



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

Audit Report

The Department of Energy's
Implementation of Homeland
Security Presidential Directive 12



Department of Energy
Washington, DC 20585

February 28, 2012

MEMORANDUM FOR THE SECRETARY

FROM: 
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department of Energy's
Implementation of Homeland Security Presidential Directive 12"

INTRODUCTION AND OBJECTIVE

Homeland Security Presidential Directive 12 (HSPD-12), *Policies for a Common Identification Standard for Federal Employees and Contractors*, was established in August 2004 to enhance national security and mandate the use of a Federal government-wide standard for secure and reliable forms of identification for Federal employees and contractors. HSPD-12 required that the identification be issued based on sound criteria for verifying an employee's identity; strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation; able to be rapidly authenticated electronically; and, issued only by providers with reliability established by an official accreditation process. Full implementation of HSPD-12 includes badge issuance, and physical and "logical access control" systems. "Logical controls" rely on computer hardware and software to prevent unauthorized access. While badge issuance is the initial step and involves providing credentials to all employees and contractors that are covered by HSPD-12, logical and physical access controls entail using the credential to gain access to information systems and Federal facilities, including those that are Government-owned and contractor-operated.

The Department of Energy initiated its HSPD-12 efforts in 2004 and has spent more than \$15 million, most of which was dedicated to issuance and maintenance of badges. However, recent Office of Management and Budget guidance directed that Federal agencies should have physical and logical access controls fully installed and that policy be issued by each agency to ensure all new systems under development be enabled to use HSPD-12 credentials. OMB also directed that, effective the beginning of Fiscal Year 2012, physical and logical access controls be upgraded to use HSPD-12 credentials prior to using development and technology refresh funds to complete other activities, and noted that agencies' processes must accept and electronically verify HSPD-12 credentials issued by other Federal agencies. In light of the updated OMB requirements, we initiated this audit to determine whether the Department implemented physical and logical access controls in accordance with HSPD-12.

RESULTS OF AUDIT

We found that, despite 7 years of effort and expenditures of more than \$15 million, the Department had yet to meet all HSPD-12 requirements. In particular, the Department had not fully implemented physical and logical access controls in accordance with HSPD-12.

Furthermore, the Department had not issued HSPD-12 credentials to many uncleared contractor personnel at its field sites. Specifically:

- None of the 5 field sites reviewed had fully implemented physical access controls in accordance with HSPD-12 for the more than 40,000 employees requiring access to those facilities. While the Oak Ridge National Laboratory and the East Tennessee Technology Park had started implementing physical controls using HSPD-12 credentials, the remaining sites had not begun work, and none had a fully developed system in place as defined by HSPD-12 and Department guidance. As noted by the National Institute of Standards and Technology, utilizing the full functionality of HSPD-12 credentials for physical access is important because it is more secure and reliable than traditional controls currently in use;
- The Department had made progress for utilizing the HSPD-12 credential to authenticate user access to information systems; however, additional work was needed. For example, although Headquarters and the Oak Ridge Office were using badges on a limited basis to allow network access, none of the sites reviewed had fully implemented logical access controls for all information systems and applications as required by HSPD-12. In fact, many sites had not even begun to implement logical controls even though the requirement to begin this work had been in place for approximately 5 years. Federal guidelines note that some of the benefits of using the HSPD-12 credential for logical access include electronic authentication of the credential at the time of use, which cannot be achieved with usernames and passwords; and,
- Contrary to the goals and requirements of the directive, four of the five field sites we reviewed did not provide HSPD-12 credentials to contractors that did not hold a security clearance. The fifth site, Oak Ridge Office, issued badges to these employees only when they met certain unique requirements, such as the need for travel to other Department sites. We noted that over 11,000 of 40,000 (27 percent) individuals without security clearances that required routine access to sites for a period in excess of 6 months had not been issued HSPD-12 credentials. While the Department's current badging processes provided certain security assurances, the processes did not include all background checks required by HSPD-12. Federal regulations emphasized that issuance of the credential be based on sound criteria for identity verification and highly resistant to identity fraud, counterfeiting and tampering.

We noted what we considered to be a lack of a coordinated approach among programs and sites related to implementation of HSPD-12 requirements. In particular, we found that guidance provided by management was fragmented and often inadequate to meet the goals of the initiative. In addition, ongoing efforts suffered from a lack of coordination among programs and sites to determine the cost, scope and schedule of work required to implement HSPD-12 requirements. Further, several programs and sites visited had not established budgets in an attempt to obtain funding to support HSPD-12 activities.

OMB has concluded that the use of HSPD-12 credentials provides more secure access to Federal facilities, enhanced cyber security and reduced overall costs. However, until physical and logical

access controls are fully implemented in accordance with HSPD-12, the Department will continue to pay significant maintenance costs for credentials without realizing the full benefits.

In response to a preliminary draft of our report, management officials noted that in certain instances, such as construction contractors that are often restricted to certain areas and never access Federal data systems, providing an HSPD-12 credential provides little additional benefit, and as such, is not cost effective. The Office of Inspector General has long been a proponent of a risk-based approach to physical and cyber security. As such, we agree that cost/benefit realities can impact the nature and extent of security control measures. That said, however, we also believe that it would be in the Department's best interest to consult with OMB if it plans to adopt a process that does not fully comport with HSPD-12.

We found that some sites had initiated action to implement physical and logical access controls supporting the goals of HSPD-12. For example, the Oak Ridge National Laboratory anticipated that its physical access controls would be compliant by March 2012. Officials from other sites, including Oak Ridge Office and East Tennessee Technology Park, stated that they planned to implement their own physical controls based on the Oak Ridge National Laboratory's outcome and lessons learned. These are positive actions; however, additional effort is necessary to ensure that controls are implemented to meet the goals of HSPD-12. As such, we have made several recommendations that, if fully implemented, should improve the Department's ability to effectively implement physical and logical access controls in accordance with HSPD-12.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had initiated corrective action to address issues identified in our report. In separate comments, National Nuclear Security Administration concurred with the report's findings and stated that it will use the findings to improve the management and oversight of its implementation of HSPD-12. Management's comments are included in Appendix 3.

Attachment

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

REPORT ON THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12

TABLE OF CONTENTS

Implementation and Credential Issuance

Details of Finding	1
Recommendations and Comments.....	8

Appendices

1. Objective, Scope and Methodology	10
2. Related Reports	12
3. Management Comments	14

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12

Implementation and Credential Issuance

Although the Department of Energy (Department) had invested 7 years of effort and expended more than \$15 million, it had yet to complete implementation of Homeland Security Presidential Directive 12 (HSPD-12) requirements. While the Department spent funds on installation of badge stations, badge issuance and monthly credential maintenance fees, we found that it had not fully implemented physical access control systems utilizing the HSPD-12 credential to restrict access to only those areas for which an individual is authorized. In addition, none of the sites reviewed had developed logical access controls to information systems and applications in accordance with HSPD-12. Furthermore, the Department had not issued HSPD-12 credentials to uncleared contractors at its field sites. While the Department's current badging processes provided certain assurances, all background checks required by HSPD-12 were not included.

Physical Access Controls Implementation

Of the 5 field sites reviewed, none had fully implemented physical access control systems using HSPD-12 credentials for the more than 40,000 employees requiring access to those facilities. HSPD-12 physical access controls allow for the user's credential to be electronically validated so that terminated or expired credentials cannot be used to inappropriately access Federal facilities. While the Oak Ridge National Laboratory (ORNL) and East Tennessee Technology Park (ETTP) had started implementing physical access controls, the remaining sites had not begun work, and none had a fully developed system in place as defined by HSPD-12 and Department guidance.

Three locations reviewed, with a total population of approximately 26,000 workers, had not begun physical access controls implementation, which would provide the Department with enhanced security and potentially reduce overall costs. For example, as of July 2011 – seven years after the directive was issued – the Oak Ridge Office (ORO) was still working to purchase and install badge readers. In addition, although the Y-12 National Security Complex (Y-12) planned to install a HSPD-12 compliant physical security system, it had not begun work on the project because of a lack of funding. Similarly, the Savannah River Site (SRS) had not implemented a physical access control system that would accept the functionality of the HSPD-12 credential. Limited progress was also observed at the remaining sites reviewed. In particular, badge readers in ORNL's high

security areas were not functional because it was in the process of obtaining software updates, and ETTP had not installed all of its HSPD-12 badge readers.

We also found that four of six locations reviewed did not utilize the internal HSPD-12 badge smart chip functionality to control access to facilities. Instead, the Department modified its HSPD-12 badges with the addition of a magnetic stripe to work with existing badge readers. Though the remaining locations used some of the smart chip's capability, validation checks were not fully performed to control facility access. This approach was appropriate during the Department's transition to HSPD-12 credential use. However, continued reliance on the magnetic stripe allowed the Department to delay utilizing the HSPD-12 credential's smart chip, that contains the owner's unique Personal Identity Verification (PIV) information and should be used to authenticate the identity of the cardholder. Notably, Headquarters had recently taken action to implement the smart chip functionality at its facilities.

Logical Access Controls Implementation

The Department had made progress utilizing HSPD-12 credentials to authenticate user access to information systems; however, additional work was needed. While Headquarters and ORO were using badges on a limited basis to allow network access, none of the locations reviewed had fully implemented logical access control systems for all information systems and applications. As noted in the table below, less than 3 percent of the nearly 23,000 users requiring system access at the field sites reviewed were using their credentials for such access.

Location	Users Authenticating via HSPD-12 Credential	Total Number of System Users	Percentage
Y-12	0	6,400	0.0%
ORO	557	1,056	52.7%
ORNL	0	6,200	0.0%
ETTP	0	1,500	0.0%
SRS	45	7,565	0.6%
Total – Field Sites	602	22,721	2.6%
Headquarters	6,630	7,030	94%
Total – All Locations	7,232	29,751	24%

According to planning documentation provided by the Department, using HSPD-12 credentials for access to information systems and applications provides for electronic authentication of the credential at the time of use, which cannot be achieved with the Department's current logical access controls of usernames and passwords. In addition, as noted in a recent U.S. Government Accountability Office report, the process of electronic authentication with the HSPD-12 credential significantly enhances the security of a computer system because it is more difficult for an intruder to circumvent. Also, each of the sites reviewed still had not acquired all of the necessary infrastructure such as PIV card readers and authentication software so that the badge's functionality could be used to access the Department's systems.

Credential Issuance

We found that four of the five sites reviewed did not provide HSPD-12 badges to contractors that did not hold a security clearance. One of the four sites, SRS, had recently curtailed its practice of issuing HSPD-12 credentials to all site personnel due to budget concerns. In addition, a fifth site issued the badges to employees only when they met certain requirements, such as the need to travel to other Department sites. According to HSPD-12 guidance issued by the Office of Management and Budget (OMB), the directive is applicable to all Federal employees and contractors requiring routine access to Federal facilities or information systems for greater than 6 months. Further, the Federal Chief Information Officers Council (CIO Council) recently clarified that badges not meeting HSPD-12 requirements could not be issued to individuals that fell within the applicability of the directive. Issuance of the HSPD-12 credential requires completion of a National Agency Check with Inquiries (NACI) investigation that includes a Federal Bureau of Investigation (FBI) name and fingerprint check; Office of Personnel Management (OPM) Suitability Clearance Index and Defense Clearance Index check; written inquiries and searches of records for the past 5 years in the areas of employment, education and law enforcement; and, written inquiries and searches of records for the past 3 years in the areas of residences and references.

Contrary to Federal direction, the Department issued guidance that HSPD-12 badges were not required for uncleared contractor employees at field sites, even if they maintained routine access to sites and/or information systems for periods in excess of 6 months. As a result, over 11,000 individuals (27 percent of the total population), without security clearances that required routine access to sites for a period in excess of 6 months, had not been

issued HSPD-12 credentials. Based on documentation provided by Department officials, we also noted that the Lawrence Berkeley National Laboratory had issued HSPD-12 badges to only 51 of 3,948 (less than 2 percent) permanent personnel – those individuals requiring site access for a period longer than 6 months.

While employees not receiving HSPD-12 badges did undergo various identity verification activities, as determined by the site, the procedures were generally less robust than, and did not include all elements of, a NACI review. For example, Y-12's site procedures, developed to meet National Nuclear Security Administration (NNSA) guidance, did not require the FBI and OPM checks described above for non-HSPD-12 badge issuance. Rather, Y-12 required the presentation of two forms of identification and a check of previous employers, education and references prior to badge issuance. As such, the site's identity verification activities were not as substantive as the NACI. In addition, identity verification activities were inconsistent among sites and were subject to change at the sites' discretion. As employees at many sites required routine access to Federal facilities and systems, their identities should have been verified in accordance with the Presidential directive. Further, one Department security official stated that not providing HSPD-12 badges to contractors that did not hold a security clearance was contrary to best business practices and allowed the largest segment of the Department's population, on which there was no background information, to have unescorted access to Department facilities.

Completion of robust background checks, such as those required by HSPD-12, may have prevented the issues related to identity proofing highlighted in two recent Office of Inspector General reports. For example, our inspection on *Verification of Lawrence Berkeley National Laboratory's Contract Workers' Eligibility to Work in the U.S.* (DOE/IG-0850, April 2011) identified eight individuals that had duplicate social security numbers, numbers belonging to deceased individuals or numbers that had yet to be issued – anomalies that would have been discovered had an effective HSPD-12 process been in place. In addition, our audit on *Environmental Cleanup Projects Funded by the Recovery Act at the Y-12 National Security Complex* (OAS-RA-L-11-02, December 2010) determined that Y-12 had not used a third party to independently verify citizenship documentation provided by its workers. In both cases, had the sites used HSPD-12 background investigation procedures to obtain independent proof of citizenship for workers, the risk of unauthorized workers inappropriately gaining access to Federal facilities would have been significantly reduced.

Rather than issue HSPD-12 credentials to all applicable contractors, the Department planned to develop a separate badge, commonly referred to as the PIV-Interoperability (PIV-I) credential. However, the CIO Council noted that while it was a valid credential, the PIV-I was only to be used for individuals not requiring routine access to Federal facilities and systems. Contrary to this guidance, the Department spent considerable time and effort determining how this credential would be implemented for its contractor personnel that did require routine access.

Coordinated Approach to HSPD-12

The issues identified were due to the lack of a coordinated approach among offices and sites related to implementation of HSPD-12 requirements. In particular, we found that leadership and guidance provided by management was fragmented and not adequate to meet the goals of HSPD-12. In addition, ongoing planning and implementation efforts suffered from a lack of coordination among offices and sites to determine the cost, scope and schedule of work required to meet HSPD-12 requirements.

Leadership and Guidance

We found that leadership and guidance provided by management was not adequate to meet the goals of HSPD-12. Specifically, a number of Department officials commented that they believed HSPD-12 would be rescinded when the current Administration took office in 2009. As a result, the Department had not developed adequate plans for implementing physical and logical access controls using the HSPD-12 credential within the designated timeframes established by OMB. In addition, while the Office of Health, Safety and Security oversaw an effort to issue HSPD-12 badges across numerous sites, the Department's guidance regarding badge issuance activities was insufficient. For example, sites relied on a 2005 Department memorandum issued by the Deputy Secretary, at the time, that allowed programs to determine whether uncleared contractors at field sites would be issued HSPD-12 credentials. In June 2011, this guidance was incorporated into a Department Order. However, the memorandum and Order both contradicted HSPD-12 and direction that was recently re-enforced by OMB. We also learned that the Department's Office of the Chief Information Officer (OCIO) recently issued a memorandum outlining a requirement to integrate physical and logical access controls using the HSPD-12 credential.

Coordinated Approach

We also noted that ongoing planning and implementation efforts suffered from a lack of coordination among programs and sites to determine the cost, scope and schedule of work required to implement HSPD-12 requirements. In particular, even though it had not implemented HSPD-12 physical and logical access control systems, the Department had not developed an implementation plan for utilization of PIV credentials as required by OMB Memorandum 11-11. For example, of the four offices reviewed, only the NNSA had developed an implementation plan that fully supported HSPD-12, and the Office of Science (Science) had developed an implementation plan supporting logical access controls. To enhance ongoing efforts, the OCIO established an Integrated Project Team (IPT) in 2011 to help align HSPD-12 implementation activities and improve coordination among offices. However, at the time of our review, the IPT had not been in existence long enough for us to evaluate its success. Finally, none of the five sites reviewed had a site-wide plan for full HSPD-12 implementation. We also noted that several of the offices and sites reviewed had not included HSPD-12 in their budgets in an attempt to obtain funding to support these activities even though the requirement had existed for 7 years.

Furthermore, communication from offices to respective field sites was not effective. For example, NNSA officials at Headquarters indicated that Y-12 was implementing physical access controls as part of its ongoing Security Improvement Project. However, during our site visit, we found that physical access controls in only a small number of closed areas were included in the project. In addition, although Science officials indicated that they believed funding should be put towards other mission-related work instead of implementation activities, we noted that ORNL was moving forward with its upgrade to its physical access control system in support of HSPD-12.

Realization of Goals and Objectives

Until physical and logical access control systems are fully implemented in accordance with HSPD-12, the Department will continue to pay significant maintenance costs for credentials without realizing the full benefits. As noted in HSPD-12, benefits can include more secure access to Federal facilities, improved cyber security, reduced costs and enhanced resistance to identity fraud, counterfeiting, tampering and terrorist exploitation. In addition, Department documentation noted that the use of HSPD-12 credentials would create a streamlined and synchronized process for managing access controls, that will work with other agencies, facilities and applications to improve operational

effectiveness and efficiency. Finally, OMB also directed that beginning in Fiscal Year 2012, development and technology refresh funding will be limited to HSPD-12 implementation activities until use of the credential is completely implemented. Therefore, until that time, the Department's activities requiring such funding will be restricted.

Also, the Department may have circumvented the intent of HSPD-12 by limiting credential issuance at its field sites to only contractor employees that had already had their identities verified through a robust security clearance process. As previously noted, the HSPD-12 process was developed in an effort to increase security by verifying the identity of any individual working at a Federal facility for an extended period of time. However, the Department's decision to rely on site-level verification processes that were not as robust and have been demonstrated to have weaknesses restricted its ability to gain this type of assurance or security for its uncleared and more transient population. In addition, as a result of its decision to exclude certain contractors, progress of the Department's HSPD-12 efforts being reported to OMB was inflated because it only included contractor personnel that held security clearances. Specifically, at the six locations for which we have data, the Department reported that 94 percent of the total population had received an HSPD-12 badge. However, as this figure did not account for uncleared workers, we determined that the Department had only provided HSPD-12 badges to 53 percent of the total population at these sites that met HSPD-12 requirements.

Furthermore, the Department continued to expend time and resources on efforts to identify alternatives to HSPD-12 badges that could have been better spent implementing the directive. As the identity-proofing alternatives did not include all verification activities required by HSPD-12, continued issuance of noncompliant credentials may hinder the Department's ability to sufficiently verify the identity of its employees and ensure that badges meet the goals of the Administration. In addition, the level of security offered by an HSPD-12 badge may not be realized due to inconsistencies in background checks.

Finally, our review identified a potential cost savings to the Department if it phased out the use of RSA[®] tokens for remote access. As noted by the National Institute of Standards and Technology, a PIV card solution must support the same technology used by tokens to allow two-factor authentication. In addition, a recent study by NNSA noted that significant savings could be realized by making such a transition. While we acknowledge there

are costs associated with implementing HSPD-12, we determined that the Department could offset some of this cost through potential savings of up to \$600,000 at the locations we visited if many of its users who possess the HSPD-12 credential were to authenticate to unclassified systems using the credential rather than a RSA[®] token. By doing so, the Department would no longer need to incur maintenance and license fees associated with the tokens – fees similar to those already being paid to maintain the HSPD-12 credential.

RECOMMENDATIONS

To help improve the Department's ability to effectively implement physical and logical access control systems in accordance with HSPD-12, we recommend that the Under Secretary for Nuclear Security, Acting Under Secretary of Energy and Acting Under Secretary for Science, in conjunction with the Department's and NNSA's Chief Information Officers:

1. Develop and implement guidance to fully meet the goals and requirements of HSPD-12;
2. Develop and implement a comprehensive plan that includes cost analyses and timeframes for implementing physical and logical access control systems in accordance with HSPD-12; and,
3. Revise Department policy as appropriate to ensure that unclassified contractors receive credentials in accordance with the requirements of HSPD-12.

In addition, to ensure the Department meets the intended goals of HSPD-12, we recommend that the Chief Information Officer:

4. Consult with OMB, as necessary, regarding the Department's planned approach for badge issuance and the use of an alternate credential for certain of its contractors.

MANAGEMENT REACTION

Department management agreed with the report's recommendations and stated that it had initiated action to address the issues identified. Management commented that the report's findings were reasonable and provided effective insight and recommendations to correct discrepancies and improve the management and oversight of the Department's implementation of HSPD-12. In addition, management stated that it had established an IPT to oversee the development of HSPD-12 policies, standards and guidelines. In separate comments, NNSA management concurred with the

report's findings and stated that it will use the findings to improve the management and oversight of NNSA's implementation of HSPD-12.

AUDITOR COMMENTS Management's comments and planned corrective actions are responsive to our recommendations. Management's formal comments are included in Appendix 3.

Appendix 1

OBJECTIVE To determine whether the Department of Energy (Department) had implemented physical and logical access controls in accordance with Homeland Security Presidential Directive 12 (HSPD-12).

SCOPE The audit was performed between April 2011 and February 2012, at Department Headquarters in Washington, DC and Germantown, Maryland; the Oak Ridge Office, Oak Ridge National Laboratory, East Tennessee Technology Park and Y-12 National Security Complex in Oak Ridge, Tennessee; and, the Savannah River Site in Aiken, South Carolina.

METHODOLOGY To accomplish our objective, we:

- Reviewed Federal laws and regulations associated with the implementation of HSPD-12;
- Obtained and reviewed the Department's policies and procedures for implementing physical and logical access controls associated with HSPD-12;
- Conducted interviews with various office and site officials to gain background information on the Department's implementation of HSPD-12;
- Obtained and reviewed site information relevant to implementation costs, badge population and implementation schedules related to HSPD-12;
- Obtained and reviewed documentation associated with both the current and future plans of physical and logical access controls at each site; and,
- Reviewed prior reports issued by the U.S. Government Accountability Office and the Office of Inspector General.

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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. 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 *Government Performance and Results Act of 1993* and determined

that it had established performance measures for implementation of HSPD-12. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our audit objective.

The Department and NNSA waived an exit conference.

RELATED REPORTS

Office of Inspector General Reports

- Audit Report on [Verification of Lawrence Berkeley National Laboratory's Contract Workers' Eligibility to Work in the U.S.](#) (DOE/IG-0850, April 2011). Not all of Lawrence Berkeley National Laboratory's (LBNL) subcontractors ensured that individuals employed to work on the site were initially eligible or maintained authorization to work in the U.S. throughout the term of their employment. In addition, some contractors failed to record required key employment eligibility elements. Further, although available for voluntary use by all employers since 2007, we found that none of the 19 LBNL subcontractors included in our review used the U.S. Government's *E-Verify* system to supplement the Form I-9 employee eligibility determination process. These problems occurred, in part, because LBNL contractors did not place sufficient emphasis on ensuring that their employment verification activities complied with Federal law. In addition, Department of Energy (Department) policy did not require site security offices to verify, or even to confirm on a sample basis, the employment eligibility of contract workers before site access is allowed. As a consequence, unauthorized workers may have inappropriately gained access to Federally-funded facilities and could have displaced U.S. citizens or other authorized workers from jobs. Management concurred with the findings and recommendations contained in the inspection.
- Audit Report on [Environmental Cleanup Projects Funded by the Recovery Act at the Y-12 National Security Complex](#) (OAS-RA-L-11-02, December 2010). The Y-12 National Security Complex (Y-12) had not included a required clause that was intended to ensure employment eligibility in the American Recovery and Reinvestment Act of 2009 (Recovery Act) subcontracts we reviewed. Although the *Employment Eligibility Verification* clause was effective in December 2009, Y-12 had not flowed down the clause to its subcontractors until September 2010. Specifically, Y-12 management decided it was more efficient to reference the clause in its *General Terms and Conditions*, which were undergoing revision, rather than incorporating it independently into each subcontract. Y-12 management stated it had mitigating controls to ensure that only U.S. citizens are issued photo badges which are required for access to the Y-12 site. However, Y-12 management acknowledged that it was not required to verify the validity of proof of citizenship as part of its badging process, and we confirmed, that Y-12 does not verify the information with independent parties. While Y-12's controls may have been beneficial, it did not provide the independent verification of employment eligibility documentation available through the *E-Verify* system as required by Federal regulations. Because of the mitigating actions initiated by Y-12, we did not make formal recommendations.

Government Accountability Office Reports

- Report on [Agencies Face Challenges in Implementing New Federal Employee Identification Standard](#) (GAO-06-178, February 2006). The U.S. Government Accountability Office (GAO) found that the Federal government faces significant challenges in implementing Federal Information Processing Standard (FIPS) 201,

Appendix 2 (continued)

including: (1) testing and acquiring compliant commercial products – such as smart cards and card readers—within required time frames; (2) reconciling divergent implementation specifications; (3) assessing the risks associated with specific vendor implementations of the recently chosen biometric standard; (4) incomplete guidance regarding the applicability of FIPS 201 to facilities, people and information systems; and, (5) planning and budgeting with uncertain knowledge and the potential for substantial cost increases. Until these implementation challenges are addressed, the benefits of FIPS 201 may not be fully realized. Specifically, agencies may not be able to meet implementation deadlines established by the Office of Management and Budget (OMB), and more importantly, true interoperability among Federal government agencies' smart card programs – one of the major goals of FIPS 201 – may not be achieved.

- [*Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards*](#) (GAO-08-292, February 2008). GAO found that although much work had been accomplished to lay the foundations for implementation of HSPD-12, a major Federal government-wide undertaking had not occurred. Agencies had made limited progress implementing and using Personal Identity Verification (PIV) cards. For the limited number of cards that had been issued, most agencies had not been using the electronic authentication capabilities on the cards and had not deployed implementation plans for those capabilities. Without implementing the cards' electronic authentication capabilities, agencies will continue to purchase costly PIV cards to be used in the same way as the much cheaper, traditional identification (ID) cards being replaced. Until OMB revises its approach to focus on the full use of the capabilities of the new PIV cards, HSPD-12's objectives of increasing the quality and security of ID and credentialing practices across the Federal government may not be fully achieved.

MANAGEMENT COMMENTS



Department of Energy

Washington, DC 20585

January 18, 2012

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: MICHAEL W. LOCATIS III 
CHIEF INFORMATION OFFICER

SUBJECT: IG Draft Report, "The Department's Implementation of
Homeland Security Presidential Directive 12"

Thank you for the opportunity to comment on this draft report. The Department of Energy (DOE) Office of the Inspector General (IG) provided a very thorough and concise review on the Department's Implementation of Homeland Security Presidential Directive 12 (HSPD-12). In reviewing the draft we agree that most of the IG findings are reasonable and provide effective insight and recommendations to correct discrepancies and improve the management and oversight of DOE's implementation of HSPD-12. The information provided in the report will enable the Office of the Chief Information Officer (OCIO) and program offices to take appropriate follow-up actions on specific findings.

In May 2011 the OCIO established the Corporate IT Project Management Office (IM-40) to provide centralized management oversight for cross-organizational IT projects within DOE. The DOE Identity, Credential and Access Management (ICAM) program was realigned under IM-40 for the purpose of providing consistent guidance and oversight for the formulation and implementation of the DOE ICAM program, to include requirements contained in HSPD-12. The IM-40 ICAM Project Manager established an Integrated Project Team (IPT) composed of Federal management representatives from the Headquarters (HQ) program and staff offices for the purposes of establishing Department-wide ICAM policies, standards and guidelines. We believe realignment of the DOE ICAM project under the Corporate IT Project Management Office remediated findings related to the Department having a coordinated approach to the ICAM program.

Detailed comments from the Office of Environmental Management (EM), Office of Health, Safety and Security (HSS) and Office of Science (SC) are contained in Appendix A.

With respect to the specific recommendations in the draft report:

Recommendation 1: *Develop and implement guidance to fully meet the goals and requirements of HSPD-12.*

Management Response: Concur.



Printed with soy ink on recycled paper

The IM-40 ICAM Project Manager established an IPT composed of Federal management representatives from the HQ program and staff offices for the purposes of establishing Department-wide ICAM policies, standards and guidelines. The ICAM IPT was chartered by the Information Management Governance Council (IMGC) to:

- 1) Establish strategic direction for the DOE Federated ICAM effort using the Federal ICAM Roadmap and Implementation Guidance [FICAM Roadmap] as the principal driver and recognizing the work already done by DOE elements;
- 2) Ensure that the following ICAM services will be available in DOE:
 - a. Enterprise view of digital identities
 - b. Credential issuance and management
 - c. Management of privileges and entitlements
 - d. Authentication and authorization
 - e. Cryptography/Public Key Infrastructure (PKI)
 - f. Comprehensive auditing and reporting
- 3) Coordinate DOE ICAM activities including:
 - a. Developing ICAM strategy, policy, business cases, architecture, requirements, and implementation plans;
 - b. Creating a uniform identity infrastructure built on common credentials; and
 - c. Ensuring that ICAM aligns with the DOE Enterprise Architecture and supports DOE's mission.
- 4) Participate in the development of policy language to be included in a DOE Order/Notice;
- 5) Define the standards for the DOE Federated ICAM effort;
- 6) Coordinate and align Program Office ICAM implementations;
- 7) Coordinate and issue responses to Office of Management and Budget (OMB) and other external stakeholders.

Secondly, the ICAM IPT unanimously approved the DOE ICAM Framework that:

- 1) Defines the Departmental approach to implementing ICAM that aligns with FICAM. DOE Organizations that implement ICAM in alignment with the Framework have high confidence of interoperability with ICAM services implemented by other DOE Organizations and by other Federal Agencies.
- 2) Establishes an enterprise and interoperable access management approach that links DOE Physical Access Control Systems (PACS) and logical access control systems (LACS) to a federated access management infrastructure.
- 3) Fosters an enterprise view of digital identity that facilitates the sharing of digital identity data across DOE Organizations as well as with external DOE entities.
- 4) Implements identity credentials at all Levels of Assurance, as defined in the OMB Memorandum 04-04, based on risk management approach and DOE Organization requirements.

- 5) Fosters a system-of-system approach where the DOE Organizations collaborate and cooperate in implementing ICAM, identifying mission needs and managing associated risks.

Consistent with the enterprise goals and objectives defined in the DOE ICAM Framework, OCIO initiated in FY11 the development of an enterprise ICAM service offering that will provide access to DOE corporate information systems using the HSPD-12 credential. This approach addresses the findings that logical access controls have not been fully implemented for information systems. The enterprise approach to access management offers a cost effective and efficient solution for implementing logical access controls to meet HSPD-12 requirements versus having each information system implement the requirement separately. The solution will also allow authentication with public credentials issued from trusted Identity Providers certified under the Trust Framework Provider Adoption Process (TFPAP) as required by the October 2011 OMB Memo, *Requirements for Accepting Externally-Issued Identity Credentials*.

Based on the steps taken within DOE to develop and implement guidance for the DOE ICAM program, as outlined above, we respectfully request Recommendation 1 be closed.

Recommendation 2: *Develop and implement a comprehensive plan that includes cost analyses and timeframes for implementing physical and logical access control systems in accordance with HSPD-12.*

Management Response: Concur.

The DOE ICAM IPT formulated the DOE ICAM Implementation Plan in November 2011, identifying major milestones to fully implement the integrated ICAM effort across the DOE Enterprise. In accordance with milestones identified in the DOE ICAM Implementation Plan, each DOE program office is developing a detailed implementation plan for their respective offices and field sites, with target completion of the program office implementation plan scheduled for February 2012. The Program Office implementation plans are to include provisions for analyzing costs associated with full HSPD-12 compliance, and establish timelines for implementing physical and logical access control systems in accordance with HSPD-12.

Recommendation 3: *Revise Department policy as appropriate to ensure that uncleared contractors receive credentials in accordance with the requirements of HSPD-12.*

Management Response: Concur.

The ICAM IPT is scheduled to develop a DOE directive governing the ICAM program, to include policy related to issuance of credentials for uncleared contractors. The ICAM IPT is scheduled to provide a draft directive for formal review and concurrence by July 2012.



Department of Energy
National Nuclear Security Administration
Washington, DC 20585



January 6, 2012

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM:


KENNETH W. POWERS
ASSOCIATE ADMINISTRATOR FOR
MANAGEMENT AND BUDGET

SUBJECT:

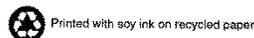
NNSA's Comments on Inspector General Draft Report titled *The Department's Implementation of Homeland Security Presidential Directive 12*; Project No. A11TG032 / IDRMS No. 2010-00655

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "*The Department's Implementation of Homeland Security Presidential Directive 12*."

Based on our review, NNSA concurs with the IG findings and will use them to improve the management and oversight of NNSA's implementation of HSPD-12. NNSA is actively participating in the Department of Energy's (DOE) Identity, Credential and Access Management (ICAM) program, which encompasses the requirements of HSPD-12. DOE's ICAM integrated project team (IPT), which is currently chaired by an NNSA employee, is developing Department-wide ICAM policies, standards, and guidelines. We believe the ICAM IPT along with the work of DOE's Office of Corporate IT Project Management are contributing to a coordinated approach for DOE to the ICAM program.

If you have any questions concerning this response, please contact Dean Childs, Director, Management Control and Assurance, at 301-903-1341.

Attachment



General Comments

1. **Last sentence of the third paragraph on page 3 of the Report** - "Further, one Department security official..."

It seems a little misleading to say that not providing HSPD-12 badges to contractors "allowed the largest segment of the Department population...unescorted access to Department facilities." While this is directed to the Department overall (and not specifically to Y-12), it implies that a non-HSPD-12 badged person could access (unchallenged) any or all Department facilities. This is not the case at Y-12.

2. **Fourth paragraph on page 3 of the Report** - "...determined that Y-12 had not consistently verified citizenship documentation provided by its workers."

This issue seems to be more accurately presented on page 9 of the report (referencing the prior audit). The issue appears to address Y-12 not using E-Verify, versus that we were not consistently verifying citizenship (as a certain set of documentation was consistently required to verify citizenship and issue a visitor badge). As such, this statement as written could be misleading. The following wording change is offered. "In addition, our audit of *Environmental Cleanup Projects...*, determined that Y-12 had not used a third party to independently verify citizenship documentation provided by its workers."

3. **Page 6 of the Report, first full paragraph** - "Finally our review identified a potential cost savings to the department if it phased out the use of RSA tokens..."

The report makes the assumption DOE could realize a savings of up to \$600,000.00 by eliminating the use of tokens. However, it is unclear if the need to purchase card readers for individuals approved for situational and/or scheduled flexiplace or network access while traveling was taken into consideration.

4. **An Overall Comment** - It should be noted that the report does not emphasize that the HSPD-12 mandate was not fully funded, which is a contributing factor to the delays in its implementation.

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 audit or 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 our office 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://energy.gov/ig>

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