GENERAL SERVICES ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

**REVIEW OF THE IMPLEMENTATION
OF HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12
REPORT NUMBER A060195/O/R/F07013
August 13, 2007**

U.S. General Services Administration
Office of Inspector General

Date: August 13, 2007

Reply to
Attn of:
R. Nicholas Goco
Deputy Assistant Inspector General
for Real Property Audits (JA-R)

Subject: Review of the Implementation of Homeland Security
Presidential Directive 12
Report Number A060195/O/R/F07013

To: Casey Coleman
Acting Chief Information Officer
Office of the Chief Information Officer (I)

This report presents the results of our review of the General Services Administration's
(GSA) implementation of the provisions of Homeland Security Presidential Directive 12
(HSPD-12). Primarily, the review assessed whether actions underway are adequate to
meet the Office of Management and Budget's (OMB) requirements and timeframes for
the implementation of HSPD-12, in accordance with Federal Information Processing
Standard Publication 201. Our review disclosed that GSA is moving forward in its
efforts to implement HSPD-12 and has met OMB's first two HSPD-12 deadlines.

It is unlikely, however, that GSA will meet OMB's October 27, 2007 deadline that
requires the issuance of HSPD-12 compliant cards to all contractors and employees
with 15 years or less of service due to the late award of a Managed Service Office
Service contractor and the limited card production capability of that contractor by the
deadline. Additional factors impacting GSA's effectiveness in implementing HSPD-12
include the lack of a detailed implementation plan and the absence of a central
database for contractors.

If you have any questions regarding this report, please contact me or R. Nicholas Goco,
Deputy Assistant Inspector General for Real Property Audits, on (202) 219-0088.

Susan P. Hall
Susan P. Hall
Audit Manager
Real Property Audit Office (JA-R)

**REVIEW OF THE IMPLEMENTATION
OF HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12
REPORT NUMBER A060195/O/R/F07013**

TABLE OF CONTENTS

REVIEW OF THE IMPLEMENTATION
OF HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12
REPORT NUMBER A060195/O/R/F07013

EXECUTIVE SUMMARY

Purpose

The objective of this review was to analyze whether actions underway are adequate to meet Office of Management and Budget (OMB) requirements and timeframes for the implementation of Homeland Security Presidential Directive 12 (HSPD-12) in accordance with Federal Information Processing Standard Publication 201 (FIPS 201), and if not, what corrective actions are needed.

Background

On August 27, 2004, President George W. Bush issued HSPD-12, which mandates the establishment of a common standard for identification credentials to be utilized by all Federal employees and contractors to gain physical and logical access to Federally controlled facilities and information systems. On February 25, 2005, the National Institute of Standards and Technology (NIST) published FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS 201 consists of two parts; the standards in PIV I support the control objectives and security requirements described in HSPD-12. The PIV II standards support the technical interoperability requirements described in HSPD-12 and specifies standards for implementing smart cards as identity credentials for use in the PIV system, including the collection, storage, and management of documentation needed to authenticate an individual's identity. On August 5, 2005, OMB issued a memorandum, "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (M-05-24), which set deadlines for HSPD-12 implementation. The first major deadline, October 27, 2005, required all agencies to establish control objectives and a common identity proofing process, as well as the registration and issuance process, and security controls. The subsequent deadline of October 27, 2006, required all agencies to begin the issuance of PIV II compliant credentials. Upcoming deadlines, falling on October 27, 2007 and October 27, 2008, require agencies to complete background investigations and issue PIV cards to all contractors and employees with fifteen years or less Federal service and those employees with greater than fifteen years of service, respectively.

The GSA HSPD-12 Project Management Office (PMO) of the Office of the Chief Information Officer was created to manage GSA's implementation of HSPD-12. In addition to the PMO, the GSA Federal Acquisition Service launched the

HSPD-12 Managed Service Office (MSO) to utilize competitively selected contract vehicles to provide all project, acquisition, and financial management necessary for GSA's customer agencies to satisfy the requirements of OMB M-05-24.

Results in Brief

GSA has met OMB's first two deadlines requiring issuance of operating procedures by October 27, 2005, and the production of a PIV II compliant card by October 27, 2006. GSA is also continuing to move forward in such aspects of HSPD-12 implementation as processing employee and contractor background investigations, developing plans for logical and physical access, and updating its general HSPD-12 policies. However, GSA will likely not meet OMB's October 27, 2007 deadline that requires the issuance of PIV II compliant cards to all contractors and employees with 15 years or less of service due to the late award of a MSO Service contractor and the limited PIV card production capability of that contractor by the deadline. In addition to the MSO Service contractor currently being inoperative, GSA is faced with other obstacles affecting its ability to implement HSPD-12. These include the lack of a detailed HSPD-12 implementation plan and the absence of a centralized database capturing GSA-wide contractor information.

Recommendations

To remedy the situation, the OCIO needs to address factors that will impact its effectiveness in implementing HSPD-12. These steps include having the PMO manager and HSPD-12 stakeholders work together to establish a detailed implementation plan outlining how GSA plans to implement HSPD-12 in its entirety and establishing a contractor identity management system, while expediting background investigations for embedded contractors.

**Review of the Implementation
of Homeland Security
Presidential Directive 12
Report Number A060195/O/R/F07013**

Introduction

Background

On August 27, 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. HSPD-12 mandates the establishment of a common standard for identification credentials to be utilized by all Federal employees and contractors to gain physical and logical access to Federally controlled facilities and information systems. This directive is intended to enhance security, reduce identity fraud, increase the efficiency of identity proofing and verification, and protect the personal privacy of those issued government credentials.

The Department of Commerce and the National Institute of Standards and Technology (NIST) were tasked with publishing a definition for common identification standards required by HSPD-12. On February 25, 2005, NIST published Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors. The standards required by HSPD-12 are made tangible in the form of a PIV card that adheres to the specifications defined in FIPS 201 and is to be used for both physical and logical access control, as well as any other agency-specific applications. FIPS 201 consists of two parts; the standards in PIV I support the control objectives and security requirements described in HSPD-12. The PIV II standards support the technical interoperability requirements described in HSPD -12 and specifies standards for implementing smart cards as identity credentials for use in the PIV system, including the collection, storage, and management of documentation needed to authenticate an individual's identity.

HSPD-12 requires Federal credentials to be secure and reliable, which is defined as a credential that: is issued based on sound criteria for verifying an individual's identity; is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; can be rapidly authenticated electronically; and is issued only by providers whose reliability has been established by an official accreditation process. The primary requirements for an agency to implement HSPD-12 are to revise the identity proofing and card issuance process of the agency to meet FIPS 201 requirements. FIPS 201 requirements include the issuance of an identity credential that utilizes smart card technology (both contact and contactless), and incorporates a standardized Card Holder Unique Identifier (CHUID), digital credentials, and biometric templates.

The major milestones for HSPD-12 implementation are outlined in Office of Management and Budget (OMB) memorandum "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (M-05-24), dated August 5, 2005. The first major deadline, October 27, 2005, required all agencies to establish control objectives and a common identity proofing process, as well as the registration and issuance process, and security controls. The subsequent deadline of October 27, 2006, required all agencies to begin the issuance of PIV II compliant credentials. The upcoming OMB deadline of October 27, 2007, requires agencies to issue PIV cards to all contractors and employees with 15 years or less of Federal service after a successful fingerprint check and a background investigation is started or complete. The final OMB deadline of October 27, 2008, requires agencies to issue PIV cards to all employees with greater than 15 years of Federal service after a successful fingerprint check and a background investigation is started or complete.

The General Services Administration (GSA) HSPD-12 Program Management Office (PMO) of the Office of the Chief Information Officer was created to develop the PIV system architecture, as well as perform analysis of access controls, coordinate training and communication, provide transition plans from the old credentialing system to the PIV system, and to assume responsibility for GSA's internal credentialing.

The GSA Federal Acquisition Service launched the HSPD-12 Managed Service Office (MSO) in response to HSPD-12. The MSO's mission is to utilize competitively selected contract vehicles to provide all project, acquisition, and financial management necessary for GSA's customer agencies to satisfy the requirements of OMB M-05-24. Although the MSO is not a mandatory source of supply, it was established to provide centralized shared services for contributing agencies who wish to take advantage of the cost savings and efficiencies realized from establishing a common, government-wide shared services platform.

Objective, Scope, and Methodology

The audit objective was to analyze whether actions underway are adequate to meet OMB requirements and timeframes for the implementation of HSPD-12 in accordance with FIPS 201, and if not, what corrective actions are needed.

To accomplish this audit objective we performed fieldwork primarily in the National Office. During fieldwork, we performed the following tasks:

* Obtained background information including: OMB memorandums, NIST publications, prior Government Accountability Office and GSA Office of Inspector General audit reports.
* Analyzed numerous GSA documents generated through the HSPD-12 PMO, the MSO, Office of Acquisition Policy, and Public Buildings Service (PBS)

such as; HSPD-12 Standard Operating Procedures, HSPD-12 Draft Informational Letter, PMO Business Plan and the HSPD-12 Implementation Overview.

∗ Held discussions with officials in the HSPD-12 PMO, the MSO, PBS, and the Office of the Chief Human Capital Officer (CHCO).

∗ Discussed the current use of building access systems and the planned transition to PIV II compliant access systems with regional credentialing officers.

∗ Analyzed a Memorandum of Understanding (MOU) between the PMO and MSO for management and service support for PIV credentials through a shared service solution.

∗ Analyzed a Memorandum of Agreement between GSA and the Department of Homeland Security for background investigation services.

∗ Analyzed HSPD-12 contracting language and the MSO Request for Quotations.

∗ Observed the enrollment process at the MSO registration station in the National Capital Region.

∗ Reviewed the bi-weekly HSPD-12 Stakeholders Meeting Minutes and the monthly HSPD-12 Program Management Updates.

The audit work was conducted from November 2006 to March 2007. The fieldwork primarily focused on the operations of the PMO office. A review of management controls was not performed due to the limited number of PIV II compliant cards currently issued. It is planned that testing of management controls will be conducted in a subsequent review when the new MSO contractor has been established.

The audit was performed in accordance with generally accepted government auditing standards.

Results of Audit

The General Services Administration (GSA) has been moving forward in its efforts to implement aspects of Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, by ensuring that it meets background investigation processing requirements and developing supplemental agency policy to meet the new requirements. In addition, GSA is beginning to develop plans on how it will utilize the PIV cards for logical and physical access.

GSA has met the Office of Management and Budget's (OMB) first two deadlines requiring agencies to establish an identity proofing and registration process meeting the control objectives in FIPS 201 by October 27, 2005, and to begin deploying PIV II compliant cards by October 27, 2006. However, it is unlikely GSA will meet the October 27, 2007 deadline requiring the issuance of PIV II compliant cards to all contractors, and to all employees with 15 years or less of service. As of March 1, 2007, GSA had only issued 71 PIV II cards and since the contract vehicle for the PIV II cards has been recompeted, GSA will most likely be unable to obtain the required number of PIV II cards by the October 27, 2007 deadline.

GSA needs to address additional factors that will impact its effectiveness in implementing HSPD-12 including the lack of a detailed HSPD-12 implementation plan and absence of a centralized database capturing GSA-wide contractor information.

GSA Has Been Moving Forward in Implementing HSPD-12 Requirements

GSA has been moving forward in its efforts to implement aspects of HSPD-12 and FIPS 201. It has been ensuring that it meets background investigation processing requirements and developing supplemental agency policy to meet the new requirements. In addition, GSA is beginning to develop plans on how it will utilize the PIV cards for logical and physical access.

To meet the background processing requirements of HSPD-12 and FIPS 201, GSA has established standard operating procedures for personal identity verification and has been working to ensure all required background investigations are performed. As of October 17, 2005, GSA adopted new standard operating procedures for personnel security. According to this policy, before a new associate or contractor is issued an identity credential, the agency must initiate a National Agency Check with Written Inquiries (NACI), and favorable results must be received from the FBI National Criminal History Check (fingerprint check). Once a favorable fingerprint check is received a PIV II card can be issued and the user will have access to low impact applications such as desktop applications, network access, email access, and home directory access.

When a favorable NACI is received and is adjudicated, a process often taking 2 to 3 months, the user will gain access to GSA moderate impact applications that may contain privacy act information.

GSA has also been working to ensure all required background investigations will be performed. The GSA Personnel Security Requirements Division (Division) within the Office of the Chief Human Capital Officer is primarily responsible for the direction, guidance, and interpretation of HSPD-12 and FIPS 201 background investigation requirements. As of March 2007, the Division has identified a possible 716 GSA employees and the PMO identified an estimated 63,000 embedded and PBS contractors that may need background investigations to meet OMB's October 27, 2007 deadline. The Division is working to complete all fingerprint checks and start the NACI investigations for GSA employees before October 27, 2007, as required. To assist in processing background clearances for contractors, GSA has entered into a Memorandum of Agreement with the Department of Homeland Security, Federal Protective Service, to provide background investigations and suitability determinations.

GSA has also been developing supplemental policies to meet HSPD -12 requirements. On April 12, 2007, GSA issued Standard Operating Procedures for HSPD-12 Personal Identity Verification and Credentialing. Additionally, it is currently drafting the GSA HSPD-12 PIV Informational Letter to supplement instructions contained in other GSA policy documents[1]. These documents provide guidance on many aspects of GSA's implementation of HSPD-12 including the HSPD-12 Investigation and Adjudication Process, PIV Credentialing Procedures, System and Network Security Access, and Physical Access to GSA-Controlled Facilities. Currently, the Informational Letter is in a draft state with varying degrees of completeness. There is no firm date on when this document will become the official policy of GSA.

Finally, GSA has begun to develop plans on how it will utilize the PIV cards for logical and physical access. GSA efforts to implement logical access using the PIV II cards have been influenced by OMB memorandum "Protection of Sensitive Agency Information" (M-06-16), which lists specific actions to be taken by Federal agencies for the protection of Personally Identifiable Information (PII). The specific intent of OMB memo M-06-16 is to compensate for the protections offered by the physical security controls when information is removed from, or accessed from, outside of the agency location. GSA intends to use the PIV II card to satisfy the directive's requirement of allowing remote access to PII with two-factor authentication where one of the factors is provided by a device separated from the computer gaining access. GSA also intends to utilize the capabilities of the card as a control for employees to log into their laptop and desktop computers. The PMO is partnering with the Directory Services PMO to

---

[1] These policies include GSA Handbook on Suitability and Personnel Security (ADM P 9732.1C); GSA Nationwide Credentials Handbook (ADM P7640.2); GSA Information Technology Security Policy (CIO P 2100.1C); and the General Services Acquisition Manual.

develop requirements for using the PIV II card for network and application access, and will be conducting a pilot program for logical access using 50 individuals with PIV II cards.

To address physical access control systems to be used in GSA leased and owned buildings, the PMO has arranged for a contractor to conduct a survey to determine the kinds of physical access controls that are currently in place across the approximately 9,000 buildings managed by GSA. This survey will result in an analysis to determine an approach to update and/or replace physical access control systems for GSA leased and owned buildings that are not HSPD-12 compliant. Once this is completed, the PMO will partner with the Public Buildings Service (PBS) to develop a plan to implement compliant physical access systems in Federal buildings.[2] Using a risk-based approach, PBS intends to issue policy regarding HSPD-12 responsibilities for access control procedures; including funding and installation of physical access controls. Current guidance from the PBS Assistant Commissioner's office on card readers is that PBS will be responsible for funding only in those locations where PBS is an occupant, and will fund a prorated share along with the other building occupants. Building Security Committees will be responsible for determining building specific access control procedures. PBS plans to model its policy upon the Interagency Security Committee draft report of October 23, 2006, *Physical Security System Migration Strategy Overview*.

Lack of a HSPD-12 Service Contractor Hinders GSA's Ability to Meet OMB's October 27, 2007 Deadline

GSA has met OMB's first two deadlines requiring agencies to establish an identity proofing and registration process meeting the control objectives in FIPS 201 by October 27, 2005, and to begin deploying PIV II compliant cards by October 27, 2006. However, it is unlikely GSA will meet the October 27, 2007 deadline requiring the issuance of PIV II compliant cards to all contractors and employees with 15 years or less of service. As of March 1, 2007, GSA had only issued 71 PIV II compliant cards and since the contract vehicle for the PIV II cards has been recompeted, GSA will likely be unable to obtain the required number of PIV II cards by the October 27, 2007 deadline.

In September 2006, the decision was made that the PMO would obtain the PIV II compliant cards through the GSA's Federal Acquisition Service (FAS) HSPD-12 Managed Service Office (MSO). Accordingly, the Office of the Chief Information Officer PMO entered into a Memorandum of Understanding (MOU) with the FAS MSO. Under the terms of this MOU, the MSO is responsible for providing end-to-end services, including enrollment processing, systems infrastructure, PKI certificates, card production, issuance, and maintenance. These services were being provided through the MSO offering contract that was awarded in August

---

[2] Currently, compliant solutions for access controls are limited and still undergoing development and certification.

2006 to BearingPoint for $104 million over an initial contract period of six months and options to extend the contract for a total of five years. The MSO also established four pilot registration stations in Atlanta, Seattle, New York City and Washington, D.C.

The PMO met the October 27, 2006, deadline by issuing six PIV II compliant cards via the MSO contract. However, shortly after the MSO contractor produced these PIV II compliant cards, FAS decided not to exercise the option under the contract to extend the initial contract period beyond the initial 6-month term. Since a change in contractor may create additional transition issues, GSA has been reluctant to issue a large number of PIV II cards. As of March 1, 2007, GSA had issued a total of 71 PIV II compliant cards. Instead, GSA has been primarily issuing legacy identification and credentials, such as the GSA Smart Card Credential, to new employees and contractors.

On January 12, 2007, GSA issued a solicitation requesting quotes for an offeror to provide end-to-end HSPD-12 services. The solicitation specifies that GSA FAS is offering services through this solicitation and subsequent contract as a shared service solution to all Federal government agencies. The solicitation notes that approximately 40 agencies have executed agreements with GSA to obtain services through this offering.[3] This represents approximately 420,000 Federal employees and offerors to be enrolled and issued credentials in the PIV Program through this vehicle. The contract was awarded on April 24, 2007; with roll out scheduled to begin July 2007. As part of the roll out, 225 enrollment stations are to be established nationwide by April 2008. These dates are predicated on a trouble-free completion of the certification and accreditation process and the resolution of the May 1, 2007 protests of the contract award.

The FAS MSO currently estimates that they will be able to produce only 61,280 cards by the October 27, 2007 deadline, and these must be allocated across the 42 agencies with agreements with the MSO. However, GSA estimates that it alone requires approximately 67,110 PIV II credentials for approximately 4,110 employees with 15 years of service or less and 63,000 contractors requiring credentials by the October 2007 deadline. Given these statistics, it is unlikely that GSA will be able to meet OMB's October 27, 2007 deadline. While waiting for the new MSO Service contractor to come on line, GSA plans to continue issuing non-compliant smart cards to its employees and contractors.

Also in abeyance until the new MSO Service contractor is fully functional is the essential HSPD-12 related training. Previously, role based training had been available to applicable GSA employees through an on-line system. We have been advised that this training has been suspended until after the new MSO contract has been awarded.

---

[3] As of April 2007, 42 agencies have executed agreements with GSA to obtain services through this offering.

Additional Obstacles Impacting GSA's Ability to Implement HSPD-12

While the MSO Service contractor limitations are a major impediment to GSA's effort to implement HSPD-12, other factors are also impacting implementation, such as the lengthy absence of a Program Manager for the HSPD-12 PMO, the need for a detailed HSPD-12 implementation plan, and the absence of a centralized database consolidating contractor information.

PMO Program Manager Vacancy

The former Program Manager of the GSA HSPD-12 PMO retired unexpectedly on January 3, 2007. Up until May 27 2007, the PMO continued with only an Acting Program Manager coordinating GSA's efforts to implement HSPD-12. For this five month period a permanent Program Manager was not in place to help coordinate the major components of GSA's HSPD-12 program which includes the acquisition of GSA Smart Cards from the MSO, physical access, logical access, and the maintenance of legacy smart cards. Numerous GSA service and staff offices (SSO) are involved in developing these major components such as: Office of the Chief Information Officer, Office of the Chief Human Capital Officer, Office of the Chief Acquisition Officer and PBS, and strong leadership was needed to coordinate everyone's efforts. With the number of SSOs involved in the HSPD-12 effort, an overall Program Manager was needed to direct and monitor the many facets of HSPD-12.

The Need for a Detailed HSPD-12 Implementation Plan

On July 11, 2006, the PMO issued a business plan that detailed GSA's alternative strategies to perform card issuance services internally as well as contracting out these services to a vendor, such as through the MSO. Once the decision was made to utilize the MSO Service contractor, a substantial part of the business plan became obsolete; however, a revised plan was not developed. On March 19, 2007, the PMO issued a GSA HSPD-12 Implementation Overview. Per the PMO, "This document is a high-level overview combining GSA's HSPD - 12 internal project plan and implementation plan and depicts the overall effort, timeline and projection of card issuance costs through FY '08." While this does provide a basic strategy for implementing HSPD-12, as the new MSO contractor comes on line and the technology for physical access controls becomes better defined a more detailed plan needs to be developed.

A detailed implementation plan is needed to ensure the success of the overall HSPD-12 program, as there are several issues that need to be addressed. For example, maintaining the operations of physical access control systems during the HSPD-12 PIV transition period is an area of concern. Currently, multiple

GSA Regions utilize Smart Card reader based physical access systems[4]. In addition, due to the multi-year deadline for full transition to the PIV II cards, employees with less than 15 years service may receive PIV II cards prior to employees with more years of service. To continue operating physical access control systems during the transition period, all employees within a building or office using Smart Card readers will still need the legacy GSA Smart Card. As a result, GSA may have to not just maintain, but also continue to issue legacy GSA Smart Cards to new employees until all building occupants have been provided PIV II cards and current access systems have been updated or replaced by systems that are PIV II compliant.

Although it is difficult to develop a final detailed implementation plan without the MSO contract vehicle in place, the issues surrounding the transition to, and implementation of, the PIV II card need to be addressed. As such, in developing and maintaining a detailed implementation plan, consideration will need to be given to how existing GSA functions will be impacted as the MSO contractor becomes fully operational. Currently, GSA credentialing officials are responsible for several tasks related to GSA card registration. Depending on the services provided by the MSO, some tasks might shift to the MSO Service contractor. If so, the role of the credentialing official will need to be assessed and the implementation plan updated to reflect any changes.

Absence of a Centralized Contractor Database

As noted previously, OMB memorandum "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (M-05-24), dated August 5, 2005, requires agencies to issue PIV cards to all applicable contractors by October 27, 2007. Effective January 3, 2006, Federal Acquisition Regulation (FAR) Parts 2, 4, 7, and 52 were revised to require solicitations and contracts to include requirements that contractors who have access to Federally-controlled facilities and information systems comply with the agency's personal identity verification process. In response to these changes, a letter was issued by the GSA Chief Acquisition Officer, effective February 3, 2006, instructing all GSA contracting associates to include the FAR clauses as well as any agency specific guidance for personal identity verification in all solicitations and contracts issued and awarded on or after October 27, 2005. In addition, contracts awarded prior to this date that are still active (more than three months from expiration) must be modified by October 27, 2007, to include the FAR clauses as well as any agency specific changes in accordance with the implementation of FIPS 201 and OMB memorandum M-05-24.

---

[4] Card readers using the GSA smart card credential are used for building and/or office access in the New England, Mid-Atlantic, and Rocky Mountain regions. The Northeast & Caribbean region uses its own unique smart card credential for access to several buildings in New York City.

While the PMO estimates that there are 13,000 embedded contractors and 50,000 PBS contractors, there is no centralized database that contains a record of all GSA contractors requiring the level of physical and systems access that necessitates favorably adjudicated background investigations and fingerprint checks. Because of this, GSA's Background Investigation Division is unsure of the true number of contractors, and correspondingly, unsure whether all contractors will have background investigations completed by the OMB deadline.

GSA has utilized embedded contractors prior to the requirements of HSPD-12. Many of these contractors may have current physical and systems access without having the level of background checks required by HSPD-12. Consequently, given the impediments to full realization of the goals of HSPD-12, embedded contractors may have physical and logical access far beyond the OMB deadlines. As such, GSA needs to expedite background investigations for embedded contractors that currently have access to GSA systems.

The PMO has raised concerns in this area, noting that there are five sources containing information on contractors, all with different populations and data formats. Consequently, the PMO proposes the establishment of a contractor identity management system, with mandatory enrollment for all current GSA contractors. We agree with the need for a contractor identity management system and recommend that such a system be put into operation.

Conclusion

Although GSA has met OMB's first two deadlines and it continues to move forward in such areas as processing employee and contractor background investigations, developing plans for logical and physical access, and updating general HSPD-12 policies, GSA will likely not meet OMB's October 27, 2007 deadline as a result of the late award of a MSO Service contractor and the limited PIV card production capability of that contractor. In addition to the MSO Service contractor limitations, GSA is faced with other obstacles affecting its ability to implement HSPD-12 such as the absence of a centralized database for contractor information and the need for a detailed HSPD-12 implementation plan. To ensure that GSA meets future OMB deadlines and implementation of HSPD-12 as envisioned by the President, the Chief Information Officer should have the PMO Manager and HSPD-12 stakeholders work together to establish a detailed implementation plan outlining how GSA plans to implement HSPD-12 in its entirety and establish a contractor identity management system, while expediting background investigations for embedded contractors.

As the OMB deadlines draw near, there also is a distinct possibility that background investigations processed by the Office of Personnel Management (OPM) may become backlogged. Within GSA alone, background investigations for employees, and contractors could reach over 67,000. However, this number could be over/under estimated due to the fact GSA does not have a centralized

database that tracks the number of actual GSA contractors. When taking into account all the other government agencies needing background investigations, there is a good possibility of a backlog at OPM. While employees and contractors can obtain limited access to GSA facilities and computer systems with an acceptable fingerprint check, full access to internal computer systems will not be authorized. Backlogs in the performance of background investigations by OPM will have a direct impact on agencies ability to accomplish their mission.

Recommendations

We recommend that the Chief Information Officer take steps to ensure the successful implementation and management of HSPD-12 initiatives by:

1. Developing a detailed implementation plan outlining how GSA plans to implement HSPD-12 in its entirety; including how it will utilize the MSO Service contractor and implement logical and physical access throughout GSA.

2. Establishing a centralized contractor database. Enrollment in this system should be mandatory for all current and future contractors.

   a. Expediting background investigations for embedded contractors that currently have access to GSA systems.

Management Comments

Management concurred with the report findings. The Chief Information Officer's comments to this report are included as Appendix A.

Management Controls

A review of management controls was not performed due to the limited number of PIV II compliant cards currently issued. It is planned that testing of the management controls will be conducted in a subsequent review when the new MSO contractor has been established.

APPENDICES

APPENDIX A

REVIEW OF THE IMPLEMENTATION
OF HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12
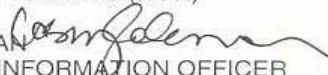## REPORT NUMBER A060195/O/R/F07013

Management's Response to the Draft Report

GSA

GSA Office of the Chief Information Officer

July 31, 2007

MEMORANDUM FOR R. NICHOLAS GOCO
        DEPUTY ASSISTANT INSPECTOR GENERAL FOR
        REAL PROPERTY AUDITS (JA-R)

FROM: CASEY COLEMAN
        ACTING CHIEF INFORMATION OFFICER
        OFFICE OF THE CHIEF INFORMATION OFFICER (I)

SUBJECT: Response to Draft Report – Review of the Implementation of
        Homeland Security - Presidential 12 Report Number A060195

Thank you for the opportunity to provide comments for inclusion with the audit report for the Implementation of Homeland Security Presidential 12 (HSPD-12). The Office of the Chief Information Officer (OCIO) concurs with the three recommendations made in the subject document as follows.

Recommendation 1: The GSA OCIO shall develop a detailed implementation plan outlining how GSA plans to implement HSPD-12 in its entirety; including how it will utilize the MSO Service contractor and implement logical and physical access throughout GSA.

Credential Issuance: The HSPD-12 Program Management Office (PMO) has prepared a draft detailed implementation plan for HSPD-12 credential issuance. The PMO is waiting for the Managed Service Office (MSO) to finalize its deployment plans so that the GSA HSPD-12 draft implementation plan can be finalized. We anticipate this to be finished by September 4, 2007.

Logical Access: The HSPD-12 PMO and the OCIO Directory Services Program Manager are conducting a pilot to test a proposed logical access solution using 50 persons selected from the various stakeholder organizations. The pilot test will validate the process for using smart cards for access to information technology assets as well as using two-factor authentication for remote access to sensitive information such as personally identifying information (PII). Upon completion of this test, a detailed implementation plan for moving GSA to utilizing smart cards for logical access will be developed.

U.S. General Services Administration
1800 F Street, NW
Washington DC 20405-0002
www.gsa.gov

APPENDIX A

Physical Access: The HSPD-12 PMO has produced an analysis of physical access control solutions throughout GSA-controlled office space. This analysis identifies a number of use-cases for controlling physical access in various building profiles and provides recommendations for migrating to an HSPD-12 compliant solution based on building security requirements. The HSPD-12 PMO will partner with the Public Building Service (PBS) security office to develop a migration strategy by October 1, 2007.

Recommendation 2: The GSA OCIO shall establish a centralized contractor database. Enrollment in this system should be mandatory for all current and future contractors.

The HSPD-12 PMO is currently gathering requirements for a Contractor Management and Credentialing Administration System. This system will track all GSA contractor personnel starting with contract award through contract closeout. Since OPM guidelines specify that personnel with less than a two-year break in service will not need a reinvestigation, contractors will have the option to have their personal data retained for up to two years so that they could begin work on a new contract immediately if within the two-year window. The prototype system is anticipated to be fielded in November 2007 for internal PMO use only with wider implementation upon certification and accreditation and full authority to operate.

Recommendation 2a: The GSA OCIO shall expedite background investigations for embedded contractors that currently have access to GSA systems.

The HSPD-12 PMO has partnered with the Office of the Chief Financial Officer (OCFO) to identify all contractors currently working in GSA facilities or accessing GSA computer systems. The OCFO was required to identify the number of contractors working in GSA facilities and asked the Services and Staff Offices to provide their contractors' name, phone number, email address, office symbol, and Government sponsor's name to the HSPD-12 PMO. This will allow the HSPD-12 PMO to cross check the embedded contractors against the CHRIS Security Tracking System and Federal Protective Service databases to ascertain which contractors need new background investigations initiated.

In summary, GSA is currently on-track to implement the investigation and credentialing requirements of HSPD-12 by the OMB milestone of October 27, 2008. Logical and physical access control measures will be phased-in once sufficient GSA personnel have the HSPD-12 identity card. If you have any questions regarding this matter, please contact Mr. William Erwin, Office of the Chief Information Office, at (202) 501-0758.

APPENDIX B

<div align="center">

**REVIEW OF THE IMPLEMENTATION
OF HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12
REPORT NUMBER A060195/O/R/F07013**

Report Distribution

</div>

<u>Copies</u>

Office of the Chief Information Officer (I) 3

Office of the Chief Human Capital Officer (C) 1

Office of the Chief Financial Officer (B) 2

Assistant Inspector General for Auditing (JA, JAO) 2

Assistant Inspector General for Investigations (JI) 1

Branch Chief, Audit Follow-up and Evaluation Branch (BECA) 1