



U.S. Department of Energy  
Office of Inspector General  
Office of Audits and Inspections

---

# AUDIT REPORT

Follow-up on the Department of Energy's  
Management of Information Technology  
Hardware

DOE/IG-0926

October 2014


---



**Department of Energy**  
Washington, DC 20585

October 30, 2014

MEMORANDUM FOR THE SECRETARY

FROM:   
Gregory H. Friedman  
Inspector General

SUBJECT: INFORMATION: Audit Report on "Follow-up on the Department of Energy's Management of Information Technology Hardware"

BACKGROUND

The Department of Energy and its facility contractors rely on various types of information technology (IT) resources to accomplish objectives related to its national security, energy, science and environmental missions. The Department spends significant funds annually to acquire and maintain its IT resources. Because many organizations did not track all IT hardware expenditures, we were unable to determine actual expenditures with precision. However, based on the cost data we could obtain, we estimated that the Department likely spent more than \$125 million in Fiscal Year (FY) 2012 on IT hardware such as servers, desktops, laptops and printers. In recent years, the Department's budget has been under enhanced scrutiny, increasing the need to ensure resources are effectively and efficiently managed.

Prior Office of Inspector General reports on *Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007), and *The Office of Science's Management of Information Technology Resources* (DOE/IG-0831, November 2009), revealed that the Department had not adequately managed the acquisition and control of IT hardware. Specifically, we found contractors had not consistently taken advantage of opportunities to reduce acquisition and support costs or ensure that accountability was maintained over sensitive computers and devices. In response to our prior reports, management planned to encourage aggregation of requirements for IT hardware to control costs. We initiated this follow-up audit to determine whether the Department effectively managed the acquisition and maintenance of IT hardware.

RESULTS OF AUDIT

Although the Department made efforts to address prior recommendations, we found that weaknesses in the Department's governance of IT hardware continued to exist. In particular, the Department had not effectively managed its IT hardware acquisition process or fully developed and implemented an IT supply chain risk management program. As such, we determined that the Department spent nearly \$2 million more than necessary in FY 2012 at just the eight sites included in our review. Specifically:

- Although seven of eight locations reviewed had developed acquisition standards for desktops and laptops, we found frequent deviations from the standards. Specifically, sites purchased nonstandard desktops and laptops over 75 percent of the time, resulting in expenditures of up to nearly \$1.7 million more than necessary. At one such facility, all of the computers purchased for administrative use were nonstandard.
- The Department paid up to \$282,000 more than necessary during the period reviewed because it purchased the same or similar IT hardware at dramatically varying prices. For example, three Office of Science and National Nuclear Security Administration (NNSA) sites paid significantly more for a specific desktop computer than did Oak Ridge National Laboratory.
- While actions had been taken, the Department had not fully developed and implemented an effective IT supply chain risk management program to protect its systems and information. The goal of such a program is to establish procurement- and cybersecurity-related policies, processes and controls over vendors to help minimize security risks that could negatively affect the Department's operations. Despite requirements to do so, programs and sites had not sufficiently addressed certain aspects of supply chain risk management, including issues related to security over IT hardware vendors, communication of security threats/risks and best practices among Departmental elements, and coordination of potential duplicative supply chain management efforts.

The problems we identified occurred, in part, because the Department had not developed and implemented a comprehensive approach to managing IT hardware. In particular, the Department and its facility contractors had not always developed and enforced hardware standards; implemented procedures to ensure organizations and sites effectively coordinated acquisition efforts; and fully leveraged enterprise-wide purchasing agreements. For instance, although NNSA recently began efforts to coordinate contract terms for IT hardware, sites continued independent contracting efforts rather than taking advantage of opportunities for potential savings associated with bulk purchase agreements. While there may be an argument for local control over contracting functions, we believe significant savings could be obtained by local bulk purchasing and pooling resources through organizations, such as the NNSA Supply Chain Management Center. In addition, the Department had not fully developed and/or implemented policies and procedures related to ensuring an effective supply chain risk management process. For example, programs and sites' risk management implementation plans were not always updated to incorporate supply chain management controls. And, programs and sites had not adequately coordinated supply chain risk management efforts or ensured that all relevant programs were involved in implementation efforts.

Notably, nearly all of the locations reviewed had developed site-specific standards for desktops and laptops. To its credit, the Office of Science told us that it plans to move its Federal personnel to a virtual desktop infrastructure that, according to officials, should result in IT hardware cost savings. In addition, officials recently updated the *Department of Energy Acquisition Guide* to emphasize the importance of strategic sourcing to reduce costs. Furthermore, the development of the Supply Chain Risk Management Resource Center by the

Office of the Chief Information Officer in October 2012 to focus on cybersecurity is a noteworthy accomplishment and a first step toward implementing an effective supply chain risk management process.

While these are positive actions, additional effort is necessary to ensure the Department effectively manages IT hardware acquisition and maintenance. As such, we have made recommendations that, if fully implemented, could help the Department realize potential savings of up to approximately \$6 million over the next 3 years at just the eight locations reviewed. These projected savings do not take into account the potential maintenance and support savings available through maintaining and ensuring cybersecurity protections are in place for commonly configured systems.

#### MANAGEMENT REACTION

Management concurred with the report's first three recommendations and partially concurred with the fourth recommendation. The Department indicated that it had taken or initiated actions to address issues identified during our review. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in Appendix 4.

#### Attachment

cc: Deputy Secretary  
Under Secretary for Nuclear Security  
Deputy Under Secretary for Management and Performance  
Deputy Under Secretary for Science and Energy  
Chief of Staff  
Acting Chief Information Officer  
Acting Chief Financial Officer  
Director, Office of Management

# AUDIT REPORT ON FOLLOW-UP ON THE DEPARTMENT OF ENERGY'S MANAGEMENT OF INFORMATION TECHNOLOGY HARDWARE

---

## TABLE OF CONTENTS

### Audit Report

Details of Finding ..... 1

Recommendations ..... 8

Management Response and Auditor Comments ..... 9

### Appendices

1. Potential Savings ..... 10

2. Objective, Scope and Methodology ..... 11

3. Related Reports ..... 13

4. Management Comments ..... 15

# FOLLOW-UP ON THE DEPARTMENT OF ENERGY'S MANAGEMENT OF INFORMATION TECHNOLOGY HARDWARE

---

## DETAILS OF FINDING

The Department of Energy (Department) had not effectively managed acquisition and maintenance of information technology (IT) hardware to reduce costs and ensure adequate security at the eight locations reviewed, including Headquarters. While we were unable to determine an exact amount spent on IT hardware because many organizations did not track such expenditures, we determined that just the sites reviewed spent more than \$45 million in Fiscal Year (FY) 2012 and estimated that the Department likely spent more than \$125 million on IT hardware such as servers, desktops, laptops and printers during the same period. Our findings revealed that the Department often deviated from established IT hardware standards and potentially paid over \$1.7 million more than necessary in FY 2012. In addition, prices paid for similar desktops and laptops varied significantly among sites, potentially costing the Department \$282,000 more than necessary. Furthermore, the Department had not developed and implemented an effective IT supply chain risk management program to protect its unclassified and national security systems and the information they process.

### Hardware Standards

Maximizing standardization of IT hardware is a key component to reducing costs associated with supporting end users. In addition to potential up-front cost savings, standardizing hardware for a large group of users, such as those supporting administrative functions, can significantly reduce maintenance costs and make deployment of system upgrades easier and less time consuming. Although seven of eight locations reviewed had developed site-specific standards for desktops and laptops, we found that several sites often deviated from those standards when acquiring IT hardware. Specifically, sites purchased outside of established hardware standards and/or standard configurations over 75 percent of the time, resulting in expenditures of up to about \$1.7 million more than necessary in FY 2012. For example:

- Based on information provided during our site visit, we found that Lawrence Berkeley National Laboratory (LBNL) purchased nonstandard administrative machines and/or configurations 100 percent of the time. Using purchase data provided by LBNL, we determined that the site routinely paid significantly more for administrative laptops and desktops than the price for a standard machine. The site paid about \$261,800 more than necessary for its administrative desktop and laptop computers in just the single year we reviewed. In our opinion, the practice of purchasing nonstandard machines essentially rendered the established standards meaningless. In addition, LBNL indicated that it did not establish standards for scientific users.
- Although Lawrence Livermore National Laboratory (LLNL) developed 21 different computing standards for desktops and laptops, we found that the vast majority of purchases at the site exceeded the recommended configuration for those standards, resulting in excessive costs for acquiring hardware. While the site paid an average of \$1,065 for a small number of standard desktops, we found that desktop purchases at

---

LLNL cost an average of \$1,662, or \$597 (56 percent) more than the standard. During FY 2012, these nonstandard purchases resulted in expenditures of up to nearly \$1.3 million more than necessary. In comments on our report, officials asserted that nearly all FY 2012 purchases met standards; however, we determined that their analysis was based only on the models purchased and did not account for potentially excessive configurations and costs.

- In contrast to LBNL, officials at Oak Ridge National Laboratory (ORNL) noted that before they developed computer standards for their scientific users, their researchers would purchase computers that were often in excess of what was needed and were thus more costly. By creating computer standards for researchers, officials noted they were able to reduce costs, improve cybersecurity and increase the amount of resources available for mission requirements, rather than spending unnecessary funds on personal preferences. Further, these officials stated that application of the computer standards to researchers had minimal affect on the researcher's ability to complete mission requirements.
- Despite what appeared to be prudent purchase standards, we found that ORNL deviated from the standards more than 80 percent of the time. ORNL officials told us that they had developed 20 different scientific and enterprise computing standards. However, the same officials indicated that the standards initially provided for our review were not accurate. While the site worked with its vendors to provide a more accurate listing, it was unable to provide sufficient evidence to support which standards were in place during FY 2012, the period we used to evaluate purchases.

Executive Order 13589, *Promoting Efficient Spending*, required each agency to establish a plan for reducing IT costs through methods such as limiting the number of IT devices, creating efficiencies through the effective implementation of technology and/or implementing appropriate agency-wide IT solutions that consolidate activities. Such improvements could be made by establishing and using hardware standards to reduce costs and ensure IT equipment is not unused and underused. However, as noted above, our findings indicated that had established standards been used, the Department could have saved up to \$1.7 million on laptop and desktop purchases in FY 2012 at five of the facility contractors included in our review. While we recognize that standard IT equipment cannot be used in every instance, the potential existed to significantly reduce costs by enforcing the use of established hardware standards.

## **Price Variations**

We found that Headquarters and sites paid widely varying prices for IT hardware products even though acquired equipment was similarly configured. Specifically, prices for similar desktops and laptops varied significantly from site to site, potentially costing the Department \$282,000 more than necessary. For instance, LBNL, Y-12 National Security Complex and LLNL each paid significantly more than ORNL for a desktop that was either minimally different or was less powerful. At LBNL, officials paid about \$130 (13 percent) more for essentially the same model desktop but with a slower processor and half the hard drive capacity and computer memory. As such, we estimated that LBNL, LLNL and the Y-12 National Security Complex could have

---

realized significant savings on similar machines had the sites made efforts to obtain similar pricing. While mission requirements could potentially affect hardware pricing, our analysis identified that the price variations occurred for hardware with consistently similar configurations.

In addition to varying prices between sites, we also found that officials paid differing costs for the same or similar computers within their own site. For example, LLNL paid three different prices throughout FY 2012 for the same desktop. Had LLNL effectively planned for the purchases and paid the lowest price during FY 2012, the site could have saved over \$26,000. Similarly, LBNL and LLNL could have realized additional savings by purchasing like laptops at the lowest available price. Although LLNL officials noted that price deviations may be due to market fluctuations, we found that LLNL paid 42 different prices ranging from approximately \$900 to over \$2,000 for one desktop model in FY 2012, as a result of varying configurations not included in the standard. Notably, LBNL officials commented that significant savings had been realized through easy-to-use, low-cost, blanket agreements with IT suppliers involving no interaction with procurement. However, we were unable to verify management's estimated savings based on documentation provided. In addition, LLNL officials commented that they had taken steps to consolidate IT purchases, including significantly reducing the number of hardware vendors and models. While these are positive steps, the issues identified are similar to those noted in our previous report on *Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007).

## Supply Chain Risk Management

The Department had taken a number of actions to address IT supply chain risk management. The goal of an effective supply chain risk management program is to establish procurement and cybersecurity related policies, processes and controls over vendors to help minimize security risks that could negatively affect operations. We found that the Office of the Chief Information Officer established the Supply Chain Risk Management Resource Center (Resource Center) in October 2012 to help deploy and sustain a security-based supply chain risk management program across the enterprise. Since its inception, the Resource Center has developed an action plan to help it reach full operating capability in FY 2016, provided supply chain management training to various organizations and completed various vendor assessments requested by programs and sites. In addition, officials updated the *Department of Energy Cyber Security Program* directive to include numerous considerations related to supply chain risk management that programs should include in their risk management implementation plans.

While these are positive actions, we identified that programs and contractors had not sufficiently addressed certain aspects of supply chain management, including issues related to security over IT hardware vendors and communication of threats and best practices among Department elements. Based on survey results and ongoing efforts, Office of the Chief Information Officer officials commented that none of the Department's major program elements had fully implemented an effective supply chain risk management program. We found:

- Four sites reviewed had not always developed and implemented a registration process to ensure equipment was not previously owned. Such a process should have involved verifying with vendors that equipment was not previously owned or used. For example, the Y-12 National Security Complex implemented a registration process only after the



---

site had received after-market equipment. In addition, vendors at the same four sites were occasionally responsible for modifying IT equipment prior to delivery, including imaging, property tagging and/or registering equipment for the sites. While these activities may provide benefits, we found that the sites had not always verified the activities, such as testing a sample of computer configurations or registrations, to ensure procurement and security requirements were met. Notably, Y-12 National Security Complex officials commented that they had taken action to improve supply chain management practices.

- All Federal agencies maintaining classified information were directed to implement the *National Industrial Security Program Operating Manual*, developed by the Department of Defense in February 2006, to ensure that, among other things, vendor-supplied equipment did not introduce anything detrimental to the classified environment. However, contrary to those requirements, a cybersecurity official at one site indicated that its vendor may have been aware that equipment would be placed into the classified environment, providing the potential for unauthorized modifications of equipment by the vendor prior to it being placed into operation. Notably, according to officials, LLNL and the Kansas City Plant had implemented measures to ensure vendors were unaware of the environment where IT hardware would be placed in an effort to protect unclassified and national security systems.
- The Department had not established an effective process to communicate supply chain management threats among programs and sites or ensure that independent supply chain management efforts were coordinated. Program and site officials told us that known supply chain management threats and/or vulnerabilities were not always communicated across programs and sites, thus preventing them from making fully informed decisions regarding hardware purchases. In addition, we found that potentially duplicative efforts existed related to supply chain management. Notably, LLNL maintained an effort to provide a more open communication process among IT, procurement, cybersecurity and counterintelligence officials, leading to a potentially more effective supply chain risk management program. In another instance, the Resource Center began a pilot project in June 2013 with one site to engage counterintelligence and IT personnel in reviewing a sample of the site's vendors as part of an IT supply chain management program.

As noted in the Government Accountability Office's report on *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks* (GAO-12-361, March 2012), agencies should develop an effective supply chain management program that includes monitoring compliance with program protection policies and procedures. In addition, we believe improved communication efforts and the sharing of threat information and experiences could reduce the likelihood of duplicative efforts and allow the Department to develop a more successful IT supply chain risk management program.

### **Standards Management, Implementation and Coordination**

The problems we identified occurred, in part, because the Department had not developed and implemented a fully effective approach to managing IT hardware. In particular, programs and

---

sites had not always developed and enforced hardware standards that met user needs or implemented procedures to ensure organizations and sites effectively coordinated acquisition efforts and fully leveraged enterprise-wide purchasing agreements. In addition, the issues related to supply chain risk management were caused by the Department's failure to fully develop and/or implement policies and procedures related to ensuring effective supply chain risk management and a lack of coordination among all relevant programs.

### **Standards and Acquisition Management**

The problems related to implementation of hardware standards occurred because sites had not always enforced previously developed standards. Based on our analysis of procurement data, we determined that users at LLNL routinely purchased computers that exceeded recommended configurations that were part of the standards. For example, users acquired over 1,000 desktops in FY 2012 that exceeded the site's established standards. In addition, LBNL officials indicated that while cost management is one goal of the Laboratory, it is not the only goal or the most important one related to IT hardware management. Although we agree that all factors must be considered, our test work revealed that there were few cost controls in place at LBNL related to hardware acquisition.

LBNL officials also commented that standard hardware is whatever is purchased in bulk and exists to support a set of identical or near-identical purchases for administrative users. However, we found that LBNL's bulk purchases only accounted for up to about 22 percent of desktops and laptops purchased in FY 2012. In addition, the cost of certain bulk purchases exceeded the established standards provided by officials at the time of our site visit. Furthermore, although LBNL officials stated that nonstandard equipment needed to be justified, our results identified that noncompliance with established standards was approved 100 percent of the time. While we understand that some deviations may be necessary and justified, developing hardware standards not only helps to achieve effective cost management, but it also facilitates hardware support and network security. We believe that the benefits could be more fully realized through the use of pre-established standards rather than establishing standards after hardware has already been purchased. Had an effective process been in place to manage standards, the Department could have reduced costs and potentially improved cybersecurity by minimizing the number of differing systems to secure.

Further, the Department had not developed and implemented policies and/or procedures to ensure organizations and sites effectively coordinated acquisition efforts and fully leveraged enterprise-wide purchasing agreements. Absent such policies and procedures, we found that 4 sites reviewed purchased 1 desktop model from 4 different contracts at 134 different prices in FY 2012. Even within sites, purchases were often not coordinated, resulting in significant price variations. In addition, although NNSA began efforts to coordinate contract terms for IT hardware through its Supply Chain Management Center, we noted that purchases continued to be made at the site level rather than through aggregated bulk purchase agreements to minimize costs. To maximize the Department's purchasing power, it is important to implement the use of enterprise-wide agreements to promote efficient and effective spending in accordance with Executive Order 13589, *Promoting Efficient Spending*.

---

## Supply Chain Risk

The issues related to supply chain risk management occurred, at least in part, because the Department had not fully developed and/or implemented policies and procedures related to ensuring effective supply chain risk management. In addition, programs and sites had not adequately coordinated supply chain risk management efforts or ensured that all relevant programs were involved in implementation efforts.

Department programs and sites had not updated and implemented their risk management implementation plans to incorporate supply chain risk management controls. For instance, program and site officials noted concerns related to the lack of implementing guidance for the Department's planned enterprise-wide supply chain risk management approach, which may have contributed to the lack of effective implementation. The lack of guidance also may have contributed to sites not implementing procedures to limit vendors' understanding of the environment where hardware would be placed or ensure appropriate registration of products to help avoid significant security risks. While various officials told us they were hesitant to implement supply chain risk management policies without appropriate guidance from the Office of the Chief Information Officer, we noted that the Department's current cybersecurity organization structure requires Senior Department Management to ensure that appropriate cybersecurity requirements are incorporated into risk management plans.

The Department also had not implemented adequate procedures to ensure that supply chain risk management activities were coordinated between all appropriate organizations. For instance, although various officials we spoke with and best practices indicated that effective IT supply chain management programs should be coordinated among IT, cybersecurity, procurement and counterintelligence personnel to achieve maximum protection, the Department had not established a mechanism or working group to include all necessary personnel. Without adequate coordination and communication, officials did not obtain a full understanding of sites' concerns related to coordination between procurement and cybersecurity organizations. As a result, supply chain management guidance had not been incorporated into procurement regulations related to purchasing IT hardware. We believe better coordination and communication could have provided programs and sites with an opportunity to express the same concerns to senior Department officials that they shared with us. A coordinated effort could also have enabled the Department to better understand how organizations and sites would benefit from a centralized supply chain management program and allocate limited resources appropriately.

### Other Matters

During the course of our review, we identified issues with the management of certain IT hardware contracts at LBNL. Specifically, we determined that two contracts, with combined values of nearly \$60 million, were awarded as sole-source contracts even though Federal regulations and best practices required that they should have been competed. Although LBNL officials told us that the contracts should have been awarded competitively, they had not taken action to compete the contracts at the time of our review. For one of the contracts, we determined that LBNL had spent nearly \$12 million even though the original award was based on acquisitions of up to \$4 million. We are concerned that without adequate competition, the Department may have paid more than necessary to acquire IT hardware at LBNL.

---

## Opportunities for Improvement

Without adequate actions to address the problems identified in this report, the Department may not realize potential cost savings of up to approximately \$6 million over the next 3 years at just the eight sites reviewed. These projected savings do not take into account the potential maintenance and support savings available through maintaining and ensuring cybersecurity protections are in place for commonly configured systems. Specifically, the Department may not realize savings through enforcement of IT hardware standards and leveraging bulk purchasing requirements for standard desktops and laptops used for nonscientific and/or research purposes. For example, we noted that the State of North Carolina recently realized savings of over 46 percent on laptops and desktops through the development of standards and subsequent bulk purchasing agreements. While we understand that a one-size-fits-all approach may not meet the objectives of the Department's varied missions, we believe that the Department could better utilize its bulk purchasing power to further decrease costs, thus realizing significant savings. In addition, without adequate management of its IT supply chain, the Department may not fully address the risk of compromise to its information systems and data and may be vulnerable to receiving suspect or counterfeit IT hardware.

---

## RECOMMENDATIONS

To improve IT hardware and supply chain risk management practices, we recommend that the Under Secretary for Nuclear Security, the Deputy Under Secretary for Science and Energy and the Deputy Under Secretary for Management and Performance, in coordination with the Department and National Nuclear Security Administration Chief Information Officers and the Director, Office of Management, as appropriate:

1. Ensure that appropriate IT hardware standards are developed and implemented and sites require valid justifications for deviating from the standards;
2. Coordinate IT hardware procurements among Headquarters and field sites, to the extent practical, to maximize potential cost savings; and
3. Develop and implement an effective supply chain risk management process that includes, among other things:
  - a. Adequate security and procurement policies and procedures for protecting the Department's IT supply chain, including updating and implementing supply chain management controls as part of the program element's risk management approach; and
  - b. Coordination of activities and communication of supply chain risks/threats and best practices among all appropriate organizations such as cybersecurity and procurement organizations.

To resolve contract management weaknesses and ensure that the site obtains the best value from vendors, we recommend that the Manager, Berkeley Site Office, direct Lawrence Berkeley National Laboratory to:

4. Review sole-source IT hardware-related contracts and compete them, as appropriate.

---

## MANAGEMENT RESPONSE

Management concurred with the report's first three recommendations and indicated that it had planned or initiated actions to address issues identified during our review. Management stated that it was working toward enhancing processes to ensure contractors and field sites justify and document deviations from IT hardware standards. In addition, management planned to develop procurement policy to emphasize the use of existing strategic procurement vehicles. Management also commented that it would continue to develop the Department's supply chain management program and that programs would update their risk management implementation plans accordingly. Notably, while the Office of Science commented that it had enhanced governance over Federal users, officials did not fully agree that more standardization was needed or that the Department spent more than necessary acquiring IT hardware.

In separate comments, LBNL partially concurred with our recommendation to review sole-source IT hardware-related contracts and compete them, as appropriate. Management stated that it is required to follow site-level procurement policy and that a valid sole-source justification existed for the contracts reviewed related to meeting small business goals. Management commented that it planned to issue competitive requests for IT contracts pending implementation of an electronic commerce system.

## AUDITOR COMMENTS

Management's comments and planned actions were generally responsive to our recommendations. For instance, management's commitment to develop a policy that emphasizes the use of strategic procurements as part of acquisition planning should, if implemented across the Department, help to remediate some of the issues identified in our report. The Department's continued efforts to enhance procurement practices should also help to minimize duplication and avoid expensive costs of issuing new contract vehicles. Contrary to comments made by the Office of Science, our report identified that opportunities existed to increase standardization and reduce costs. For example, although hardware standards had been established, sites did not always use them when acquiring IT hardware.

In regards to LBNL's comments, while we understand that small business goals exist, we do not agree with LBNL's assertion that the contracts were properly awarded. Specifically, LBNL's actions were inconsistent with fair and open competition requirements and best practices. In our opinion, LBNL's need to meet identified goals for awarding contracts to small businesses could have been met through fair and open competition rather than issuing sole-source contracts for commercial IT hardware equipment. In addition, the significant expenditures under the contracts reviewed highlighted the need to ensure the contracts were competitively awarded. Management's planned corrective actions, if fully implemented, should address the acquisition weaknesses identified in our report. Management's comments are included in Appendix 4.

**POTENTIAL SAVINGS**

We calculated the savings that the Department of Energy (Department) could have realized in Fiscal Year (FY) 2012 at the eight locations reviewed by acquiring desktops and laptops at the lowest prices available through other existing agreements. In particular, we compared the pricing of the same models and specific configurations of four desktops and four laptops at Headquarters and sites reviewed. Based on our analysis, we estimated that the Department could realize potential savings of over \$846,000 over the next 3 years at just the sites reviewed by ensuring it purchases these desktops and laptops at the lowest available prices.

We also reviewed the eight locations, five of which purchased outside the established site-specific hardware standards, to determine potential savings that could be achieved by enforcing standards for information technology hardware across the Department. Specifically, we analyzed the FY 2012 desktop and laptop purchases to determine whether the Department could have realized savings by procuring within site standards as recommended. Based on our calculations, we estimated that the Department could realize potential savings of over \$5.1 million over the next 3 years at just the sites reviewed through better enforcement of standards. These projected savings do not take into account the potential maintenance and support savings available through maintaining and ensuring cybersecurity protections are in place for commonly configured systems.

Due to the dollar thresholds sites used to track items and the limited information available regarding purchase details, we were unable to calculate savings for items such as printers and other peripherals. The table below summarizes the total estimated potential savings of \$5,971,353 that the Department could realize over the next 3 years at just the eight sites reviewed through more effective management of its information technology hardware.

|                                 | <b>Identified Fiscal Year<br/>2012 Savings</b> | <b>Potential Savings<br/>(3 years)</b> |
|---------------------------------|--|--|
| <b>Varied Pricing</b>           |  |  |
| Desktop                         | \$219,807                                      | \$659,421                              |
| Laptops                         | \$62,314                                       | \$186,942                              |
| <b>SUBTOTAL</b>                 | <b>\$282,121</b>                               | <b>\$846,363</b>                       |
| <b>Deviation from Standards</b> |  |  |
| Desktop                         | \$1,631,570                                    | \$4,894,710                            |
| Laptop                          | \$76,760                                       | \$230,280                              |
| <b>SUBTOTAL</b>                 | <b>\$1,708,330</b>                             | <b>\$5,124,990</b>                     |
| <b>TOTAL SAVINGS</b>            | <b>\$1,990,451</b>                             | <b>\$5,971,353</b>                     |

## **OBJECTIVE, SCOPE AND METHODOLOGY**

### **Objective**

To determine whether the Department of Energy (Department) effectively managed the acquisition and maintenance of information technology (IT) hardware.

### **Scope**

This audit was performed between December 2012 and October 2014, at Department Headquarters in Washington, DC, and Germantown, Maryland; Lawrence Livermore National Laboratory in Livermore, California; Lawrence Berkeley National Laboratory in Berkeley, California; the Kansas City Plant in Kansas City, Missouri; and Oak Ridge National Laboratory, Oak Ridge Office, East Tennessee Technology Park and the Y-12 National Security Complex in Oak Ridge, Tennessee. The audit was conducted under Office of Inspector General Project Number A13TG014.

For our review, we utilized the National Institute of Standards and Technology's definition of supply chain and IT. Specifically, the National Institute of Standards and Technology identified supply chain as a set of organizations, people, activities, information and resources for creating and moving a product or service from suppliers through to an organization's customers. This review specifically focused on the security aspects of supply chain management rather than the logistical. In addition, the National Institute of Standards and Technology defined IT as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. This includes, among other things, computers, software, firmware and services (including support services). Our review was limited to IT hardware—primarily desktops and laptops. Information pertaining to mobile devices and software was considered under separate engagements.

### **Methodology**

To accomplish the audit objective, we judgmentally selected a sample of eight Department locations, including Headquarters, at which to conduct test work. This selection was based on the IT budget at the locations, information obtained during interviews with Headquarters officials and the need to follow up on prior reports. Additionally, we:

- Reviewed Federal regulations, Department directives, Office of Management and Budget guidance, and other policies and guidance pertaining to IT hardware and IT supply chain management.
- Reviewed prior reports issued by the Office of Inspector General and the U.S. Government Accountability Office and corrective actions taken in response to those reports.



- Reviewed numerous documents related to the Department's management of IT hardware acquisition and maintenance activities to determine whether potential cost savings opportunities existed.
- Evaluated the roles, responsibilities and costs associated with IT hardware and supply chain management. We also examined best practices in use at other government agencies regarding the management of IT hardware acquisition and maintenance and supply chain management.
- Determined whether organizations and sites established performance metrics and goals specific to management of IT hardware acquisition and maintenance and supply chain management.
- Held discussions with program officials and personnel from Department Headquarters and field sites reviewed, including representatives from the Offices of the Chief Information Officer, Environmental Management, Science and Fossil Energy, as well as the National Nuclear Security Administration.

To calculate potential savings, we reviewed purchasing and inventory data available to identify costs associated with IT hardware purchased during Fiscal Year (FY) 2012. Using computer-assisted audit techniques, we identified patterns in hardware purchases. Additional configuration information was obtained from organizations and sites to allow us to make specific comparisons among purchases. For example, when identifying a difference in price between two sites for a specific desktop model, information was obtained to determine if such differences were the result of additional components.

We conducted this performance 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 the evidence obtained provides a reasonable basis for our findings and conclusions 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 not established performance measures for managing IT hardware and/or the IT supply chain. 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 solely rely on computer-processed data to satisfy our objective. However, we used data analysis software to evaluate IT hardware inventories and cost details provided by organizations and sites for FY 2012. We obtained the data in electronic format and used computer-assisted audit techniques to identify patterns and anomalies. This included compiling all available inventories into one spreadsheet for each organization and site. We combined all available data and analyzed by type (e.g., desktop, laptop, etc.) to identify significant purchases made throughout the organizations and sites reviewed. We validated the data by reviewing a sample of purchase orders and computer configurations.

An exit conference was held with Berkeley Site Office officials on October 21, 2014. Department management waived an exit conference.

---

## RELATED REPORTS

### Office of Inspector General Reports

- Audit Report on [\*Management of Bonneville Power Administration's Information Technology Program\*](#) (DOE/IG-0861, March 2012). The audit identified concerns in the areas of cybersecurity, project management and procurement of information technology (IT) resources. Specifically, the report noted instances where the supply chain organization purchased software that did not conform to organizational standards. The issues identified were due, at least in part, to inadequate implementation of policies and procedures related to security and project management. Further, we found that Bonneville Power Administration's Office of the Chief Information Officer did not have authority over the entire IT program, including certain cybersecurity and procurement functions. Management concurred with the report's recommendations and indicated that corrective actions would be taken.
- Audit Report on [\*The Office of Science's Management of Information Technology Resources\*](#) (DOE/IG-0831, November 2009). The audit found that the Office of Science had taken a number of actions to improve its cybersecurity posture and align its program to Federal requirements. However, the Office of Science had not taken some basic steps to enhance security and reduce costs. The identified weaknesses were attributed, in part, to a lack of policies and procedures for ensuring effective cybersecurity and hardware acquisition practices. In addition, the Office of Science had not effectively monitored the performance of its field sites to ensure that previously reported internal control weaknesses were addressed and had not implemented an appropriate mechanism to track its IT-related costs. Management generally concurred with the recommendations but did not concur with the recommendation that it evaluate joining the Department of Energy's (Department) common IT environment. Management indicated that it planned to address many of the issues identified in the report.
- Audit Report on [\*Facility Contractor Acquisition and Management of Information Technology Hardware\*](#) (DOE/IG-0768, June 2007). We found that certain Department facility contractors had not adequately managed the acquisition and control of IT hardware. A number of contractors had not consistently taken advantage of opportunities to reduce acquisition and support costs, address security concerns related to aging systems or ensure that accountability was maintained over sensitive computers and devices. These problems occurred because the Department had not developed a coordinated approach to IT hardware acquisition, management and control. Management concurred that action is necessary to improve the Department's practices for acquiring commodity-type IT hardware.

### Government Accountability Office Report

- Report on [\*IT Supply Chain: National Security-Related Agencies Need to Better Address Risks\*](#) (GAO-12-361, March 2012). The report noted that reliance on global supply chain introduces multiple risks to Federal information systems. Specifically, the report

identified threats to the IT supply chain that can adversely affect an agency's ability to effectively carry out its mission. The Department had acknowledged these threats; however, it had not yet defined supply chain protection measures for information systems and was not in a position to have implementing procedures or monitoring capabilities to verify compliance with and effectiveness of any such measures. The Department was concerned that many of the Government Accountability Office's conclusions may have underestimated the deep complexities and interdependencies posed by this threat but concurred with the spirit of the recommendations.

## MANAGEMENT COMMENTS



Department of Energy

Washington, DC 20585

September 12, 2014

MEMORANDUM FOR RICKEY HASS

DEPUTY INSPECTOR GENERAL  
FOR AUDITS AND INSPECTIONS  
OFFICE OF INSPECTOR GENERAL

FROM:

DONALD E. ADCOCK   
CHIEF INFORMATION OFFICER, ACTING

SUBJECT:

Draft Report, "Follow-up on the Department of Energy's  
Management of Information Technology Hardware" (A13TG014)

Thank you for the opportunity to comment on the subject draft report. The Department of Energy (DOE) recognizes that the Inspector General's (IG) objective in this review was to determine whether DOE effectively managed the acquisition and maintenance of information technology (IT) hardware. We appreciate the IG's efforts to review our programs.

Departmental Programs and Offices contributed to the management response to the specific recommendations in the draft report as outlined below. Program-specific plans of action and technical comments are included in the attachments.

**Recommendation 1:** *Ensure that appropriate IT hardware standards are developed and implemented and sites require valid justifications for deviating from the standards.*

**Management Response:** Concur.

The Department concurs with the recommendation that deviations from IT hardware standards should require valid and documented justifications. However, the Department believes that the Program Secretarial Offices (PSOs) should be responsible for putting mechanisms in place that establish standards appropriate to their mission.

The IG's recommendation has already been implemented within the DOE Federal environment, which includes direct support contractors. Existing DOE and National Nuclear Security Administration (NNSA) policy includes guidance to the sites to use applicable hardware standards in the development of new systems but does permit risk-based for existing systems. DOE policy, 205.1B, *Department of Energy Cyber Security Program*, references a broad range of guidance such as NIST Special Publications and Federal Information Processing Standards. These publications afford DOE a comprehensive selection of approaches. Existing contracts and missions can dictate the type of equipment being purchased and replaced in order to prevent mission compromise



Printed with soy ink on recycled paper

or compliance with existing contract provisions. Our view is that no further action is required to create new standards in light of DOE and NNSA policy. Some PSOs are enhancing processes to ensure that contractor and field sites justify and document deviations from IT hardware standards, based on the site's requirements. Specific actions are outlined in the attachments.

**Estimated Completion Date:** July 31, 2015.

**Recommendation 2:** *Coordinate IT hardware procurements among Headquarters and field sites, to the extent practical, to maximize potential cost savings.*

**Management Response:** Concur.

The Department's Office of Acquisition and Project Management (MA-60) will develop policy that requires an order of preference in creating new procurements that emphasizes the use of existing strategic procurement vehicles as part of the procurement planning process. Strategic procurement planning includes both (i) evaluating the suitability of known existing vehicles before creating new agency-specific vehicles to avoid expensive and inefficient duplication and (ii) determining the best ways to create new vehicles where there is a void or insufficient choice. These actions require an ongoing commitment of time and resources. Accordingly, to ensure that the expected return from investment in a new contract or agreement is worth the effort and cost associated with planning, awarding, and managing a new vehicle, business cases for contracts and blanket purchase agreements will be required for any new procurements that do not use an existing procurement vehicle when one is available for that commodity. The estimated completion date for policy to be posted/distributed is August 29, 2014.

It should also be noted that the National Nuclear Security Administration began efforts to coordinate contract terms for IT hardware. These efforts are not reflected in the FY12 financial data collected since the coordination began in FY13 and as implemented business processes have continued to evolve since then. With the establishment of the Kansas City Plant's Supply Chain Management Center, NNSA has addressed this recommendation and considers it closed for NNSA.

**Recommendation 3:** *Develop and implement an effective supply chain risk management process that includes, among other things:*

- a) *Adequate security and procurements policies and procedures for protecting the Department IT supply chain, including updating and implementing supply chain management controls as part of the program element's risk management approach; and*
- b) *Coordination of activities and communication of supply chain risks/threats and best practices among all appropriate organizations such as cybersecurity and procurement organizations.*

**Management Response, 3a: Concur**

Policy and guidance for supply chain risk management has been and continues to be developed. In 2012 the Government Accountability Office (GAO) recommended that DOE begin aggressively addressing information and communications technology (ICT) supply chain threats by formalizing an enterprise program through Departmental policy, procedures, and monitoring. In October 2012, the Office of the Chief Information Officer (OCIO) launched the Enterprise Supply Chain Risk Management (eSCRM) Program by establishing a Departmental “focal point,” the Resource Center, to address ICT supply chain concerns and meet the recommendations in GAO’s report<sup>1</sup>. The Resource Center (SCRM-RC) coordinates development of policy and implementing guidance, administers programs for education and information-sharing, provides vendor and product risk assessment capabilities, and will monitor the overall effectiveness of supply chain risk management (SCRM) activities across the Department, including the National Nuclear Security Administration (NNSA). The PSOs are updating their risk management implementation plans in accord with the requirements in DOE O 205.1B.

**Estimated Completion Date:** June 30, 2015

**Management Response, 3b: Concur.**

The Committee on National Security Systems Directive (CNSSD) 505, *Supply Chain Risk Management*, directs all Agencies that operate National Security Systems, including DOE, to develop Agency-level policy and programs and deploy standard practices. DOE completed the initial strategic framework for the eSCRM in January 2013 and reached initial operating capability in July 2013. Since the launch of the Resource Center, the OCIO has steadily progressed towards providing SCRM support Department-wide, including amending DOE Order 205.1B (Change 2, issued March 2013). This policy establishes program requirements to incorporate ICT SCRM considerations into the Risk Management Implementation Plans of Program Secretarial Offices, identifies ICT SCRM leadership roles and responsibilities, defines ICT SCRM organizational structure, and provides program focus on ICT product integrity.

The enterprise program is on track to complete implementation of the OCIO responsibilities in the revised Order and achieve full operational capability by 3<sup>rd</sup> Quarter 2016, which is in advance of the Fiscal Year (FY) 2018 deadline required by CNSSD 505.

For FY 2014 and the first two quarters of FY 2015, this project is focused on standing up a developmental open source threat assessment capability to streamline the supplier management process and provide open source threat support to program managers. The Resource Center will continue to support the development of program-level policy as directed by DOE O 205.1B and develop execution strategies for supply chain management activities across the enterprise.

<sup>1</sup> GAO-12-361, *IT SUPPLY CHAIN: National Security-related Agencies Need To Better Address Risks*, published March 23, 2012

**Estimated completion date:** 3<sup>rd</sup> Quarter FY 2016.

Please note that Recommendation 4 will be addressed under separate cover by the Manager, Berkeley Site Office.

If you have any questions regarding this response, please contact me on 202-586-0166.

Attachments

1. Program-specific Actions
2. Technical Comments

## **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](mailto: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.