



U.S. Department of Energy  
Office of Inspector General  
Office of Audit Services

# Audit Report

---


The Office of Science's  
Management of Information  
Technology Resources



**Department of Energy**  
Washington, DC 20585

November 20, 2009

MEMORANDUM FOR THE SECRETARY

FROM:   
Gregory H. Friedman  
Inspector General

SUBJECT: Audit Report on "The Office of Science's Management of Information Technology Resources"

BACKGROUND

The Department of Energy's Office of Science (Science) and its facility contractors are aggressive users of information technology (IT) to support fundamental research in areas such as energy, environmental remediation and computational sciences. Of its \$4 billion Fiscal Year 2008 budget, Science spent about \$287 million to manage its IT program. This included cyber security activities, acquisition of hardware and software, and support service costs used to maintain the operating environments necessary to support the missions of the program.

Prior Office of Inspector General reports have identified various issues with Science's management of its IT programs and resources. For instance, our report on *Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007) noted that the Science sites reviewed spent more than necessary when acquiring IT hardware. In another example, our review of *The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007) disclosed that Science's reluctance to adopt the Department of Energy Common Operating Environment (DOE-COE) at Headquarters contributed to the Department's inability to fully realize potential cost savings through consolidation and economies of scale. In light of the magnitude of the Office of Science IT program and previously identified program weaknesses, we initiated this audit to determine whether Science adequately managed its IT resources.

RESULTS OF AUDIT

Science had taken a number of actions to improve its cyber security posture and align its program to Federal requirements. Yet, our review disclosed that it had not taken some basic steps to enhance security and reduce costs. In particular, we found that:

- For their non-scientific computing environments, all seven of the field sites reviewed (two Federal, five contractor) had implemented security configurations that were less stringent than those included in the Federal Desktop Core Configuration. This configuration was designed by the National Institute of Standards and Technology and its use was mandated by the Office of Management and Budget;

- Although we previously highlighted weaknesses and recommended corrective actions, Science still had not fully established or enforced IT hardware standards for acquiring hardware such as desktop and laptop computers or related peripherals, contributing to significant unnecessary expenditures; and,
- While we have noted in a series of past reports that significant savings could be realized from aggregating demand for IT services and products across the enterprise, Science had not implemented a common infrastructure for users at its Federal sites and continued to maintain an IT environment independent of the Department's Common IT Operating Environment.

The weaknesses identified were attributable, at least in part, to a lack of adequate policies and procedures for ensuring effective cyber security and hardware acquisition practices. In addition, 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.

Without improvements, Science may be unable to realize the benefits of improved security over its information systems, reduce costs associated with hardware acquisition, and lower IT support costs through consolidation of services. In particular, we determined that Science could potentially realize savings of more than \$3.3 million over the next three years by better controlling hardware costs and implementing standards for certain equipment. Furthermore, Science could continue to pay for duplicative IT support services and fail to take advantage of opportunities to lower costs and apply potential savings to mission-related work.

During the course of our audit work, we learned from Science officials that they had initiated the process of revising the Program Cyber Security Plan to better clarify its policy for implementing Federal cyber security requirements. In addition, we noted that the Oak Ridge National Laboratory had taken action to establish and enforce hardware standards on both its administrative and scientific workforce. Although these actions are positive steps, additional action is needed to strengthen Science's IT program. To that end, our report contains several recommendations that, if fully implemented, should help Science improve the management of its IT resources.

### MANAGEMENT REACTION

Management generally concurred with the first three recommendations, but did not concur with our recommendation that it evaluate joining the Department's common IT environment. Management indicated that it planned to address many of the issues identified in our report. However, management believed that its decision not to participate in DOE-COE was appropriately justified. Management's comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary  
Chief of Staff  
Under Secretary for Science  
Chief Information Officer

# **REPORT ON THE OFFICE OF SCIENCE'S MANAGEMENT OF INFORMATION TECHNOLOGY RESOURCES**

---

## **TABLE OF CONTENTS**

### **Science Information Technology Management Program**

Details of Finding .....	1
Recommendations and Comments.....	10

### **Appendices**

1. Objective, Scope, and Methodology .....	13
2. Prior Reports.....	15
3. Management Comments .....	16

## Science Information Technology Management Program

### **Management of Information Technology Resources**

The Office of Science (Science) had dedicated \$287 million in Fiscal Year (FY) 2008 to information technology (IT) activities including, among other things, cyber security activities, acquisition of IT hardware and software, and maintaining IT services necessary to support the missions of the program. However, our review of seven sites and Headquarters disclosed that Science had not adequately managed its IT resources. In particular, we found that none of the sites reviewed had fully implemented the Office of Management and Budget's (OMB) mandated initiative for enhancing security configurations on their information systems. In addition, Science had not always established or enforced IT hardware standards and it spent significantly more than necessary to acquire hardware. Furthermore, Science had not implemented a common support services infrastructure for users at its Federal sites and continued to maintain an IT environment independent of the Department of Energy Common Operating Environment (DOE-COE).

#### Secure System Configurations

The Federal Desktop Core Configuration (FDCC) was designed by the National Institute of Standards and Technology (NIST) to improve overall cyber security and reduce IT costs at Federal agencies. We recognize that FDCC is only one part of an organization's strong defense-in-depth program. However, despite the benefits of FDCC and the OMB mandate to either implement FDCC settings on agency systems by February 1, 2008, or document why deviations from the settings were necessary, all seven field sites reviewed had implemented security configuration settings that were less stringent than those required by the FDCC. In addition, although Science Headquarters had documented its rationale for deviating from the FDCC configuration, none of the seven field sites had identified and documented their deviations, as required.

While six of seven field sites reviewed had implemented security configurations that were based on benchmarks developed by the widely recognized Center for Internet Security (CIS), we found that all seven of the sites had established configuration settings such as password settings, audit policy changes, encryption settings, or logon controls, that were less stringent than required by the FDCC. For example:

- 
- The Oak Ridge National Laboratory (ORNL) had developed its own security configuration standard that was not based on a nationally recognized standard such as those developed by CIS or NIST. As such, the site's standard configuration settings conformed to less than 50 percent of FDCC requirements. For instance, although the FDCC required that encryption algorithms compliant with the Federal Information Processing Standards issued by NIST be used, ORNL had not defined this setting in its minimum security configuration standards. Notably, ORNL officials recognized the need for more secure configurations and had begun piloting the FDCC settings on 500, or more than 20 percent, of its administrative desktops;
  - At the Fermi National Accelerator Laboratory (FNAL), 17 of 36 desktop configuration settings sampled were less rigorous than required by the FDCC. For example, FNAL did not log successful changes to its system audit policies even though the FDCC required that an audit entry be generated when a change to user rights or audit policies was successful, an action that could help detect unauthorized access to systems and data; and,
  - At Lawrence Berkeley National Laboratory (LBNL), there were 168 instances where LBNL's established configuration settings differed from those required by the FDCC. Although certain of the differences may have enhanced security, 18 of 36 settings sampled were less stringent than FDCC, including the requirement to rename default settings for system administrator and guest accounts. Leaving the default system administrator account name unchanged increases the risk that an attacker or unauthorized user could successfully log on to the system.

Although deviations to configuration settings are necessary to account for varying operational environments such as research and development, OMB instructed agency Chief Information Officers to provide NIST with documentation of any deviations from the FDCC configurations and the rationale for doing so. However, we found that none of the seven field sites reviewed had met this requirement. For example, officials at five sites noted that since the use of FDCC settings was not required by the Science Program Cyber Security Plan (PCSP), they had not taken action to review the FDCC requirements and, therefore,

---

had not documented the rationale to deviate. Although Science had taken positive steps to strengthen IT security by correcting cyber security weaknesses identified by various assessments, we noted that successful implementation of the FDCC settings should help to further strengthen its security posture by reducing opportunities for hackers to access and exploit the program's systems. In addition, the use of readily available and easily implemented security settings such as those in the FDCC can help reduce the risk of compromise without, in most cases, adversely impacting the program's mission.

### IT Hardware Acquisition

Our prior report on *Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007) highlighted several issues and provided recommendations to improve management of IT hardware acquisition within the Department. In response to our recommendations, Science officials issued a memorandum in March 2008 directing field sites to establish IT hardware standards and utilize such standards to streamline acquisitions. However, we found that Science still had not implemented a fully effective process for acquiring IT hardware. In particular, Science had not always established and enforced IT hardware standards – such as system configuration and acquisition standards – for desktop and laptop computers or related peripherals, resulting in higher than necessary expenditures.

We found that system configuration standards and the prices paid for desktop and laptop computers and related peripheral equipment varied widely at the sites reviewed. Specifically, the average price paid for a desktop computer ranged from \$1,628 to \$2,814 at the five laboratories reviewed, a price variance of 73 percent. At FNAL and the SLAC National Accelerator Laboratory (SLAC), neither of which had developed standards for desktop computers, average prices were \$1,677 and \$2,814, respectively. Notably, SLAC offered to its users a customizable website recommending particular desktop and laptop models. However, users were able to configure their requested computers with a wide variety of additional accessories and options, effectively diminishing the benefits of using more standardized configurations.

Similar to findings noted in our prior report, we determined that the lack of common hardware standards for desktops and laptops contributed to an overall variance of \$2.7 million in



---

acquisition costs over the past three years. In addition, five of seven sites reviewed had not established standards for IT peripheral equipment such as monitors and printers. At SLAC, prices paid for computer monitors that were the same or similar to one another ranged from \$256 to \$1,236. While SLAC officials disclosed that the average prices paid for three different sizes of monitors ranged from \$239 to \$289, acquisition data provided by the site demonstrated that the actual average prices paid were higher than this for all three sizes. In total, we found that the four facility contractor sites reviewed could have saved over \$125,000 in FY 2008 by enforcing standards for computer monitors.

Even when sites had developed standards for IT hardware, such standards were not always enforced. For instance, although Argonne National Laboratory (ANL) established only one recommended brand for its standard desktop and laptop computers, we found that the laboratory had purchased computers from 24 manufacturers over the past year. As noted in our prior report and numerous industry best practices, adherence to existing standards and the elimination of multiple brands and models of computers has the potential to significantly reduce support costs related to maintenance and cyber security.

LBNL limited the application of its established desktop and laptop standards to only a small group of administrative personnel and not to the larger scientific workforce. In particular, even though there were 5 recommended models of computers, we noted that over 25 different models were purchased in FY 2008. An official at the site informed us that this condition existed because the hardware needs differed from project to project. While we agree that needs may vary, we noted that ORNL – which has scientific projects similar to LBNL – established hardware standards and enforced them on both its administrative and scientific workforce. Officials at ORNL informed us that while the site allows for limited exceptions to their standards, employees are required to follow a rigid process to justify the purchase of non-standard hardware.

#### IT Support Services

Science had not implemented a common infrastructure for users at its Federal sites and continued to maintain an IT environment independent of DOE-COE. In particular, each of

---

Science's three primary Federal sites implemented IT infrastructures independent of one another. In addition, Science maintained its reluctance to migrate to DOE-COE – the Department's shared IT environment – an environment that was designed to decrease costs, improve security, and enhance user satisfaction. In short, Science maintained a bifurcated IT infrastructure that did not take advantage of opportunities to eliminate duplication. In addition, program officials had not appropriately tracked the costs to support Federal users to help ensure they were providing IT support services at the lowest costs.

Despite having similar missions and computing requirements, each of Science's three primary Federal sites at the Oak Ridge Office (Oak Ridge), Chicago Office (Chicago), and Headquarters had implemented IT support solutions independent of one another. Although Science had the opportunity to consolidate its Federal IT environment to leverage potential cost savings, each of the three locations utilized a different contractor to manage support services such as helpdesk support, operated different IT infrastructures, and purchased hardware and software from different vendors. In particular, while opportunities existed for the three support centers to integrate functions such as email infrastructures and file servers, they each managed their own services at varying costs.

In addition, each of the Science Federal facilities utilized different contractors to support their helpdesk functions, offsetting any potential savings that could have been realized through consolidation. Each of the three Federal sites also utilized different hardware and varying methods to acquire the hardware. For instance, the average price of hardware for a desktop package acquired in FY 2008 was \$1,472 at Chicago, but only \$783 at Headquarters. Oak Ridge chose to lease its desktop package at a cost of about \$1,160 over a four-year period rather than purchase equipment as the rest of the Federal community had done. By consolidating into a single, integrated IT infrastructure similar to other efforts such as DOE-COE, it is likely that Science could realize reduced IT costs through economies of scale, allowing for easier management of its infrastructure, and potentially enhancing its overall security posture.

While Science chose not to consolidate its Federal IT environments, we found that the program was unable to

---

document the true cost of providing IT support services to its Federal users. Specifically, each of the three Federal facilities reviewed tracked their support costs differently, making it virtually impossible to compare the actual cost of supporting a user. For instance, the reported monthly costs per user ranged from \$172 at Chicago to \$351 at Oak Ridge. However, we noted that Chicago had not included costs related to items such as cyber security and network infrastructure in its calculations. IT officials at Chicago commented that an attempt was made to calculate IT support costs, but they were unable to conclude what the true cost per user was. In addition, we found that Science Headquarters excluded costs for items such as network administration and security monitoring software in its calculation.

Absent effective cost tracking, Science's methodology for calculating IT support costs did not adequately support its decision not to migrate to DOE-COE. Specifically, Science disclosed that it calculated, based on DOE-COE cost categories, the full-cost of its IT support program to be \$203 per user per month at Headquarters as compared to \$300 charged by the Office of the Chief Information Officer (OCIO) under DOE-COE. However, as previously noted above, we found that certain cost elements such as network administration and security monitoring software were excluded from Science's cost calculation. Based on available supporting documentation reviewed, we determined that the actual cost paid for each Science user at Headquarters could be as much as \$350 each month, or 17 percent more than DOE-COE. Our calculations were based on information reported by Science to OMB in the Department's Exhibit 53, as well as services worth about \$52 per month per user that were provided to Science, but were subsidized by the OCIO. Although Science officials commented that they did not utilize all of the services provided by the OCIO such as firewall operations and maintenance, email filtering, and patch management, they did not notify the OCIO so that these services could be discontinued. In addition, Science planned to independently acquire many of the same services already provided by the OCIO, potentially increasing costs for the Department.

Contrary to the information noted above, Science officials disclosed in preliminary comments to our report that they continued to believe the program's costs for IT support services and needed hardware were lower than DOE-COE. However, even if Science was able to successfully calculate the full-cost,

---

continuing its stand-alone position may not be advantageous to the Department. As we have noted in a series of past reports related to consolidation of IT services and products, significant savings could have been realized from aggregating demand across the enterprise. For instance, our report on *The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007) disclosed that organizations' reluctance to participate in DOE-COE prevented the Department from realizing significant savings through consolidation of common infrastructures. Realizing these goals should, if properly executed, help to eliminate redundancy at Headquarters and other locations and further increase savings in a truly enterprise-wide DOE-COE environment.

## **Policies and Performance Monitoring**

These problems occurred because Science had not developed adequate policies and procedures relevant to implementing the FDCC and acquiring IT hardware. In addition, Science had not effectively monitored the performance of its program elements and had not implemented an appropriate mechanism to track IT related costs.

### Policies and Procedures

Science Headquarters and its field sites had not developed adequate policies and procedures for ensuring effective implementation of the FDCC and IT hardware acquisition practices. Specifically, Science had not incorporated into its PCSP or site-level contracts the Federal requirement for implementing FDCC configurations. While Science officials directed field sites, through the management and operating contracts, to utilize security configurations such as the FDCC in all IT acquisitions, we found that the direction was neither adequate nor followed by sites. In particular, the direction required that the FDCC be applied to new IT acquisitions, but it did not apply to computers acquired before the direction was issued. In addition, the direction did not address the need to document risk-based decisions to deviate from the FDCC, a key requirement of OMB. Furthermore, we found that although the purpose of the PCSP is to identify cyber security requirements for Science and provide a consistent method of ensuring security of information and systems across the program, officials at five of seven field sites noted that the FDCC was not required in the PCSP or site-level contracts, and therefore it was not implemented in their environments.

---

Additionally, Science had not developed and implemented policies requiring establishment and enforcement of hardware standards, and coordination of IT hardware purchases both within the program, and across the Department. The lack of such a policy resulted in an uncoordinated approach to acquisition of hardware and support services at the sites reviewed. Notably, Science officials disclosed that they had initiated changes to the PCSP to provide more guidance on Federal requirements and two of the sites reviewed had initiated testing of the FDCC settings in their environment.

#### Monitoring Performance and Costs

Science Headquarters had not adequately monitored performance to ensure that prior recommendations made by the Office of Inspector General were addressed and had not implemented a process to track IT-related costs. In particular, despite prior recommendations that the Department, including Science, develop and implement hardware standards and utilize such standards to streamline acquisitions, officials had not ensured that these recommendations were adequately addressed. For instance, an official at LBNL commented that his site did not concur with the findings raised in the previous audit, and therefore had not implemented any of the recommendations. However, the LBNL official also noted that the site had implemented certain cost savings measures such as an automated system for purchasing hardware. Similarly, our review of *The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007) recommended that the Department complete migration of program elements to DOE-COE. At the time, a request from Science for a waiver on migration was disapproved by the then Deputy Secretary, but Science has continued to resist. Although program officials noted that a waiver was subsequently granted in February 2008, they were unable to provide documentation to support this statement.

Officials also had not implemented a process to effectively capture the total cost of providing IT support services. As noted earlier, each of the three Federal sites reviewed tracked their costs differently, effectively eliminating the ability to compare the costs of the programs and determine whether they were successful based on the amount of funds expended. Furthermore, the lack of adequate cost information prevented the program from developing a cost-benefit analysis to determine whether migration to DOE-COE would be

---

advantageous. Although Science Headquarters attempted to align its costs categories with DOE-COE for comparison purposes, neither Chicago nor Oak Ridge was able to provide similar comparisons. Without a consistent methodology, both the OCIO and Science were unable to determine who could provide a more efficient IT support solution.

### **Information Security and Cost Savings Opportunities**

Absent an effective IT management program, Science may be unable to realize the benefits of improved security over its information systems, reduce costs associated with hardware acquisition, and lower IT support costs. For instance, according to an analysis conducted by the National Security Agency, as many as 90 percent of all vulnerabilities can be eliminated through up-to-date patching and implementation of secure configurations such as those included in the FDCC. In addition, the Office of Health, Safety and Security recently completed a review of Science sites that disclosed numerous security vulnerabilities that could have been addressed through stronger configurations, including better management of network administrator password controls. In addition to the security benefits, significant cost savings could be realized through the implementation of standard configurations. For example, the United States Air Force was able to reduce its IT management costs by 30 percent and save \$56 million by deploying configuration standards similar to the FDCC on more than 500,000 workstations. While the Department may not be able to achieve identical savings, this example demonstrates the likelihood that significant cost reductions could be realized.

Furthermore, Science may continue to spend more than necessary acquiring IT hardware and support services. Specifically, we determined that Science could potentially realize savings of more than \$3.3 million over the next three years at the sites reviewed by better controlling hardware costs and implementing standards for certain equipment. In addition, Science will continue to pay for duplicative IT support services and fail to take advantage of opportunities to lower costs and apply potential savings to mission-related work. An OCIO official also told us that if Science was included in the DOE-COE infrastructure, it could potentially reduce the overall cost per user for each of the programs participating in the initiative and enable the Department to fully realize the expected cost savings of the DOE-COE initiative.

---

## RECOMMENDATIONS

To address the issues identified in this report, we recommend that the Under Secretary for Science:

1. Include the FDCC in the Science program-level cyber security policies and site-level contracts and ensure implementation of the requirements, as appropriate; and,
2. Require sites to establish and follow IT hardware standards and coordinate purchases, where applicable, to take advantage of volume discounts including the use of enterprise-wide purchasing agreements.

To ensure that a uniform approach is consistently applied to measure the cost-effectiveness of IT support programs, we also recommend that the Under Secretary for Science, in conjunction with the Department's Chief Information Officer:

3. Develop and implement a methodology for consistently capturing and reporting common IT support costs; and,
4. Re-evaluate whether Science should leverage the DOE-COE services.

## MANAGEMENT REACTION

Science management generally concurred with the first three recommendations, but non-concurred with recommendation four. In addition, management indicated that it planned to address many of the issues identified in our report. However, management indicated concerns with a number of assertions made in our report. We have addressed management's comments below and made technical changes to the report, as appropriate. Management's comments are included in their entirety in Appendix 3. The OCIO did not comment on the report.

While management agreed with our recommendation to implement the FDCC, as appropriate, it did not believe that the FDCC set minimum security configuration requirements. However, management noted that it plans to modify existing site-level contracts to require the evaluation and implementation of the FDCC.

Management disclosed that it supported the report's recommendation to lower IT hardware acquisition costs and implement hardware standards, as appropriate, to meet mission

---

needs. However, Science disagreed with several of the report's conclusions and noted that an analysis of the costs and benefits of implementing standards must be considered. Management also commented that it had established and enforced IT hardware standards that meet local mission needs. Furthermore, management stated that it would evaluate the effectiveness of guidance issued in March 2008 to its federal Site Offices related to the development and implementation of hardware standards, and issue additional guidance, as appropriate.

Management commented that it had evaluated the DOE-COE model on numerous occasions, but believed it had implemented a federated IT model that provided the best costs and service to meet the mission needs of the program. Science disagreed with the report's assertion that it did not provide costs that aligned with DOE-COE for comparison and that the methodology of tracking costs did not adequately support the decision not to migrate to DOE-COE. Management pledged to work with the Department's OCIO to ensure that a uniform approach is applied to measure the cost-effectiveness of IT support programs.

## **AUDITORS COMMENTS**

Management's comments are generally responsive to the report's first three recommendations. However, we continue to recommend that Science, in conjunction with the OCIO, re-evaluate whether the program should leverage the DOE-COE services. Although management commented that FDCC does not set minimum requirements, OMB directed agencies to adopt and implement, at a minimum, the FDCC configuration settings on their systems, including those operated on their behalf by contractors. While OMB allows deviations from the FDCC, agencies are required to assess and implement the FDCC in their environment to the extent possible and document any deviations.

We commend management's support for lowering IT hardware acquisition costs and implementing hardware standards. However, as demonstrated by our audit work, Science had not established and enforced hardware standards. Specifically, as noted in the report, two sites reviewed had not established standards for desktop computers. Five of seven sites reviewed had not established standards for IT peripheral equipment such as monitors and printers. Furthermore, we continue to note that significant savings could be realized by the program through the implementation of hardware standards.



---

Although Science indicated that it had implemented a federated IT model, our review found that each of the federal sites reviewed utilized different mechanisms for acquiring and managing IT hardware and support services. In addition, as demonstrated in our report, the methodology used by Science Headquarters to calculate its costs was different from DOE-COE and excluded costs for items such as network administration and security monitoring software. Issues related to the inability to track and compare support costs were also identified at Chicago and Oak Ridge. Based on reviews conducted by both the Office of Inspector General and industry experts, we noted that significant savings could be realized by moving towards shared services and a common infrastructure.

## Appendix 1

---

**OBJECTIVE** To determine whether the Office of Science (Science) adequately managed its information technology (IT) resources.

**SCOPE** The audit was performed between October 2008 and August 2009 at the Department of Energy (Department) Headquarters in Washington, DC, and Germantown, Maryland; the Argonne National Laboratory and the Chicago Office, Argonne, Illinois; the Fermi National Accelerator Laboratory, Batavia, Illinois; the Lawrence Berkeley National Laboratory, Berkeley, California; the SLAC National Accelerator Laboratory, Menlo Park, California; and the Oak Ridge Office and Oak Ridge National Laboratory, Oak Ridge, Tennessee.

**METHODOLOGY** To accomplish the audit objective, we:

- Reviewed applicable laws and regulations, Department of Energy (Department) directives, and Office of Management and Budget guidance pertaining to cyber security practices and acquisition of IT resources;
- Reviewed prior reports issued by the Office of Inspector General, the Government Accountability Office, and the Department's Office of Health, Safety and Security;
- Reviewed numerous documents related to the Department's management of hardware acquisition, as well as cost and functionality of Science's IT support services solutions;
- Evaluated security configuration standards implemented on certain operating systems;
- Held discussions with program officials and personnel from Department Headquarters and field sites reviewed; and,
- Selected numerous weaknesses identified in various cyber security assessments to determine whether the weaknesses were corrected in a timely manner.

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 objectives.

## Appendix 1 (continued)

---

We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We also assessed performance measures in accordance with the *Government Performance and Results Act of 1993* relevant to the management of Science's information technology program. We did not rely on computer-processed data to satisfy our audit objective.

Management waived an exit conference.

### PRIOR REPORTS

- *Evaluation Report on The Department's Unclassified Cyber Security Program - 2008* (DOE/IG-0801, September 2008). The Office of Inspector General (OIG) found that while the Department of Energy (Department) made positive accomplishments, additional action is required to further enhance the Department's unclassified cyber security program and help reduce risks to its systems and data. For instance, the review identified opportunities for improvements in areas such as certification and accreditation of systems, systems inventory, contingency planning, and segregation of duties. These internal control weaknesses existed, at least in part, because not all Department program organizations had revised and implemented policies incorporating Federal and Departmental cyber security requirements in a timely manner.
- *Audit Report on Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007). The OIG review established that certain Department facility contractors had not adequately managed the acquisition and control of information technology (IT) hardware. A number of contractors had not consistently taken advantage of opportunities to reduce acquisition and support costs, addressed security concerns related to certain aging systems, or ensured 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.
- *Audit Report on The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007). The OIG identified that although the Department had made progress in implementing the Department of Energy's Common Operating Environment (DOE-COE) at Headquarters, it had not fully achieved the goals and objectives envisioned by the original initiative. Five major organizations, accounting for 40 percent of the user population, had not migrated to DOE-COE. Officials responsible for implementation did not always follow Department and Federal project management practices, such as developing formal migration plans and conducting requirements analyses.
- *Audit Report on Information Technology Support Services at the Department of Energy's Operating Contractors* (DOE/IG-0725, April 2006). The Department continues to face a number of challenges related to contractor procured or furnished IT support services. In particular, contractors failed to take advantage of opportunities to aggregate demand to leverage or reduce IT support service costs. In addition, per user support costs varied substantially between contractor sites. A number of contractors did not actively capture or track functional IT support costs. In the absence of a framework, the Department did not require contractors to adopt other available methods for reducing costs such as coordinating with established consortium buying groups to consolidate demand and obtain volume discounts.

## Appendix 3



Department of Energy  
Washington, DC 20585

September 29, 2009

MEMORANDUM FOR RICKEY R. HASS  
DEPUTY INSPECTOR GENERAL FOR AUDIT SERVICES  
OFFICE OF INSPECTOR GENERAL

FROM: JEFFREY T. SALMON *J Salmon*  
DEPUTY DIRECTOR FOR RESOURCE MANAGEMENT  
OFFICE OF SCIENCE

SUBJECT: Response to Inspector General's Draft Report, "The Office of  
Science's Management of Information Technology Resources."

The Office of Science (SC) appreciates the opportunity to review and comment on the subject audit. The following reflects the views of the Office of Science. The Office of the Chief Information Officer (OCIO) did not have comments on the subject audit.

SC is committed to implementing cyber security in a risk-based approach at SC Federal sites and at the National Laboratories, while ensuring it does not hinder the innovative research and development mission of the National Laboratories. SC generally concurs with the recommendation to implement the Federal Desktop Core Configuration, "as appropriate".

SC supports the Report's recommendation to lower IT hardware acquisition costs and implementing hardware standards, as appropriate to meet the mission needs. However, SC respectfully disagrees with several of the Report's conclusions. The Report unfavorably compares the Lawrence Berkley National Laboratory (LBNL) to the Oak Ridge National Laboratory (ORNL) but it does not provide analysis on the costs/benefits of the approach being used by each respective laboratory. The information, the scientific productivity, the morale of the employees, and the costs to administer the program must be considered alongside the strategic and thoughtful approach being used by each Laboratory to build systems and processes designed to support their diverse environment and maximally deliver productive technologies. Standardization at the National Laboratories to achieve potential cost savings should more accurately be compared to Tier 1 research environments, as the National Laboratories are an environment that generates diverse ideas and computer needs.

Argonne National Laboratory (ANL) purchases all equipment and supplies in accordance with its fundamental scientific mission. The Report does not recognize that only 20% of the vendors used by ANL in a particular year receive 90% of ANL's dollar volume in computer purchases. Wherever possible, ANL uses its preferred vendors and contracts to supply computer equipment. Periodically, the scientific mission requires ANL to go outside of its preferred vendors and contracts.

SC has established and enforces IT hardware standards that meet the local mission needs. The Report does not take into account the one-quarter refresh rate at Oak Ridge Office or the 100%

refresh at SC Headquarters (HQ) that resulted in better pricing compared to the negotiated DOE pricing. Each year the hardware vendors change hardware models multiple times during the year and modify their pricing, which explains the variation in price for the same item. It is more accurate to analyze the three or four year life cycle costs to acquire IT hardware, instead of comparing individual years.

SC has evaluated the DOE-COE model on numerous occasions and implemented a federated IT model and in doing so has obtained the best costs and service to meet the mission needs of the program. SC disagrees with the Report's assertion that SC did not provide costs that align with DOE-COE for comparison and the methodology of tracking costs did not adequately support the decision to not migrate to DOE-COE. Oak Ridge provided sufficient detail to the IG that aligned with the DOE-COE categories and Chicago's cost aligned with the categories at the time of original submission. The Report compares the "...\$300 charged by the Office of the Chief Information Officer (OCIO)...", but does not provide evidence this is the true cost under DOE-COE, nor that the per seat cost for the Department would be decreased by SC joining DOE-COE. The then SC Deputy Director of Resource Management met with the then Deputy Secretary and Chief Information Officer in February 2008 to discuss DOE-COE and the pricing for SC HQ compared to DOE-COE. The result of the meeting was that SC would not be included in DOE-COE because the SC model was more cost effective.

SC disagrees with the Report's claims that "significant savings could be realized" by modifying/consolidating IT purchasing and joining DOE-COE. The only savings noted is "\$3.3 million over three years" which is 0.027% per year and explained by variations in a product's price over the course of a single year from a single vendor and including computer equipment specifically ordered to meet the scientific mission.

SC continues to evaluate the IT costs for support and hardware. As part of its mission to deliver open science and support basic scientific research, SC provides funding for the high-speed Energy Science Network (ESnet). The ESnet infrastructure is part of the overall SC direction to reduce costs and SC is evaluating the long-term approach to use ESnet to meet its mission needs, as all of SC currently maintains connections to ESnet. This approach will reduce the infrastructure-related costs to SC and provide for a more open environment to support the SC mission in support of the Department.

Attached are SC's responses to the facts presented, proposed recommendations, and estimated potential monetary impact.

Attachment

Cc  
Steve Binkley/SC-1  
Patricia Dehmer/SC-2  
George Malosh/SC-3  
Thomas Phan/SC-45

## CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?
5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name \_\_\_\_\_ Date \_\_\_\_\_

Telephone \_\_\_\_\_ Organization \_\_\_\_\_

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)  
Department of Energy  
Washington, DC 20585

ATTN: Customer Relations

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

This page intentionally left blank.



The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page  
<http://www.ig.energy.gov>

Your comments would be appreciated and can be provided on the Customer Response Form.