactors. To carry out this program, the Department of Energy (Department) decided to construct the Mixed Oxide Fuel Fabrication Facility (MOX Facility) at the Savannah River Site near Aiken, South Carolina. Shaw AREVA MOX Services, LLC (MOX Services), the current Facility contractor, has been working on the design of the facility since 1999.

The National Nuclear Security Administration (NNSA) and MOX Services have been largely unsuccessful in controlling the cost and schedule for the MOX Facility. A March 2012 construction project review conducted by NNSA concluded that the MOX Facility had a very low probability of being completed according to the approved baseline. NNSA directed MOX Services to develop a baseline change proposal with updated project completion, cost and schedule projections. Under the revised baseline, it was estimated that total project costs would grow to about $7.7 billion and that completion would slip to November 2019. This represents cost growth of about $2.9 billion and project schedule slippage of over 3 years.

The anticipated cost and time required to complete the MOX Facility were significantly underestimated due to a number of factors. This included, most prominently, the Department's 2007 approval of a project baseline that was developed from an immature design, understating the level of effort to install various construction commodity items, and high personnel turnover rates. Prior to approval, the Department's own independent review of the project baseline found that the design review of the MOX Facility was incomplete. We also noted that additional work scope added at NNSA's direction caused some of the cost growth in the baseline change proposal developed by MOX Services. Despite project expenditures of about $4 billion and a proposal to place the MOX Facility construction project into cold standby status in Fiscal Year 2015, we remain concerned with the project management issues observed during the audit.

The full report is available at: http://energy.gov/sites/prod/files/2014/05/f16/DOE-IG-0911.pdf.

Cybersecurity

Given the importance and sensitivity of the Department's activities, along with the vast array of data it processes and maintains, cybersecurity has become a crucial aspect of the Department's overall security posture. Although the Department has implemented numerous countermeasures in recent years, security challenges and threats to the Department's information systems continue and are constantly evolving. Adversaries routinely attempt to compromise the information technology assets of the Department. Recent intrusions of the Department's information technology systems, which in one notable instance, resulted in the exfiltration of personally

identifiable information on more than 100,000 individuals, have highlighted the importance of protecting such systems as well as the difficulty and diligence required to guard against such intrusions. During our annual evaluation of the Department's information technology systems, we highlighted specific weaknesses and offered recommendations to aid in correcting recognized deficiencies. Clearly, it is critical that cybersecurity protective measures keep pace with the growing threat. As a result of these inherent risks and the sensitivity of much of the Department's work, we have identified Cybersecurity as a continuing and significant management challenge.

Department of Energy's July 2013 Cyber Security Breach
December 2013, DOE/IG-0900

To facilitate its administrative and operational needs, the Department of Energy maintains a substantial amount of personally identifiable information (PII). The Department's Management Information System (MIS) provides a gateway for users to access a system known as the DOE Employee Data Repository (DOEInfo) database. Because of the importance of ensuring the security of the Department's systems and sensitive information and at the request of the Chief Information Officer, we commenced a special review into the circumstances surrounding the MIS/DOEInfo breach.

In spite of a number of early warning signs that certain personnel-related information systems were at risk, the Department had not taken action necessary to protect the PII of a large number of its past and present employees, their dependents and many contractors. We concluded that the July 2013 incident resulted in the exfiltration of a variety of PII on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. We also identified numerous contributing factors related to inadequate management processes. We also found that the extent of PII stolen was much more extensive than that originally reported by the Department.

These issues created an environment in which the cybersecurity weaknesses we observed could go undetected and/or uncorrected. While we did not identify a single point of failure that led to the MIS/DOEInfo breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease.

The full report is available at: http://energy.gov/sites/prod/files/2013/12/f5/IG-0900.pdf.

The Department of Energy's Unclassified Cyber Security Program – 2013
October 2013, DOE/IG-0897

Cybersecurity threats are a major concern for all Federal entities, including the Department of Energy. The *Federal Information Security Management Act of 2002* (FISMA) established the requirement for Federal agencies to develop, implement and manage agency-wide information

security programs, and provide acceptable levels of security for the information and systems that support the operations and assets of the agency. As part of our responsibilities under FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Department's unclassified cybersecurity program adequately protected its unclassified data and information systems.

The Department had taken a number of positive steps over the past year to correct cybersecurity weaknesses related to its unclassified information systems, including corrective actions to resolve 28 of the 38 conditions we identified during our FY 2012 evaluation. In spite of these efforts, we found that significant weaknesses and associated vulnerabilities continued to expose the Department's unclassified information systems to a higher than necessary risk of compromise. Our testing revealed various weaknesses related to security reporting, access controls, patch management, system integrity, configuration management, segregation of duties and security management. In total, we discovered 29 new weaknesses and confirmed that 10 weaknesses from the prior year's review had not been resolved. These problems were spread across 11 of the 26 Department locations where we performed testing. The weaknesses identified occurred, in part, because Department elements had not ensured that cybersecurity requirements were fully developed and implemented.

The full report is available at: http://energy.gov/sites/prod/files/2013/11/f4/IG-0897.pdf.

Environmental Cleanup

With the end of the Cold War, the Department's environmental remediation mission took on a greater focus as the agency began to dispose of large volumes of radioactive waste resulting from more than 50 years of nuclear defense and energy research work. This effort involves 2 million acres of land and employs more than 30,000 Federal and contractor employees. For example, one of the largest cleanup efforts of its kind in the world is at the Hanford Site in southeastern Washington, where 11,000 employees are working to remediate 40 years of plutonium processing which resulted in, among several challenges, millions of gallons of radioactive waste stored in 177 large underground tanks. Cleanup activities at most sites are governed by one or more regulatory agreements or court orders that establish scopes of work, timeframes, and specific achievement milestones. The disposal and cleanup effort is complex and costly. In fact, these efforts are projected to cost more than $280 billion and will continue well into the foreseeable future. As has been the case in previous years, Environmental Cleanup remains a management challenge that warrants attention on the part of Department management.

Department of Energy Quality Assurance:
Design Control for the Waste Treatment and Immobilization Plant at the Hanford Site
September 2013, DOE/IG-0894

The Department is constructing the $12.2 billion Waste Treatment and Immobilization Plant (WTP) to vitrify approximately 56 million gallons of radioactive and chemically hazardous

waste stored at the Hanford Site. To ensure the vitrification process is safe for workers, the public and the environment, the Department required the contractor for the WTP, Bechtel National Inc., to develop and follow a quality assurance program based on the American Society of Mechanical Engineer's Quality Assurance Requirements for Nuclear Facility Applications Standard. In response to an allegation that Bechtel was missing design control documentation for the WTP and as such, could not demonstrate that equipment was appropriately manufactured, a September 2013 OIG review revealed significant shortcomings in the Department's process for managing the design and fabrication changes of waste processing equipment procured for the WTP. The Department had not ensured that Bechtel subjected design changes requested by suppliers to the required review and approval by Bechtel's Environmental & Nuclear Safety Group. Further, the Department had not ensured that Bechtel properly verified that deviations from design requirements that could affect nuclear safety were implemented.

The full report is available at: http://energy.gov/sites/prod/files/2013/10/f3/IG-0894.pdf.

Nuclear Waste Disposal

Under the *Nuclear Waste Policy Act of 1982*, as amended, the Department is responsible for the management and safe disposal of high-level defense and commercial waste and spent nuclear fuel. For a number of years, the centerpiece of the Department's efforts relating to the disposal of nuclear waste was the development of the Yucca Mountain Nuclear Waste Repository in Nye County, Nevada. The Department's FY 2010 budget request, however, included no funding for the Yucca Mountain Project, effectively terminating the Office of Civilian Radioactive Waste Management. Since that time, the Blue Ribbon Commission on America's Nuclear Future issued a report at the direction of the President on policies for managing the end of the nuclear fuel cycle, which includes alternative storage sites. Subsequently, in January 2013, the Department released its *Strategy for the Management and Disposal of Used Nuclear Fuel and High-Level Radioactive Waste*, and is currently working to plan, develop, and implement this strategy. In addition, the Department faces a number of additional challenges related to the disposal of transuranic and other waste products. Given the importance of a coherent strategy on nuclear waste disposal that protects public health, safety, and the environment, and until a viable solution for disposal and storage is developed, the area of Nuclear Waste Disposal will be recognized as a significant challenge facing the Department.

Remediation of Selected Transuranic Waste Drums at Los Alamos National Laboratory – Potential Impact on the Shutdown of the Department's Waste Isolation Pilot Plant
September 2014, DOE/IG-0922

The Department of Energy's Los Alamos National Laboratory (LANL) is one of the Nation's premier national security laboratories. Los Alamos National Security, LLC manages and operates LANL. As part of its mission, LANL generated a large volume of transuranic (TRU) waste consisting mostly of radioactively contaminated clothing, tools, rags, debris and soil. In January 2012, a framework agreement was established between the Department and the New Mexico Environment Department (NMED) to ship 3,706 cubic meters of combustible and

dispersible TRU waste from LANL to the Department's Waste Isolation Pilot Plant (WIPP) located in Carlsbad, New Mexico, for permanent disposal by June 30, 2014. The Department established the Central Characterization Project to characterize and certify waste to help ensure that it met WIPP's waste acceptance criteria.

On February 14, 2014, a radiological release from one TRU waste drum was detected in the underground repository at WIPP. As a consequence, underground operations at WIPP were suspended and the Nation's only operating deep geologic repository for the permanent disposal of defense-related TRU waste was shut down for an indefinite period. The impact of the shutdown, both incurred to date and in the future is valued in terms of tens of millions of dollars. We initiated a special inquiry to determine whether LANL appropriately managed the remediation and repackaging of waste shipped to WIPP.

Our review identified several major deficiencies in LANL's procedures for the development and approval of waste packaging and remediation techniques that may have contributed to the radiological event. Of particular concern, not all waste management procedures at LANL were properly vetted through the established procedure revision process nor did they conform to established environmental requirements. In our view, immediate action is necessary to ensure that these matters are addressed and fully resolved before TRU waste operations are resumed, or, for that matter, before future mixed radioactive hazardous waste operations are initiated. Management concurred with the report's findings and recommendations and stated that the results of our investigation are generally consistent with findings from internal investigations.

The full report is available at: http://energy.gov/sites/prod/files/2014/10/f18/DOE-IG-0922.pdf.

Safeguards and Security

While the Department has shifted its focus over time, since the origin of the Manhattan Project, special emphasis on safeguards and security has remained a vital aspect of the Department's mission. In order 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 our FY 2013 report, Safeguards and Security was elevated to the management challenges list primarily as a result of events at the Y-12 National Security Complex, which highlighted the need for a robust security apparatus with effective Federal oversight. Further, as a direct result of the Y-12 security breach, the Department reported the Y-12 incident as a material weakness in its FY's 2012 and 2013 Statement of Assurance. Given the policy issues that have arisen as a result of this event and the importance of ensuring the safe and secure storage of nuclear materials at Department sites, Safeguards and Security remains a significant management challenge.

Review of Controls Over the Department's Classification of National Security Information March 2014, DOE/IG-0904

The Department of Energy handles and manages a broad spectrum of classified information, including National Security Information (NSI). The Office of Health, Safety and Security's

Office of Classification, manages the Department-wide classification program and establishes policies to conform with Federal classification requirements. Implementation of classification requirements is shared among various organizations within the Department. In addition, the Department's Office of Intelligence and Counterintelligence is required to follow NSI policies and procedures instituted by the Office of the Director of National Intelligence. Similarly, NNSA separately develops and implements policies and procedures, in coordination with the Office of Classification, for the protection and security of classified information at NNSA sites. Our inspection revealed that the Department had established and implemented critical elements of its classified NSI program. However, our review revealed that certain aspects of the NSI program could be improved. For instance, our inspection determined that a classification marking tool embedded in the classified email system at an NNSA site automatically marked emails as Secret/Restricted Data, regardless of content. The classification related issues we observed occurred, in part, because of ineffective oversight of classification activities and inadequate training and guidance.

The full report is available at:
http://energy.gov/sites/prod/files/2014/04/f14/Inspection%20Report-IG-0904_0.pdf.

Stockpile Stewardship

The Department is responsible for the maintenance, certification, and reliability of the Nation's nuclear weapons stockpile. To help ensure that our nuclear weapons continue to serve their essential deterrence role, the Department conducts stockpile surveillance and engineering analyses, refurbishes selected nuclear systems, and sustains the ability to restore the manufacturing infrastructure for the production of replacement weapons. Our reviews in recent years have suggested that sustained efforts to improve operational efficiency are necessary to manage problems associated with an aging weapons complex and the implementation of multiple, overlapping weapons life extensions within a constrained budget environment. While the Department has taken action in recent years to further enhance the safety and reliability of the Nation's nuclear weapons stockpile, sustained efforts will be necessary if the Department is to extend the life of aging warheads and maintain a viable weapons stockpile.

National Nuclear Security Administration Nuclear Weapons Systems Configuration Management
March 2014, DOE/IG-0902

The Office of Inspector General received multiple allegations regarding NNSA's management of configuration management (CM) information. The allegations related to incomplete product definitions for NNSA nuclear weapons, and ineffective management of classified nuclear weapons drawings, a situation that could lead to unauthorized changes to the drawings. In response, we initiated this audit to determine whether NNSA had maintained accurate and complete CM information for nuclear weapons and nuclear weapons components to support safe, sound and timely decisions related to these devices.

Our review substantiated the allegations and identified instances in which NNSA had not maintained accurate and complete CM information for its nuclear weapons and components. We

also identified additional concerns with the use of nuclear weapons parts and components that did not conform to specifications. For instance, we found that NNSA sites could not always locate 'as-built' product definitions or associated drawings for nuclear weapons and components in its official records repositories, and sites did not always ensure that parts that did not conform to specifications were actually fit for use in a nuclear weapon.

Management concurred with our recommendations and stated that NNSA remains vigilant in configuration management information for its nuclear weapons and components as well as in supply chain management issues. Additionally, management's proposed and initiated corrective actions are responsive to our findings and recommendations.

The full report is available at: http://energy.gov/sites/prod/files/2014/03/f14/IG-0902.pdf.

The Resumption of Criticality Experiments Facility Operations at the Nevada National Security Site
September 2013, OAS-M-13-09

Citing safety and security concerns, in 2004, NNSA halted criticality experiments at Los Alamos National Laboratory and authorized a capital project to transfer this capability to the Device Assembly Facility at the Nevada National Security Site (Nevada). The project remodeled a portion of the Device Assembly Facility to form the National Criticality Experiments Research Center (NCERC).

We found that NNSA restored many of the former capabilities of the Criticality Experiments Facility at the NCERC in Nevada. We noted, however, that several problems with start-up activities resulted in delays in restoring the full array of experimental capabilities included in the project. Specifically, NNSA was unable to authorize the start-up of NCERC operations until May 2011. The program experienced further delays in the start-up activities of each criticality machine. Further, NCERC has been unable to restore its full capability to perform plutonium-based criticality experiments.

The delays in restoring capabilities occurred because NNSA had not ensured that contractors had developed adequate procedures for correcting concerns identified during the process to authorize the start-up of NCERC, the safety basis documentation matched facility conditions, and procured safety equipment met cited standards. Additionally, NNSA had not ensured effective management of the multiple contractors involved in developing and amending the safety basis documentation. Finally, NNSA has struggled to successfully integrate and resolve issues between the multiple contractors involved in NCERC facility operations.

The full report is available at: http://energy.gov/sites/prod/files/2013/10/f3/OAS-M-13-09.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 OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed 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.