OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-19-22 March 2019

DEPARTMENT OF ENERGY'S MANAGEMENT OF LEGACY INFORMATION TECHNOLOGY INFRASTRUCTURE

Department of Energy
Washington, DC 20585

March 27, 2019

MEMORANDUM FOR THE CHIEF INFORMATION OFFICER

FROM: Sarah B. Nelson
Assistant Inspector General
for Technology, Financial, and Analytics
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on the "Department of Energy's Management of Legacy Information Technology Infrastructure"

BACKGROUND

The Federal Government spends close to $90 billion annually on information technology (IT) resources. Approximately 80 percent of funds budgeted for IT are dedicated to maintaining legacy IT that is outdated or obsolete. Legacy IT resources are particularly vulnerable to malicious cyber activity and may require additional funding for hardening or support. To address concerns over aging technologies, Congress authorized up to $500 million to fund the *Modernizing Government Technology Act* that was signed into law in 2017. The law is designed to improve, retire, or replace existing IT; transition legacy systems to commercial cloud computing services; and support efforts to provide adequate risk-based solutions to address evolving threats to information security. In fiscal year 2018, the Department of Energy received $15 million under the *Modernizing Government Technology Act* to accelerate an enterprise electronic mail migration.

The Department and its contractors operate many types of IT systems and infrastructure to support its diverse missions related to nuclear security, scientific research and development, and environmental management. Prior reviews conducted by the Office of Inspector General have identified weaknesses related to the existence of outdated software and hardware. We initiated this audit to determine whether the Department effectively managed the lifecycle of legacy IT systems and components. Our review focused on the Department's unclassified information systems and did not include industrial control and national security systems.

RESULTS OF AUDIT

We determined that while actions to manage the lifecycle of unsupported IT systems and components had been taken at the sites reviewed, opportunities for improvement exist. For example, the Department, including contractor-managed locations, had not developed a

comprehensive plan to identify and replace legacy IT. Specifically, we found that the Pacific Northwest National Laboratory, Lawrence Livermore National Laboratory (Livermore), SLAC National Accelerator Laboratory (SLAC), and the Hanford Site had taken actions to identify and reduce legacy systems and components. However, improvements are necessary related to the identification of legacy IT infrastructure, and development and implementation of plans to modernize IT systems and components. Unfortunately, our review of several sites did not reveal any requirements within the Department to identify and eliminate legacy IT; as such, we made a recommendation that, if fully implemented, should improve the Department's management of legacy IT.

IDENTIFICATION AND MODERNIZATION OF LEGACY IT

We found that a formal definition for legacy IT resources had not been developed nor had a comprehensive plan to reduce or eliminate legacy IT across the Department been developed and implemented. In the absence of a documented definition, thus ensuring consistency in the identification of legacy IT, officials at the sites reviewed indicated that legacy IT included hardware and software that was no longer supported by the manufacturer. Site officials further noted that they relied upon system owners and system scans to identify legacy IT. While legacy IT typically includes these aforementioned items, not having a documented definition may result in the sites not always including systems incapable of meeting the organizational requirements or those using outdated program languages. Specifically, without a documented definition of legacy IT resources, the Department cannot ensure that it is consistently identifying and accounting for all legacy IT.

While site representatives acknowledged that legacy IT existed at the locations reviewed, none of the locations reviewed had a comprehensive plan for the modernization of legacy IT. In addition, we were unable to quantify the exact amount of legacy IT at each of the sites visited because three of the four sites visited did not track legacy status in their inventory systems. We did find that each of the locations had identified various legacy IT and developed projects to modernize several of those items. However, these projects did not culminate into an overarching plan to reduce or eliminate legacy IT Department-wide. Furthermore, we found that sites were still in the process of implementing those projects. For instance, we found that:

- While Pacific Northwest National Laboratory indicated that it was in the process of implementing several IT modernization projects, including a data center migration, officials stated that they had to manually review an inventory report in response to our audit to identify which items were legacy IT. Although the data center migration project is a positive step in reducing legacy IT, not having an identified inventory of all legacy IT could limit modernization at a site-level. We do credit Pacific Northwest National Laboratory with a reduction in end-of-life servers from 67 percent to 20 percent between March 2017 and July 2018.

- Livermore reported 58 applications, 35 operating systems, and 118 unclassified network devices that were all legacy IT. To its credit, Livermore had six modernization projects ongoing to replace some of these legacy IT applications and operating systems and had plans to replace 45 of the 118 legacy IT network devices by the second quarter of fiscal year 2019. Livermore had already replaced 37 of the 45 at the time of our audit.

- SLAC's system inventory did not always identify legacy IT infrastructure. Specifically, the site's inventory did not identify any applications or operating systems as legacy IT; however, SLAC officials indicated that there were legacy IT systems running at the site, including the previous enterprise resource planning system. Additionally, SLAC's inventory included 2,267 legacy servers and 53 legacy Macintosh workstations. To its credit, SLAC was in the process of retiring its legacy IT enterprise resource planning system. SLAC representatives stated that they will decommission the legacy IT enterprise resource planning system once its database and required pages/tables are fully migrated into the new system, which has already been deployed and put in service. The process is expected to be completed in 2019. Furthermore, we noted that the number of legacy workstations had been reduced. SLAC representatives indicated that they spent approximately $850,000 each year on a lifecycle management project to modernize hardware at the site with mostly leased hardware.

The actions taken by Pacific Northwest National Laboratory, SLAC, and Livermore were positive steps toward IT modernization. However, without a standard definition to identify legacy IT and a comprehensive plan to replace it, program offices and sites may not be able to fully identify legacy IT and plan for its replacement or modernization.

BARRIERS TO MODERNIZATION

Department officials reported several barriers impacting the ability to modernize legacy IT infrastructure, including the availability of funding. In addition, contrary to Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, the Department's Office of the Chief Information Officer had not developed processes and policies to phase out, as rapidly as possible, all unsupported information systems and system components. As such, we found that the lack of Department requirements potentially created a barrier for reducing or eliminating legacy IT. Specifically, without requirements, funding that might be available could potentially be used for other projects that have set deadlines.

Each of the four sites visited consistently indicated that funding was an issue. For instance, the Richland Operations Office's infrastructure and site services contractor at the Hanford Site reported nearly $10.2 million in unfunded priorities. As of June 30, 2018, only 3 of 18 items, an estimated $1.8 million in project costs, had been funded and a fourth was partially funded. In addition, while Livermore was able to fund a majority of its modernization projects, four projects planned for fiscal year 2018 were placed on hold due to funding restrictions. Additionally, SLAC officials stated that for a 5-year lifecycle, legacy IT equipment replacement would require $1.5 million above the current budget that covers the existing leases.

Although sites reported funding as an issue, the Department may not have taken full advantage of the *Modernizing Government Technology Act*, which authorized funding to assist in

modernizing Federal IT to mitigate current risks and accelerate the acquisition and deployment of modernized IT solutions by addressing impediments in the areas of funding, development, and acquisition practices. The *Modernizing Government Technology Act* required agencies to articulate funding requests that include a strong business case, technical design, procurement strategy, and program management, thereby potentially assisting some of the sites reviewed to achieve their goals.

IMPACT

If the Department continues to operate legacy IT systems and system components, there is an increased level of operational risk, including maintenance costs, and may lead to an inability to meet mission requirements. In addition, there is an increased level of security risks, including the inability to use current cybersecurity best practices, such as data encryption and multi-factor authentication, making these systems particularly vulnerable to malicious cyber activity. The continued use of unsupported IT is especially concerning in light of the Department's July 2013 cybersecurity breach. The Special Report on the *Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013) following the breach found that it had been caused, in part, by a failure to assign the appropriate level of urgency to replacing end-of-life systems. In addition, the Department had not taken appropriate action to remediate known vulnerabilities through patching, system enhancements, or upgrades.

RECOMMENDATION

We have reported on various concerns related to legacy IT resources over the years, ranging from security over outdated software to implementing new information systems to replace aging systems. To continue to improve activities related to the Department's management of legacy IT, we recommend that the Department's Chief Information Officer, in coordination with Department elements, including the National Nuclear Security Administration:

1. Develop policies and procedures to ensure unsupported IT systems and system components be phased out as rapidly as possible, including defining the resources that should be considered legacy IT and establishing a comprehensive plan to replace legacy IT across the Department to include its contractors.

MANAGEMENT RESPONSE

Management concurred with the report's recommendation and commented that corrective actions were ongoing to address the issues identified in the report. Management indicated that it was in the process of finalizing a memorandum to address IT asset management, including IT legacy and other enterprise considerations.

AUDITOR COMMENTS

Management's comments and planned actions were responsive to our recommendation. Management's comments are included in Attachment 3.

Attachments

cc: Deputy Secretary
Chief of Staff
Assistant Secretary for Environmental Management
Administrator, National Nuclear Security Administration
Deputy Director, Office of Science

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

We conducted this audit to determine whether the Department of Energy effectively managed the lifecycle of legacy information technology (IT) systems and components.

SCOPE

The audit was performed between February 2018 and March 2019. We conducted work at Department Headquarters in Washington, DC, and Germantown, Maryland; Richland Operations Office in Richland, Washington; Pacific Northwest National Laboratory in Richland, Washington; Lawrence Livermore National Laboratory in Livermore, California; and SLAC National Accelerator Laboratory in Menlo Park, California. The review was limited to evaluating whether the Department effectively managed the lifecycle of legacy IT. Our test work did not include the Federal Energy Regulatory Commission or the Power Marketing Administrations. The audit was conducted under Office of Inspector General project number A18TG015.

METHODOLOGY

To accomplish the objective, we:

- Reviewed applicable laws and regulations;
- Reviewed applicable standards and guidance issued by the Department, including the Department's Office of the Chief Information Officer;
- Reviewed prior reports issued by the Office of Inspector General and Government Accountability Office;
- Held discussions with Federal and contractor officials and personnel from Department Headquarters and the sites reviewed related to management of legacy IT, including representatives from the Office of the Chief Information Officer;
- Determined whether sites identified legacy IT, developed modernization plans, and made progress with respect to those plans; and
- Reviewed documents, such as IT inventories and modernization plans, related to unsupported information technology systems and components.

We conducted this audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our objective. Accordingly, we assessed significant internal controls

and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures and/or goals related to management and performance. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our objective.

Management waived an exit conference on March 15, 2019.

RELATED REPORTS

Office of Inspector General

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2018* (DOE-OIG-19-01, October 2018). The Office of Inspector General found that at least 10 locations continued to use software on workstations and servers that were missing security patches or were no longer supported by the vendor. While we identified weaknesses at each of the 10 locations, a number of them had either documented the acceptance of risk or had developed corrective action plans with respect to the vulnerabilities identified.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2017* (DOE-OIG-18-01, October 2017). The Office of Inspector General found that two locations were running applications that the vendor no longer supported. For example, at one site, the Office of Inspector General identified at least 14 servers operating unsupported software applications related to financial management. The review also noted that sites had not appropriately documented and/or accepted the risks of operating the unsupported applications.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2016* (DOE-OIG-17-01, October 2016). The Office of Inspector General found that four locations were running applications that the vendor no longer supported. For instance, at one site, the Office of Inspector General identified at least five unsupported software applications. In addition, one site was running unsupported client applications on more than half of the workstations tested.

- Audit Report on *The Energy Information Administration's Information Technology Program* (DOE-OIG-16-04, November 2015). The audit found that numerous cybersecurity weaknesses existed. In some instance, the Energy Information Administration used software that was no longer supported by the vendor, leaving potential vulnerabilities unmitigated.

Government Accountability Office

- *INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems* (GAO-16-468, May 2016). The Government Accountability Office found that the Federal Government spends more than $80 billion on information technology, with about 75 percent spent on operating and maintaining legacy information technology systems. The Government Accountability Office recommended that the Department of Energy identify and plan to modernize or replace legacy systems as needed.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

March 13, 2019

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: STEPHEN (MAX) EVERETT
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "Department of Energy's Management and Use of Legacy Information Technology Infrastructure (Job Code A18TG015)"

Thank you for the opportunity to comment on the Draft Evaluation Report, "Department of Energy's Management and Use of Legacy Information Technology Infrastructure". The Department, including the National Nuclear Security Administration, understands the importance of phasing out unsupported IT systems and system components as rapidly as possible.

DOE concurs with the recommended path forward. Details are in the attached enclosure.

If you have any questions or need additional information, please contact Ms. Pamela Isom, Deputy CIO for Architecture, Engineering, and Technology & Innovation at 202-287-1450.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Enclosure

MANAGEMENT RESPONSE
IG Draft Report
Department of Energy's Management of Legacy Information Technology Infrastructure
(Job Code A18TG015)

Recommendation: *The Department's Chief Information Officer, in coordination with Department elements, including the National Nuclear Security Administration, should Develop policies and procedures to ensure unsupported IT systems and system components be phased out as rapidly as possible, including defining the resources that should be considered legacy IT and establishing a comprehensive plan to replace legacy IT across the Department to include its contractors.*

Response: Concur

The Deputy CIO for Architecture, Engineering, and Technology & Innovation (IM50) has initiated a memorandum through the Enterprise Architecture governance process, to document the current state, future state, and a three year technology roadmap for the Department. The memorandum addresses IT asset management, including IT legacy, and other enterprise architectural considerations. The memorandum is pending Departmental review and approval.

Estimated Completion Date: September 30, 2019

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 us:

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) 586-1818. For media-related inquiries, please call (202) 586-7406.