VA Office of Inspector General

OFFICE OF AUDITS & EVALUATIONS

Department of Veterans Affairs

VA Has Opportunities to Strengthen Program Implementation of Homeland Security Presidential Directive 12

September 30, 2010
10-01575-262

ACRONYMS AND ABBREVIATIONS

AAIP	Authentication and Authorization Infrastructure Project
C&A	Certification and Accreditation
CIO	Chief Information Officer
FATO	Final Authority To Operate
FIPS	Federal Information Processing Standards
FMS	Financial Management System
FTE	Full-Time Employees
FY	Fiscal Year
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
IATO	Interim Authority To Operate
IAM	Identity and Access Management
IT	Information Technology
NIST	National Institute for Standards and Technology
OHR&A	Office of Human Resources and Administration
OI&T	Office of Information and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSP	Office of Operations, Security, and Preparedness
PACS	Physical Access Control System
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
PMO	Program Management Office
VA	Department of Veterans Affairs
VACO	Veterans Affairs Central Office
VISN	Veterans Integrated Service Network

Report Highlights: VA Has Opportunities to Strengthen Program Implementation of HSPD-12

Why We Did This Audit

This audit evaluated VA's progress in implementing a reliable and effective system of personal identity verification (PIV) in compliance with Homeland Security Presidential Directive 12 (HSPD-12). This Directive mandates the use of Government-wide identification credentials for employees and contractors.

What We Found

While VA has made little progress in implementing a reliable and effective program in compliance with HSPD-12, management efforts are underway to strengthen program implementation. VA is almost 2 years behind the Government-wide October 2008 deadline for full compliance with HSPD-12. As of June 2010, VA had only issued approximately 9 percent of the necessary credentials to its workforce, including contractors. In addition, VA issued some credentials without the required background investigations.

The PIV System used to support the credentialing process and HSPD-12 Program operations do not meet all critical mission requirements, and controls needed to track and provide accountability over program costs are weak. VA's lack of progress in implementing HSPD-12 occurred because it did not make it a priority or have an effective management structure in place to adequately direct this Department-wide effort. Although a Program Management Office (PMO) has been in place since October 2009, the PMO lacks the resources and critical management tools necessary to direct and operate a VA-wide program.

What We Recommend

We recommend the Assistant Secretary for Operations, Security, and Preparedness ensure that the PMO has the necessary resources and management tools in place to direct and implement the HSPD-12 Program. In addition, we recommend that the Assistant Secretary for Operations, Security, and Preparedness and the Assistant Secretary for Information Technology address PIV System and other operational deficiencies related to critical HSPD-12 Program requirements.

Agency Comments

The Assistant Secretary for Operations, Security, and Preparedness concurred with our findings and recommendations and provided target dates to complete planned actions. We consider their planned actions acceptable and will follow up on their implementation. Appendix D includes the full text of the Assistant Secretary for Operations, Security, and Preparedness comments.

(original signed by:)

BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

This audit assessed VA's progress in implementing a reliable and effective system of personal identity verification (PIV) in compliance with Homeland Security Presidential Directive 12 (HSPD-12) to improve the security of its facilities and to protect sensitive information stored in VA networks.

Homeland Security Presidential Directive 12

On August 27, 2004, the President of the United States signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, which mandated the use of Government-wide identification credentials for employees and contractors to enhance physical and logical security, increase efficiency, reduce identity fraud, and protect personal privacy. In February 2005, the Department of Commerce issued Federal Information Processing Standards (FIPS) Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. This publication established the minimum requirements for Agencies issuing credentials and for developing a Federal PIV System. To implement HSPD-12, on August 5, 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-24, *Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors.*

VA's HSPD-12 Program

In March 2009, VA designated the Office of Operations, Security, and Preparedness (OSP) as the overall VA Business Sponsor to provide policy, guidance, and oversight for the HSPD-12 Program. VA then established a Program Management Office (PMO) in October 2009. The Office of Information and Technology (OI&T) is responsible for analysis, design, implementation, operations and maintenance, help desk functions, field site deployment, full software development life cycle, and hardware/software procurement related to the HSPD-12 Program. By June 2010, VA had established approximately 200 Enrollment Centers, which were equipped to process applicant information and issue PIV credentials.

RESULTS AND RECOMMENDATIONS

Finding VA Has Made Little Progress Implementing the Personal Identification Verification Provisions of HSPD-12

Summary

Although VA is now making HSPD-12 implementation a priority, VA made little progress implementing a reliable and effective system of personal identity verification in compliance with HSPD-12 to enhance access security controls over VA facilities and systems. VA is almost 2 years behind OMB's October 2008 deadline for full compliance with HSPD-12 and is unlikely to meet the VA Chief of Staff's October 2011 deadline. Most notably:

- Our analysis of OMB and VA credential-issuing information relating to the 20 Federal Agencies authorized to manage their own PIV credential programs disclosed that 59 percent of Federal employees and other personnel required to obtain the enhanced-security ID cards had received them as of March 2010. However, as of June 2010, VA had only issued approximately 9 percent of the necessary credentials to its workforce, including contractors.

- The PIV System and program operations do not meet all critical mission requirements, and controls needed to track and provide accountability over program costs are weak.

- PIV credentials are not being used to enhance access controls over VA facilities and systems.

- Some credentials were issued without required background investigations.

VA's lack of progress in implementing HSPD-12 occurred because the Department did not have elements of an effective organizational structure in place. Further, VA management did not make it enough of a priority to adequately direct this Department-wide effort. Although a PMO has been in place since October 2009, the PMO lacks the resources and critical management tools necessary to direct and operate a VA-wide program.

As a result:

- Issuance of an estimated 741,000 credentials (needed for employees, contractors, and others) may not be completed before 2017.

- If the PIV System is not load tested, certified and accredited, and other unaddressed system requirements are not defined and/or resolved, VA cannot ensure that system performance will be reliable and effective and meet the requirements of HSPD-12.

Weaknesses in HSPD-12 Program management need immediate attention to minimize and mitigate the risks related to schedule slippage and performance issues, and to provide reasonable assurance and accountability over project costs. Appendix C provides a summary "scorecard" for the Department's performance in implementing key HSPD-12 Program requirements.

VA Met Some Critical HSPD-12 Milestones

Since HSPD-12 was signed in August 2004, VA has made some progress in implementing provisions of HSPD-12. Specifically:

- VA submitted the required HSPD-12 implementation plan to OMB prior to September 2006.

- VA's PIV credentials were accredited by the General Services Administration (GSA) in August 2008 and meet visible and electronic security features that comply with FIPS 201.

- VA adopted and accredited a registration process for PIV credential applicants.

- VA installed the equipment and services necessary to issue credentials to VA employees, contractors, and other personnel at approximately 200 PIV Enrollment Centers nationwide by June 2010.

Little Progress in Issuing PIV Credentials

Despite these achievements, VA has made limited progress in issuing PIV credentials to employees, contractors, and others. Under HSPD-12 and OMB memoranda, all Agencies must have completed background checks and issued credentials compliant with HSPD-12 to their workforce by October 27, 2008. Although many Agencies found meeting this milestone challenging, our analysis of OMB and VA credential-issuing information disclosed an estimated 59 percent of the Federal workforce received the required enhanced security ID cards by March 2010. However, as of June 2010, VA only issued about 76,000 (9 percent) of the estimated 817,000 PIV credentials to VA employees, contractors, and other personnel.

VA is unlikely to meet its revised milestone for fully complying with the requirements of HSPD-12. Senior officials advised that, in August 2009, the VA Chief of Staff established October 2011 as the revised milestone for VA to achieve full compliance with HSPD-12. The PMO's 2009 Business Plan indicates that not all PIV credentials will be issued before FY 2014.

To issue all credentials by October 2011, VA would need to issue an average of over 49,000 per month as of June 2010. We found VA has:

- Issued an average of only 8,100 credentials per month over a 3-month period (March 1, 2010–May 31, 2010).
- Never issued more than 9,600 credentials nationwide in any single month since deployment of the PIV System began in January 2008.

We therefore concluded that the Department is unlikely to issue all remaining credentials by 2014 and, at the current rate, is unlikely to issue the remaining credentials (estimated at about 741,000) before 2017.

A contributing factor to the inadequate rate of PIV credential issuance may be that a significant portion of the approximately 200 Enrollment Centers have issued relatively few PIV credentials. Of Enrollment Centers established before January 2010, ninety were operational for an average of 18 months and have not issued all their required credentials. Instead of each Enrollment Center issuing an average of seven credentials per workday, they have been issuing an average of only one credential per workday. Of the ninety Enrollment Centers, two have not issued any PIV credentials, even though they became operational in 2009. Additionally, 19 Enrollment Centers issued five percent or less of their required credentials, and 11 Enrollment Centers issued two percent or less of their required credentials.

Unmet Critical Mission and Operational Requirements

VA's PIV System and HSPD-12 Program operations do not meet certain critical mission requirements. Specifically, while deployed to approximately 200 Enrollment Centers, the PIV System has not been properly accredited and certified for operation, lacks the functionality to validate the identity of credential applicants, has not been tested to ensure the capacity to meet functional and performance needs, and cannot provide management with standard performance reports. Additionally, program operations lack effective controls for safeguarding personally identifiable information (PII), detecting unlawful and unauthorized PIV System activities, and restricting access to VA facilities and systems.

PIV System Lacks Key System Interfaces

The PIV System lacks the functional capability to interface with internal and external systems to verify PIV credential applicant information electronically. The PIV System cannot automatically validate the existence of a background investigation, an applicant's driver's license and other Government-issued identification, or whether the applicant is on a terrorist watch list, prior to issuing credentials.

OI&T's *PIV Integrated Project Plan* states the PIV System will interface with internal and external verification services to validate Government-issued identification, background checks of employees through VA's Personnel and Accounting Integrated Data System, and terrorist checks with the Federal Bureau of Investigations and other Agencies. In addition, FIPS 201 requires the use of an approved identity proofing and registration

process that includes, among other things, electronic verification of the authenticity of the source identification documents, such as a driver's license and validation using Government-wide databases and services in accordance with HSPD-11, *Comprehensive Terrorist-Related Screening Procedures.*

PIV System Needs Testing

VA does not have assurance the PIV System will meet the functional and performance needs of the HSPD-12 Program because VA has not defined or approved PIV System performance requirements or adequately tested the system against these benchmarks. OI&T's *Program Management Guide* requires developing a system's functional, performance, and reliability requirements and demonstrating that the system meets these requirements through testing before full-scale deployment. System speed was evaluated through stopwatch testing; however, OI&T only performed this limited testing more than three years after deployment of the PIV System began.

Additionally, VA did not perform required load testing of the PIV System to assess potential degradation under maximum operating conditions. They did not replicate demands placed on the PIV System as a result of simultaneous use by most of or all of the Enrollment Centers. Without functional and performance requirements, system testing will produce data of minimal value for benchmarking performance. Even though deployment began in January 2008, the OI&T Technical Team in charge of PIV System development and deployment did not initiate efforts to obtain appropriate load testing of the PIV System until September 2009.

PIV System Lacks Accreditation and Certification for Operation

The PIV System has not been adequately certified and accredited for operation. The PIV System has been fully deployed since June 2010, but it has never been granted a Full Authority to Operate (FATO) and instead, it has been operating under an Interim Authority to Operate (IATO) since January 2008.

Certification and Accreditation (C&A) is a process to ensure that Information Technology (IT) systems and major applications adhere to the established security requirements and is required by the Federal Information Security Management Act of 2002. VA Handbook 6500.3 requires that all VA systems undergo a C&A to ensure security controls meet all applicable requirements and are in place and working properly. Based on results of the assessment, the system will receive an IATO, a FATO, or a Denial of an Authority to Operate. While VA policy allows an IATO to be granted for up to 6 months, a FATO is necessary prior to a VA-wide deployment. However, in violation of VA policy, the PIV System has been operating under an IATO for more than 2½ years.

PIV System Lacks Standard Performance Reports

The PIV System does not provide standard performance reports to assist the PMO, system administrators, and other users to effectively manage the HSPD-12 Program. Although OI&T's PIV *Configuration Management Plan* states the PIV System will provide management with incident, problem, and

status reports, VA can only obtain limited information using ad hoc queries, which were termed by the PMO as not being "user-friendly." The PMO identified the need and has taken steps to define the requirements for standard performance reports, such as credentials:

- Issued by Enrollment Center and VA facility.
- Issued by card type (such as PIV, non-PIV, and Flash) and affiliation type (employee, contractor, and other personnel).
- Terminated by location.
- Issued without finger prints.
- Issued with a background check started versus finalized.

HSPD-12 Program Did Not Adequately Protect PII

The HSPD-12 Program operations did not adequately safeguard personal information collected from credential applicants from unauthorized disclosure. We found significant weaknesses in protection of information contained in the PIV System and in Enrollment Center operations. In addition, VA failed to adequately analyze and certify that PII collected as part of issuing credentials to meet the requirements of HSPD-12 were being adequately protected.

In April 2010, the VA Office of Inspector General (OIG) reported to the Assistant Secretary for Operations, Security, and Preparedness that more than 10,000 PIV System users had access without restriction to personal information of approximately 200,000 credential applicants in the system. System information available to all users on all enrollees and cardholders included items such as home addresses, phone numbers, dates of birth, and Social Security numbers. Further, while the PIV System has an automated "audit trail," the OI&T's Identity and Access Management (IAM) personnel advised that the automated function related to viewing records was not activated. They also indicated that no monitoring was being performed because IAM lacks the staffing to handle the volume of system user activity. In response, the PMO shut the PIV System down to implement stronger audit capabilities and enhance controls over user activity and access to PII.

Section 208 of the *E-Government Act* requires that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with IT systems that collect, maintain, and/or disseminate PII. However, VA has not completed a comprehensive PIA annually for the PIV System, as required, since FY 2007. While VA did prepare draft PIAs annually, none of those documents were approved by the Office of Cyber Information Security, nor did any of the assessments note control weaknesses associated with access to cardholder and applicant PII.

In addition, Enrollment Centers did not adequately protect PII from unauthorized disclosure due to the use of noncompliant shredders. VA deployed approximately 91 shredders that did not comply with FIPS 201 to Enrollment Centers to be used for destroying documents and PIV credentials that contain PII. We found that at least some of the shredders may still be in use as of April 2010, even though VA management was aware of the problem as early as August 2009 and directed the removal of the shredders in October 2009.

Management stated neither the PMO nor the VA Administrations provided oversight to ensure noncompliant shredders were removed. An inspection in April 2010, of the noncompliant shredder in the VA Central Office (VACO) Enrollment Office immediately after use, disclosed neatly cut, but clearly readable documents and what appeared to be an intact memory chip. Additionally, a general cleaning contractor removed the shredded contents and placed them in unsecure bins to await disposal.

PIV System User Activity Poorly Monitored

The HSPD-12 Program lacks effective monitoring of PIV System users for unlawful, unauthorized, or inappropriate activities. While the system administrator stated the actions of users are recorded and retained when creating or editing records, the PIV System does not generate standard reports that management could use to identify potential suspicious activities. Even if the System could generate such reports, the PMO lacks the staffing necessary to analyze and investigate any system-identified activities. The PMO advised that steps were underway to define standard performance reports on user activity.

FIPS 201 requires Agencies to assure that the technologies used in the implementation of the PIV system allows for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program. Additionally, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires Agencies to create, protect, and retain IT audit records to enable monitoring, analyzing, investigating, and reporting of unlawful, unauthorized, or inappropriate IT activities. The PIV *Configuration Management Plan* states the PIV System will track the actions of specific roles and users and provide management with incident, problem, and status reports.

PIV Credentials Not Enhancing Security

VA is generally not using already issued PIV credentials to enhance access controls over VA facilities and systems, as required by HSPD-12. In many VA facilities, the HSPD-12 PIV credentials are not used differently than previously issued VA credentials. This is occurring because VA has yet to define the extent to which PIV credentials will be required to access facilities and information systems, develop plans, test software, or deploy the infrastructure necessary to implement these requirements.

OMB M-05-24 required the use of PIV credentials and card-to-reader interfaces that are FIPS-201 compliant and that Agencies perform a risk-based determination to establish controls over the access to facilities and systems by October 2007. However, VA has not fully defined or implemented physical and logical requirements. The PMO did not begin working with the OI&T to establish criteria to ensure Physical Access Control System (PACS) are compliant with FIPS 201 until April 2009. VA did not start surveying its sites regarding PACS used by each facility until April 2010, more than 2½ years after the October 2007 deadline. Additionally, the software necessary to allow FIPS 201-compliant card-to-reader interfaces with personal and other VA computers had not been tested until February 2009. Furthermore, actual use of the PIV credential identified technical issues with encryption key recovery (such as Public Key Infrastructure or PKI), and the memory chip on the PIV credential does not retain all previously issued PKI certificates. These issues remain unresolved.

Some PIV Cardholders Lack Background Investigations

VA issued PIV credentials to some employees without background investigations, and VA does not know how many contractors and other personnel require background investigations. In September 2009, VA identified 1,278 VACO employees with PIV credentials who did not possess the necessary background investigation, including seven SES-level employees. As of April 2010, 1,007 VACO employees, including these seven SES-level employees, still did not have the required completed background investigation. In addition, as of June 2010, VA did not know how many of the estimated 535,000 contractors and other personnel require a background investigation.

OMB M-05-24 required Agencies to complete background investigations on their entire workforce by October 2008. FIPS 201 requires Agencies to ensure that only individuals with a background investigation on record are issued PIV credentials. As of July 9, 2010, the HSPD-12 Program Manager stated the PMO will complete the identification of the total number of VA employees, contractors, and other personnel requiring background investigations by August 2010.

HSPD-12 Not a Consistent Priority

VA's lack of progress in implementing HSPD-12 occurred because it did not make it a priority to adequately direct this Department-wide effort. Further, VA did not consistently have elements of an effective management structure in place to direct this effort. Senior officials advised there were periods of time the program was not provided sufficient resources and attention. Responsibilities for the program passed between and among organizations since 2004, and the program experienced periods where it lacked a Program Manager, Business Plan, and Executive Committee. Although more attention and priority have been recently placed on the program, the PMO (established in October 2009) lacks the resources necessary to direct and operate a VA-wide program, performance metrics to measure progress, and

the necessary controls needed to accurately track and provide accountability over program costs.

Lack of Management Continuity

Frequent transfers and significant gaps in program management responsibilities hampered implementation of the HSPD-12 Program in the Department. Originally under the direction of OI&T from 2004 to 2005, VA transferred program responsibility to the Office of Human Resources and Administration (OHR&A) from 2005 to 2007. Under OHR&A's direction, the program reported significant progress and accomplishments. These achievements included:

- A required HSPD-12 Implementation Plan developed and submitted to OMB.
- A pilot-tested PIV System and processes.
- A draft VA Policy Directive and Handbook.
- A completed PIV-I rollout.
- Primary and backup data centers operational in August 2006.

After transferring the program to the Deputy Chief Information Officer (CIO) for the Office of Enterprise Development in April 2007, VA did not take adequate steps to ensure continuation of the Business Sponsor, Program Manager, and Executive Committee to guide the program. The Deputy CIO acknowledged that VA failed to meet OMB milestones during this period, in part, because the program was not considered a high priority by the Department or within OI&T; it lacked sufficient resources; and it lacked a Business Sponsor, Business Plan, and Executive Committee to assist in directing program implementation.

VA reestablished a Business Sponsor and Program Management Office within the OSP in October 2009. As the HSPD-12 Business Sponsor, OSP assumed responsibility for program management, communications, policy, training, defining requirements, and oversight of program implementation VA-wide. While OSP is responsible for managing the program, OI&T retained responsibility for developing, deploying, and managing the PIV System. Under OSP's direction, VA also developed a Business Plan and reestablished an Executive Committee comprised of Senior Executives representing each Administration and other stakeholders and commissioned a contractor assessment of the HSPD-12 Program.

PMO Lacks Necessary Resources and Management Tools

While steps taken by VA indicate a higher priority is currently being placed on HSPD-12 implementation, VA still does not have all of the necessary resources and management tools needed to successfully implement the program. VA has not developed milestones targeted for meeting the VA Chief of Staff's October 2011 deadline for implementing HSPD-12. In fact, the 2009 HSPD-12 Program Business Plan shows a timeline for full implementation after FY 2013. VA has yet to develop and implement measurement tools that establish baselines against which to measure program progress. Finally, three years have lapsed since OHR&A drafted the VA Directive and VA Handbook defining the roles, responsibilities, and processes for implementation and on-going operations of the program Department-wide, which VA has yet to finalize.

The PMO lacks the resources necessary to operate the HSPD-12 Program. While OSP's 2009 HSPD-12 Program Business Plan shows a requirement for seven Full-Time Employees (FTEs) and nine contractors, the PMO only had a staff of two FTEs and four contractors dedicated to this initiative as of June 2010. Inadequate staffing impairs the Program Manager from accomplishing important oversight responsibilities. PMO management indicated that it might take up to one year to fully staff the office. Without sufficient staff, the PMO will not be able to develop and monitor progress against quantifiable performance measures, provide adequate oversight and evaluation of program implementation at VACO and field sites, and present progress reports or scorecards to VA leadership on a regular basis.

Lack of Accountability over Program Costs

VA has not established adequate accountability for HSPD-12 Program costs or ensured reliable future estimates of resources needed to fully implement the program. Both the PMO's 2009 Business Plan and VA's draft Directives did not address estimating, tracking, and reporting of expenditures for implementing the Program and ongoing operations. Although actual cost information is available in the Department's Financial Management System (FMS), the PMO has not utilized the resource for monitoring program expenditures. Without assigning accountability over program spending and implementing an effective process to accurately account for expenditures, VA lacks reasonable assurance that amounts reported to OMB and Congress are accurate and reliable. VA could spend on average more than $490 per individual PIV credential issued with total costs exceeding $400 million through FY 2011.

Additionally, information for continued deployment of the PIV System, developing and deploying PACS VA-wide, and other operational and maintenance activities are not accumulated and reported in total under the PMO. Without complete and reliable information, VA is unable to accurately determine HSPD-12 Program expenditures or estimate funding needs in annual submissions to Congress.

The lack of a single organization or individual responsible for compiling all budgetary and cost data for the program may have contributed to VA underreporting more than $28.5 million in obligations for developing and deploying the PIV System in their Exhibit 300s submitted to OMB in FY 2007. While VA reported obligations totaling almost $5.8 million for the PIV System in FY 2007, we found that actual obligations for the same period totaled almost $34.3 million. As a result, VA significantly underreported HSPD-12 Program costs to OMB.

Conclusion

VA is not meeting its obligations under HSPD-12 to increase the security of VA facilities and IT systems and provide better protection for veterans and employees through personal identity verification and strong authentication for preventing logical and physical intrusions. Issuance of more than 90 percent of the required PIV credentials may not be completed until 2017. Further, the issuance of PIV credentials to certain personnel without required background investigations impairs the integrity of the HSPD-12 Program. VA has also made inadequate progress in defining the requirements and implementing VA-wide physical and logical security to make full use of the upgraded credentials. Lastly, if unaddressed system requirements are not defined and/or resolved, VA cannot ensure that system performance will be reliable and effective.

The lack of strong controls to track and report costs associated with implementing HSPD-12 and the inability to accurately forecast budgetary needs in the future places VA at risk of expending funds unnecessarily and not realizing the program security benefits as intended. Weaknesses in HSPD-12 Program management need immediate attention to minimize and mitigate the risks related to schedule slippage and performance issues and to provide reasonable assurance and accountability over project costs.

Recommendations

1. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, develop a plan to ensure the PIV System interfaces with internal and external systems to electronically verify PIV credential applicant information.
2. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is tested, certified, and accredited for operation.
3. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is modified to generate standard performance reports to assist the PMO, system administrators, and other users to effectively manage the HSPD-12 Program.

4. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is modified to provide effective monitoring of System users for unlawful, unauthorized, or inappropriate activities.
5. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the required Privacy Impact Assessment for the PIV System is prepared and approved annually.
6. We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, define the extent to which PIV credentials will be required to access VA facilities and information systems and develop plans to test and implement the infrastructure necessary to establish these controls.
7. We recommend the Assistant Secretary for Operations, Security, and Preparedness staff program vacancies in the HSPD-12 Program Management Office.
8. We recommend the Assistant Secretary for Operations, Security, and Preparedness finalize the VA Directive and VA Handbook defining the roles, responsibilities, and processes for implementation and ongoing operations of the HSPD-12 Program.
9. We recommend the Assistant Secretary for Operations, Security, and Preparedness develop quantifiable performance measures for the HSPD-12 Program.
10. We recommend the Assistant Secretary for Operations, Security, and Preparedness implement a formal oversight process to monitor progress in achieving compliance with the requirements of HSPD-12.
11. We recommend the Assistant Secretary for Operations, Security, and Preparedness establish accountability over program costs and estimated costs of future HSPD-12 operations.

Management Comments and OIG Response

The Assistant Secretary for Operations, Security, and Preparedness concurred with our findings and recommendations and provided target dates to complete planned actions. We consider the following summarized planned actions acceptable and will follow up on their implementation.

The Assistant Secretary indicated that OSP, in cooperation with an Integrated Project Team, is developing a comprehensive plan to direct OI&T, Administration, Staff Office, and HSPD-12 Program Office efforts. In addition, the Assistant Secretary's response indicated the Department is already taking significant steps to address identified PIV System and program management deficiencies in areas such as safeguarding personally identifiable information, access controls, system testing, program

performance measures, and system reporting and monitoring. The Assistant Secretary also indicated that OSP will be fully staffed by November 30, 2010, and OSP will work with other VA elements to identify program funding, obligations, expenditures, and estimations of future costs to provide management oversight of VA's HSPD-12 Program. The final completion date for corrective actions is expected to occur on or before September 30, 2012.

Appendix D contains the full comments of the Assistant Secretary for Operations, Security, and Preparedness.

Appendix A Background

Vulnerability of Traditional Government Identification

Until the recent past, ID cards issued to most Federal employees and contractors were used to access Federal facilities solely on the basis of visual inspection by security personnel. However, these traditional forms of credentials issued by individual Federal Agencies could be easily forged and other limitations contributed to an increased risk of identity theft and related security problems. One means available to reduce these risks is through the use of "smartcards." Unlike traditional identification credentials, smartcards contain an integrated memory chip capable of processing information in addition to storing and exchanging data with other systems.

Homeland Security Presidential Directive 12

The need to protect government facilities, information, and resources moved to the forefront in the wake of the terrorist attacks of September 11, 2001. In response, President George W. Bush issued the National Strategy for Homeland Security in July 2002, which sets forth three overall objectives to prevent terrorist attacks within the United States: (1) reduce America's vulnerability to terrorism, (2) minimize the damage, and (3) assist in the recovery from attacks that may occur. The President also issued a series of Homeland Security Presidential Directives, providing additional guidance related to the mission areas outlined in the National Strategy.

Recognizing that wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where a potential for terrorist attacks needed to be eliminated, the President signed HSPD-12 on August 27, 2004. The Directive established a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. Secure and reliable forms of identification are those that meet the security and control objectives of HSPD-12 by being: (1) issued based on sound criteria for verifying an individual employee's identity; (2) strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) rapidly authenticated electronically; and (4) issued only by providers whose reliability has been established by an official accreditation process.

FIPS 201

HSPD-12 assigned responsibility to the Secretary of Commerce to develop the Federal standard for secure and reliable forms of identification. Accordingly in February 2005, the National Institute of Standards and Technology (NIST) published FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* The standard specifies the technical requirements for PIV systems to issue secure and reliable forms of ID to Federal employees and contractors for gaining physical access to Federal facilities and logical access to information systems and software applications.

FIPS 201 is composed of two parts. The first part, called PIV-I, sets standards for PIV systems in three areas: (1) identity proofing and registration, (2) card issuance and maintenance, and (3) protection of card applicants' privacy. The second part of the FIPS 201 standard, PIV-II, provides technical specifications for interoperable PIV credentials.

OMB Implementing Guidance for HSPD-12 and Key Milestones

OMB is responsible for overseeing the implementation of HSPD-12 by executive agencies. In August 2005, OMB issued Memorandum M-05-24, *Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors,* which requires Federal Departments and Agencies to:

- Adopt and accredit an identity proofing, registration, and card issuance process for employees and contractors consistent with the security and control objectives of HSPD-12 by October 27, 2005.
- Begin deploying products and a card issuance system that meets the requirements of HSPD-12 by requiring PIV credentials for facility access and developing credentials that allow interoperability for physical and logical access by October 27, 2006.
- Issue and require the use of identity credentials for current employees and contractors by October 27, 2007.
- Verify and/or complete background investigations and issue PIV credentials for all employees by October 27, 2008.

PIV Credentials

The form factor for the HSPD-12 "common identification standard" is an integrated-circuit identification card (PIV credential) that contains identity credentials such as cryptographic keys and biometrics to achieve graduated levels of security from least secure to most secure, ensuring flexibility in selecting the appropriate level of security for Federal application. The identity credentials are stored and protected on an integrated memory chip. Cryptographic key material and personal identification numbers on the card provide for the protection of sensitive stored and communicated data using NIST approved algorithms.

VA's Implementation of HSPD-12 Requirements

The PIV Project began in VA in 2002 as the Authentication and Authorization Infrastructure Project (AAIP) managed by the Office of Cyber and Information Security. One of the objectives of AAIP was to establish an enterprise and standards-based authentication and authorization infrastructure framework. The initial conceptual approach for the VA PIV System was to build upon the existing AAIP System by adding the required functionality and services to achieve compliance with HSPD-12 and FIPS 201. The PIV System is compromised of sub-systems and primary interfaces designed to work collaboratively to provide the services required to meet the objectives of FIPS 201. These services include, among other

things, enrollment, identity and access management, security, data support, audit functions, card management, and PKI.

On March 25, 2009, OSP was designated as the overall VA Business Sponsor to provide policy, guidance, and oversight for the HSPD-12 Program. As HSPD-12 Business Sponsor, OSP is responsible for program management, communications, policy, training, defining requirements, and oversight for VACO and national implementation of the program. In addition, the Business Sponsor supervises the VACO HSPD-12 Enrollment Office. OI&T, the current IT Program Management Office, is responsible for analysis, design, implementation, operations and maintenance, help desk functions, field site deployment, full software development life cycle, and hardware/software procurement related to HSPD-12 Program.

OMB Concerns with VA's Implementation of HSPD-12

At a January 2010 meeting with VA officials, OMB expressed significant concerns, including the lack of adequate governance, the lack of a clear strategy or plan, and concerns regarding HSPD-12 Program management. OMB personnel stated that VA senior leadership provided little oversight and lacked program management accountability for VA's HSPD-12 Program. At the time, OMB noted that only 6 percent of the VA workforce had been issued credentials and deployment of the credentialing infrastructure was incomplete. OMB also observed that since 2005, multiple program managers were assigned to the VA HSPD-12 Program. OMB also remarked that VA has not updated its HSPD-12 implementation plan since 2006. OMB officials also noted that PMO appeared to have limited influence over the activities of the CIO staff responsible for contract oversight and the Human Resources staff responsible for tracking investigations. OMB also noted that VA did not complete a December 2009 quarterly status report. After almost 3 years of OMB requests, VA had not reported the status of the background investigations required by HSPD-12.

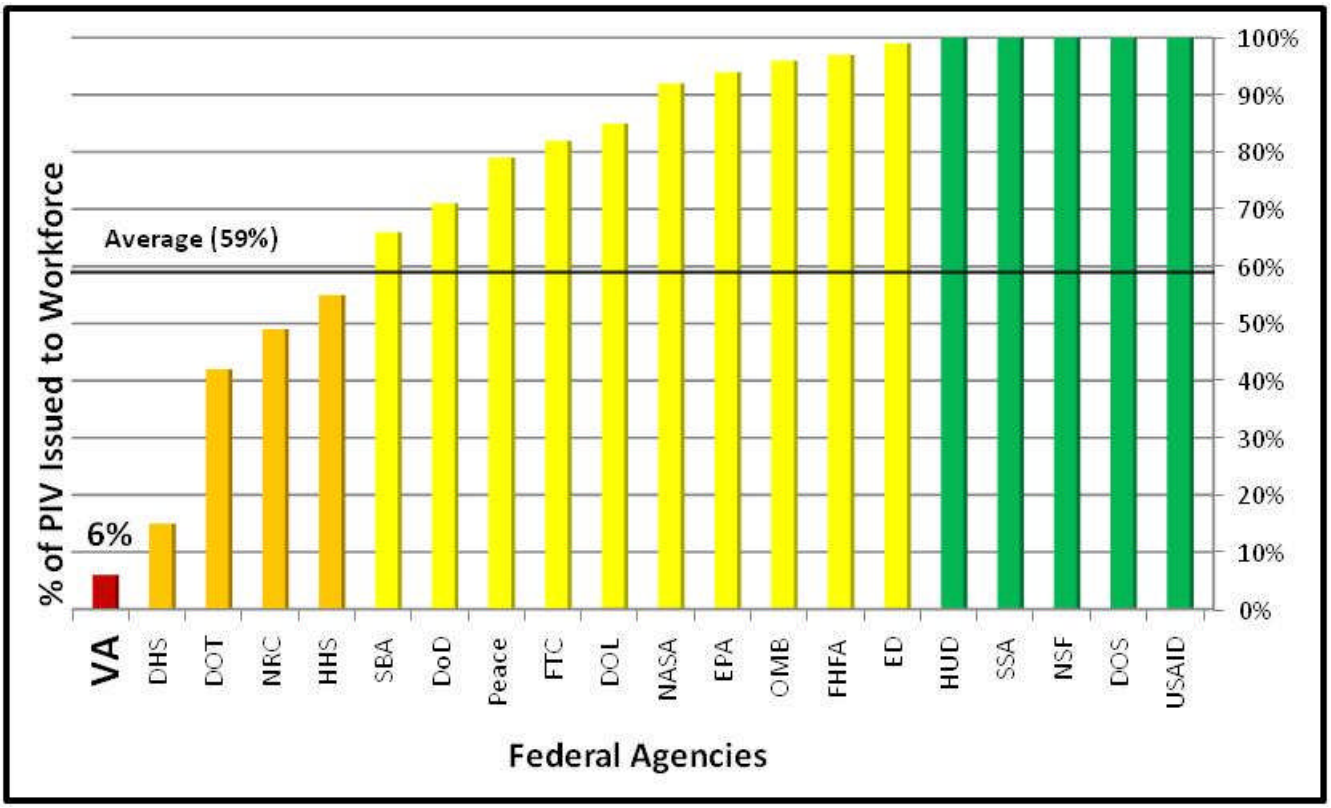
Comparison of VA to Other Agencies

We analyzed OMB and VA credential-issuing information relating to Federal Agencies authorized to develop and issue their own PIV credentials as of March 2010.[1] Our analysis disclosed the 20 Agencies issued 3.3 million (59 percent) of the 5.5 million credentials to employees, contractors, and other personnel. Our analysis also disclosed the Department of Defense (DOD) accounted for 4 million (73 percent) of the 5.5 million required credentials. Excluding DOD's information, the remaining 19 Agencies issued 455,217 (29 percent) of the 1.5 million credentials to employees, contractors, and other personnel. As shown in Figure 1, VA had only issued six percent of the estimated 817,000 credentials to its workforce as of March 2010. We did not verify the reliability and accuracy of the data. We

[1] GSA is providing PIV credential services to other Federal clients.

obtained updated data that indicated that, as of June 2010, VA had issued approximately nine percent of the required PIV credentials.

Figure 1. PIV Credentials Issued to Workforce by Federal Agencies
(As of March 2010*)



*The information presented above was calculated using Agency self-reported credential issuance information published in the March 2010 OMB status report.

AGENCY ACRONYMS			
DHS	Department of Homeland Security	**HUD**	Department of Housing & Urban Development
DOD	Department of Defense	**NASA**	National Aeronautics & Space Administration
DOL	Department of Labor	**NRC**	Nuclear Regulatory Commission
DOS	Department of State	**NSF**	National Science Foundation
DOT	Department of Transportation	**OMB**	Office of Management & Budget
ED	Department of Education	**Peace**	Peace Corps
EPA	Environmental Protection Agency	**SBA**	Small Business Administration
FHFA	Federal Housing Finance Agency	**SSA**	Social Security Administration
FTC	Federal Trade Commission	**USAID**	US Agency for International Development
HHS	Department of Health & Human Services	**VA**	Department of Veterans Affairs

Appendix B Scope and Methodology

Our audit focused on VA's implementation of the HSPD-12 Program for Calendar Years 2003–2010.

To assess the Department's progress in implementing the requirements of HSPD-12, we reviewed laws, regulations, policies, and external reviews applicable to HSPD-12. We interviewed VA's HSPD-12 Program Management Office; VA's PIV Project Manager and PIV Project team members; the Director of Personnel Security and Suitability Services; the VACO Director of Facility Services; and various representatives from VA, the Veterans Benefits Administration, and the Veterans Health Administration. We reviewed the strategic and program management plans for program funding, staffing, performance metrics, program monitoring, and policy development. We also reviewed VA's PIV Privacy Impact Assessments and implementation reports. We evaluated PIV System controls to assess its safeguarding of personal information and processing of PIV credentials.

We conducted our fieldwork from March 2010 through July 2010 at the Enrollment Centers in VACO, Washington, DC; Veterans Integrated Service Network (VISN) 8, VA Sunshine Healthcare Network, Bay Pines, FL; and James A. Haley Veterans' Hospital, Tampa, FL. We observed the processing of PIV credentials at Enrollment Offices at VACO, VISN 8, and James A. Haley Veterans' Hospital. We also evaluated whether background investigations were conducted for VACO employees. We reviewed the card management system certification and accreditation, functionality, and performance testing. We also analyzed VA's funding and tracking of PIV costs by reviewing VA's Congressional Submissions from FY 2009 to 2011, funding (obligated costs), and actual costs from VA's FMS. We also reviewed the budgeted costs presented in the PMO Business Plan.

Reliability of Computer Processed Data

We obtained and analyzed credential issuance data from the PIV System to support the scope of our audit. To assess the reliability of the computer-generated data, we tested for obvious errors in accuracy and completeness, reviewed existing information about the data and the system that produced them, and interviewed OI&T officials knowledgeable about the data. We determined the computer-generated data was sufficiently reliable to meet the audit objectives and support our recommendations. We also obtained and analyzed summary level financial data applicable to the PIV System from FMS. We compared the information in FMS to amounts reported in VA's Congressional Submissions. Our analysis concluded the summary level financial data was sufficiently reliable to meet the audit objectives and support our recommendations.

Compliance with Government Auditing Standards

Our assessment of internal controls focused on those controls relating to our audit objectives. We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix C VA Implementation of HSPD-12 "Scorecard"

Table 1. Implementation Status of VA HSPD-12 Program
(Includes OMB M-05-24 and FIPS 201 Requirements as of July 2010)

Selected HSPD-12 Program Requirements	OMB Milestone	VA Implementation Status	See Page
Submit an implementation plan to OMB	June 2005	Completed (documentation could not be located to identify the date)	-
Adopt and accredit a registration process	October 2005	Completed (documentation could not be located to identify the date)	-
Develop system to support the credentialing process	October 2005	Completed January 2008	-
Issue policy specifying roles and responsibilities	October 2005	In draft since August 2007	10
PIV credentials comply with FIPS 201 visible and electronic security features	October 2007	Completed August 2008	-
Issue and require use of identity credentials to access facilities and systems	October 2008	Only 9 percent of credentials issued as of June 2010 Up to 741,000 individuals may still require PIV credentials Physical and logical controls not implemented	2 4 8
Complete background investigations for all personnel	October 2008	Some credentials issued to VACO employees without background investigations VA conducting survey of its facilities to obtain information about completed background investigations	8 8
Protect personal information of applicants from unauthorized disclosure	October 2007	PIV System PII weakness addressed May 2010 Privacy Impact Assessment not approved since FY 2006 Noncompliant shredders at some Enrollment Centers	6 6 7
Install equipment and services necessary to issue credentials	October 2008	Completed June 2010	-
PIV System Security Certification and Accreditation	October 2008	Inadequately certified and accredited for operation and operating under an IATO since January 2008	5
PIV System validation of applicant's identity documents and verification of background investigation.	October 2008	Lack of interface with other government-wide databases prevents electronic validation of applicant identification and background investigations	4

Appendix D Agency Comments

Department of Veterans Affairs

Memorandum

Date: September 28, 2010

From: Assistant Secretary for Operations, Security, and Preparedness (007)

Subj: Updated Draft Report – VA Has Opportunities to Strengthen Program Implementation of Homeland Security Presidential Directive 12 (VAIQ # 7038795)

To: Inspector General (50/52)

1. This memorandum provides amended consolidated comments from the Office of Operations, Security, and Preparedness and the Office of Information and Technology on the Draft Audit Report; *VA Has Opportunities to Strengthen Program Implementation of Homeland Security Presidential Directive 12*, as directed in your memorandum of August 24, 2010, and subsequent discussions with Office of Inspector General auditors. The Audit assessed the Department of Veterans Affairs progress in implementing a reliable and effective system of personal identity verification (PIV) in compliance with Homeland Security Presidential Directive 12 (HSPD-12) to improve the security of its facilities and to protect sensitive information stored in VA networks. Our responses on specific recommendations are attached.

2. Please contact Mr. Thomas Muir, Director, Office of Personnel Security and Identity Management at 202-461-7531, or Mr. Jay Herod, OI&T Program Manager at 732-578-5528, if you require additional information. Thank you for your efforts in identifying areas for improvement in VA's HSPD-12 Program.

(Original signed by Thomas Muir for)

Jose D. Riojas

Attachment

cc: Assistant Secretary for Information & Technology (005)

Attachment

The following comments are provided from the Office of Operations, Security, and Preparedness (OSP) and the Office of Information and Technology (OI&T) in response to the OIG audit, "*VA Has Opportunities to Strengthen Program Implementation of Homeland Security Presidential Directive 12*."

Comments in Response to OIG Report Recommendations

Recommendation 1: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System develops a plan to interface with internal and external systems to electronically verify PIV credential applicant information.

Concur. OSP, in cooperation with an Integrated Project Team (IPT), is currently establishing a comprehensive Integrated Management Plan (IMP) to manage OI&T, the Administrations, Staff Offices, and HSPD-12 Program Office efforts. This IMP is being developed in accordance with industry-standard program management principles.

OI&T has included money in fiscal year 2011 (FY11) and fiscal year 2012 (FY12) for this integration project. At this time however, more detailed requirements are needed to adequately cost and schedule this project beyond a rough order of magnitude (ROM) estimate of $15 million and the scheduled completion date below.

During the Preparedness Initiative Offsite on August 23-27, 2010, there was discussion among stakeholders, the HSPD-12 Program Management Office (PMO), the Security Investigation Center (SIC, responsible for contractor background investigations), and OI&T about integrating SIC contractor background investigation and suitability adjudication status information with the PIV system; the schedule, level of effort, and requirements have not been detailed. However, the project has been initiated and is currently in the planning and initial requirements gathering stage. As more details become available, the Preparedness Initiative HSPD-12 Integrated Master Schedule will be updated.

OSP Comprehensive Plan Target Completion Date: October 31, 2010

Overall OI&T Integration Project Target Completion Date: October 1, 2012

Recommendation 2: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is tested, certified and accredited for operation.

Concur. Please see OI&T comments below. OSP will incorporate the OI&T schedule below into the HSPD-12 Project Management Plan (PMP). There are five phases to the Certification and Accreditation (C&A) process to obtain an Authority to Operate (ATO). According to the Security Management and Reporting Tool (SMART), the PIV System's C&A commenced with Phase One, Communications Outreach, and Phase Two, Document Review, on November 19, 2009. Phase Three, the Security Control

Assessment, began on November 23, 2009, and was completed on December 8, 2009. Phase Four, Assessment Report, commenced on January 1, 2010, and achieved Certification Program Office (CPO) Certification on May, 17, 2010.

The package is currently in Phase Five, Authorization Determination. Within this phase, the ATO package was submitted to the Security Reports and Oversight Management (SROM) Analyst on May 24, 2010. As of July 30, 2010, the Office of Cyber Security issued a Temporary Authority to Operate while the system's ATO package is going through a review by the CIO. The package is currently pending CIO concurrence and final signature.

Target Completion Date: September 30, 2010

Recommendation 3: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is modified to generate standard performance reports to assist the PMO, system administrators, and other users to effectively manage the HSPD-12 Program.

Concur. Currently, OI&T's Office of Enterprise Development (OED) is providing daily ad hoc reports to the HSPD-12 PMO as well as other Executive stakeholders. These reports provide the following information: the number of cards issued (both PIV and non-PIV), the number of cards per site, and the top performing site. A graph is included displaying the production VA-wide for the current week.

In addition, a PIV System reporting capability has been added to the requirements process through the PIV Project Change Control Board process. OSP, along with OI&T, has submitted change requests PIV00000657 (Monthly Program Card Issuance Report), PIV00000651 (Implement Audit Logging and Reporting), PIV00000654 (Long Term Audit Solution), and PIV000000627 (PII Incidence Response Requirements), which are documented in the OI&T Rational Tools Suite Clear Quest PIV change management repository. These change requests are currently Program Management Accountability System (PMAS) deliverables (increments).

In addition to developing system reporting capabilities, the OI&T PIV Team is procuring an Independent Validation and Verification (IV&V) of the PIV System. The IV&V Team's deliverable of various test scripts will serve as a valuable tool for the systems OED PIV integration team to leverage system performance testing and tuning.

Target Completion Date: January 31, 2011

Recommendation 4: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the PIV System is modified to provide effective monitoring of System users for unlawful, unauthorized, or inappropriate activities.

Concur. Several privacy-related corrections identified by the OIG audit team were implemented during the audit period. Additional privacy protections will be incorporated

into future system upgrades. In response to an email request from the HSPD-12 Program Manager, OI&T mitigated the Personal Identifiable Information (PII) risks identified to continuous operation of the PIV System.

PIV System updates were developed and released to address the recent PII concern that approximately 12,000 individuals within the PIV System could view the PII of any other individual in the system.

The PIV System has the following roles: Sponsor, Manager, Registrar, Issuer, PCI Manager, and System Administrator. The former "VIEW VA PIV USER" function allowed all roles to view the PII of any user regardless of their state in the system. By eliminating the "VIEW VA PIV USER" function, roles could only view the PII of users correlated to their role. As an immediate mitigation, OI&T removed the "VIEW VA PIV USER" function and developed an auditing capability until full requirements are received by OSP, the business sponsor.

To address the audit concern, OI&T technical staff developed an auditing capability that logs the selection of any record within the PIV system. The development was completed on April 22, 2010, and implemented in production on April 27, 2010.

Also in April 2010, OI&T changed the capability to search by SSN alone. A user must now search by the combination of SSN and Last Name.

On Friday, May 28, 2010, the new "VIEW VA PIV USER" function was released with specified PII fields eliminated, as documented in business sponsor requirements. The fields eliminated were Social Security Number, Home Address, Home City, Home State, Home Zip Code, Height, Weight, Eye Color, Place of Birth, Race, Gender, Identity Proofing Document Information, and Background Investigation Status Information.

On Friday, May 28, 2010, VA's Office of General Counsel approved a PII notification and acceptance screen that was also implemented based on guidance from VA Directive and Handbook 6500. A user must accept prior to viewing any PII within the PIV system.

OED hosted a two-day offsite meeting on September 15-16, 2010, to continue collaborating with OI&T's Office of Enterprise Operations and Field Development (EOFD), Field Services, and the Office of Information Protection and Risk Management, on how to add additional monitoring and auditing capabilities to the PIV system.

During the offsite meeting, it was concluded that Operations (EOFD) is better suited than Development (OED) for monitoring the system on a daily basis. As part of the transition, a Service Level Agreement (SLA) will be established as well as the necessary tools to accomplish monitoring. The HSPD-12 PMO will establish performance metrics, requirements, and metrics for monitoring and auditing the system on both an automatic and ad hoc basis.

These requirements are change requests PIV00000651 (Implement Audit Logging and Reporting), PIV00000654 (Long Term Audit Solution), and PIV000000627 (PII

Incidence Response Requirements), which are documented in the OI&T Rational Tools Suite Clear Quest PIV change management repository.

Target Completion Date: September 30, 2011

Recommendation 5: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, ensure the required Privacy Impact Assessment for the PIV System is prepared and approved annually.

Concur. According to SMART, the Privacy Impact Assessment (PIA) was submitted for approval to the Privacy Service in November 2009. The PIV Program did not receive a copy notating the PIA as approved, nor is it known why it was not published to the VA PIA website maintained by the Privacy Service. The PIA for the PIV system is currently pending final concurrence and signatures.

Target Completion Date: November 30, 2010

Recommendation 6: We recommend the Assistant Secretary for Operations, Security, and Preparedness, in conjunction with the Assistant Secretary for Information and Technology, define the extent to which PIV credentials will be required to access VA facilities and information systems and develop plans to test and implement the infrastructure necessary to establish these controls.

Concur. In response to the recommendation, there are two separate projects (logical access to computer system and physical access to facilities) under the same HSPD-12 program umbrella. The logical access project is being managed by OI&T and the physical access is being managed by OSP. For this reason both are addressed separately below. Both offices continue to collaborate on the efforts.

OSP and OI&T recognize that logical access is broad and crosses the boundaries of Identity and Access Management, Public Key Infrastructure (PKI) Enablement, Single-Sign-On, and Smart Card Authentication.

Therefore, the scope of logical access within HSPD-12 comprises usage of the PIV smart card credential to gain access to the VA network from a Windows Client Workstation. The use of the PIV credential to gain access to individual applications beyond sign-on is considered out-of-scope for this initiative. To successfully implement logical access, the requirements are for the end user to have a PIV credential, establish a Personal Identification Number (PIN), own a Universal Serial Bus (USB) smart card reader, and have the ActivClient middleware installed on their personal computer or laptop. The user will establish their PIN during the issuance process when obtaining the PIV credential. The target for fulfillment of the requirement for PIV card enablement to achieve Logical Access Control Systems (LACS) Compliance is October 31, 2010. The final dependency is PIV Card deployment to the target VA workforce. In February 2010 an action memo was sent from OI&T Field Operations and Development, Office of Executive Support with the following action required: Deploy PIV ActivClient

(middleware) to all workstations. The instructions to complete the action include installation of USB smart card readers.

Collaboration among members of OSP and OI&T are ongoing to establish an Integrated Master Plan (IMP) which will include the schedule for both physical and logical access. OSP will incorporate the OI&T LACS and Physical Access Control Systems (PACS) schedules into the HSPD-12 PMP. The HSPD-12 Program Office is coordinating with the Administrations and key Staff Offices to define PACS and identify the current status of PACS within VA. OSP and VA stakeholders are moving toward establishing an HSPD-12 compliant enterprise-wide standard.

The Preparedness Initiative's HPSD-12 Program is currently working with OI&T to finalize the IMP, which will detail the response to this recommendation. OSP and OI&T participated in a three-week offsite during August 2010 to begin collaborating on an IMP, which includes logical and physical access.

Target Completion Date: November 30, 2010 (Integrated Master Plan)

Recommendation 7: We recommend the Assistant Secretary for Operations, Security, and Preparedness staff program vacancies in the HSPD-12 Program Management Office.

Concur. The OSP HSPD-12 Program Office is nearly fully staffed. The OSP staffing plan implementation requires an additional 30 days due to adjustments identified during the program management class hosted by VA's Office of Acquisition, Logistics, and Construction. Specifically, an outreach position description is being amended to provide instead a program management expert position and the program office training position is awaiting hiring action through VA's Veteran hire program.

Target Completion Date: November 30, 2010

Recommendation 8: We recommend the Assistant Secretary for Operations, Security, and Preparedness finalize the VA Directive and VA Handbook defining the roles, responsibilities, and processes for implementation and ongoing operations of the HSPD-12 Program.

Concur. VA Directive 0735 has completed the concurrence period and the HSPD-12 Program Office is working to resolve stakeholder comments. The Handbook is in draft stage with stakeholder involvement.

Target Completion Date: Directive: October 31, 2010

Handbook: November 30, 2010

Recommendation 9: We recommend the Assistant Secretary for Operations, Security, and Preparedness develop quantifiable performance measures for the HSPD-12 Program.

Concur. As part of the HSPD-12 Program Office effort to establish a comprehensive PM plan, performance measures will be established for all stakeholders to ensure program deliverables are identified, tracked, and displayed in dashboard format for VA leadership.

Target Completion Date: November 30, 2010

Recommendation 10: We recommend the Assistant Secretary for Operations, Security, and Preparedness implement a formal oversight process to monitor progress in achieving compliance with the requirements of HSPD-12.

Concur. The program management plan currently under development will be used to provide formal oversight to the HSPD-12 Program and all its components. The VA Office of Acquisition, Logistics, and Construction is partnering with OSP to apply industry-standard PM principles to the program and its oversight processes.

Target Completion Date: November 30, 2010

Recommendation 11: We recommend the Assistant Secretary for Operations, Security, and Preparedness establish accountability over program costs and estimated costs of future HSPD-12 operations.

Concur. A plan to implement this recommendation will be developed in cooperation with VA Administrations and Staff Offices. OSP will work with Administrations to identify program funding, obligations, expenditures, and estimations of future costs to provide management oversight of VA's HPSD-12 Program.

Target Completion Date: November 30, 2010

Appendix E OIG Contact and Staff Acknowledgments

OIG Contact	Timothy J. Crowe, Director, 727-395-2425
Acknowledgments	Charles Chiarenza Thomas McPherson Alan Brecese Johnny McCray Debra Cato Dawn Creter Brandon Guadalupe

Appendix F Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG's Web site at **http://www.va.gov/oig/publications/reports-list.asp**. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.