VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Audit of Enrollment Centers' Implementation of Personal Identity Verification Requirements

September 30, 2011
10-04037-295

ACRONYMS AND ABBREVIATIONS

DAA	Designated Accreditation Authority
FBI	Federal Bureau of Investigations
FIPS	Federal Information Processing Standards
HSPD-12	Homeland Security Presidential Directive 12
IDMS	Identity Management System
NIST	National Institute of Standards and Technology
OI&T	Office of Information and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSP	Office of Security and Preparedness
PCI	PIV Credential Issuer
PIV	Personal Identity Verification
SP	Special Publication
TSDB	Terrorist Screening Database
VACO	Veterans Affairs Central Office
VAMC	Veterans Affairs Medical Center
VARO	Veterans Affairs Regional Office

Report Highlights: Audit of Enrollment Centers' Implementation of Personal Identity Verification Requirements

Why We Did This Audit

Compliant Personal Identity Verification (PIV) credentials issued to Federal employees and contractors strengthen the security of access to VA and other Federal facilities and information systems. We assessed the effectiveness of VA's Enrollment Centers to provide PIV credentials that meet Homeland Security Presidential Directive 12 (HSPD-12) and other Government-wide requirements.

What We Found

Missing procedures and significant control lapses in Enrollment Center operations have compromised the integrity of VA's PIV credentialing process. VA may have issued at least 147,000 PIV credentials without determining whether applicants are known or suspected terrorists and presented genuine and unaltered identity source documents. Further, VA may have issued at least 5,100 credentials without verifying applicants' background investigations, and 5,600 credentials where staff circumvented separation of duty control requirements.

Program management did not identify these significant deficiencies because VA has not evaluated and certified that its PIV credentialing operations meet Government-wide requirements. According to this same guidance, major deficiencies in meeting these requirements requires an immediate halt to all credentialing operations until corrective actions are taken and the credentialing process is re-assessed and re-accredited. The costs to remediate these deficiencies are estimated at approximately $6.7 million as of June 2011.

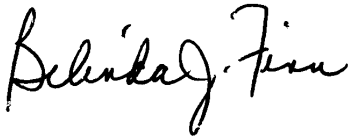
What We Recommend

We recommended the Assistant Secretary for Operations, Security, and Preparedness immediately direct Enrollment Centers to stop issuing PIV credentials until control deficiencies in the credentialing process are addressed, and VA assesses and accredits the adequacy of the existing processes in meeting Government-wide requirements.

Agency Comments

The Assistant Secretary for Operations, Security, and Preparedness concurred in principle with Recommendation 1 and fully concurred with the other recommendations. He advised us the Department has taken immediate actions to mitigate the risks associated with the VA PIV Program.

We consider their initiated and 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.



BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

This audit assessed the effectiveness of VA Enrollment Centers in implementing requirements of Homeland Security Presidential Directive 12 (HSPD-12) to provide Personal Identity Verification (PIV) credentials and to meet other operational requirements of HSPD-12 for identity proofing and PIV credential issuance.

Program Background

HSPD-12 established a mandatory standard for secure and reliable forms of identification issued by the Federal Government for employees and contractors. In response to HSPD-12, the National Institute of Standards and Technology (NIST), U.S. Department of Commerce, developed and published Federal Information Processing Standard (FIPS) 201-1.[1] FIPS 201-1 established the architecture and technical requirements to implement HSPD-12 requirements for a common credential standard.

NIST guidance defines the requirements regarding certification and accreditation. Agencies are required to adopt HSPD-12, implement FIPS 201-1, and use Special Publication (SP) 800-79 to assess and accredit the adequacy and reliability of processes involved in issuing PIV credentials.[2] FIPS 201-1 specified that NIST establish a Government-wide program to accredit official issuers of PIV credentials, which led to SP 800-79. This document established an assessment and accreditation methodology that Federal departments and agencies must use to document that their PIV credentialing process is adhering to HSPD-12 and FIPS 201-1 standards. Federal organizations are required to halt operations and address identified deficiencies when PIV credentialing processes are not accredited to operate, or they fail an accreditation, and to determine whether to revoke issued PIV credentials.

VA's HSPD-12 Program

Designated in March 2009, the Office of Security and Preparedness (OSP) is responsible for program management, communications, policy, training, defining requirements, and oversight for VA Central Office (VACO) and national implementation of the program. VA established approximately 200 Enrollment Centers nationwide to issue credentials. Appendixes A and B provide additional background and scope and methodology information.

[1] Federal Information Processing Standard (FIPS) 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006.
[2] Special Publication (SP) 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, July 2005. NIST updated the publication and issued SP 800-79-1 in June 2008.

RESULTS AND RECOMMENDATIONS

Finding — Enrollment Centers Issued PIV Credentials That Do Not Meet Critical HSPD-12 Requirements

Summary

Significant control lapses in Enrollment Center operations undermine the integrity of all PIV credentials issued to date. The credentials issued by Enrollment Centers to VA's workforce do not meet critical HSPD-12 requirements to verify the suitability and identity of individuals seeking access to VA facilities and information systems. Specifically, Enrollment Centers are issuing PIV credentials without conducting steps required under FIPS 201-1 to determine whether applicants:

- Are known or suspected terrorists
- Have a completed and successfully adjudicated background investigation
- Presented genuine and unaltered identity source documents to establish their identity

Enrollment Center personnel have further compromised the integrity of the PIV process by circumventing separation of duty requirements during the issuance of some credentials. This occurred because program managers did not conduct required program assessments and formally certify Enrollment Center operations to satisfy Government-wide requirements. Additionally, despite identifying significant control lapses in Enrollment Center operations, program managers did not develop oversight procedures to detect and prevent future occurrences.

As a result, 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 authentication. Missing procedures and significant control lapses in Enrollment Center operations have compromised the integrity of VA's PIV credentialing process and all PIV credentials issued to date. As of January 2011, VA may have issued at least 147,000 PIV credentials without verifying these PIV applicants were not known or suspected terrorists and presented authentic identity source documents prior to issuing PIV credentials.

Furthermore, VA may not have verified the completion of a background investigation for at least 5,100 of the 147,000 PIV credentials holders. We estimate the cost to mitigate risks associated with existing PIV credentials at approximately $6.7 million, based on the cost of labor to ensure that

applicants are not on a Government terrorist watch list, have a background investigation, and used authentic source documents.

Applicants Not Checked Against the Terrorist Screening Database

FIPS 201-1 prohibits the issuance of a PIV credential to an applicant who is known or suspected of being a terrorist by the Federal government, including renewing or reissuing a PIV credential to the same holder. The standard also requires PIV credential issuers to collect a full set of fingerprints from all PIV credential applicants who can provide them, and to use the fingerprints for one-to-many matching with the database of fingerprints maintained by the Federal Bureau of Investigations (FBI).

The one-to-many check consists of searching the Security/Suitability Investigations Index, the Defense Clearance and Investigations Index, the FBI Name Check, the FBI National Criminal History database, and the Terrorist Screening Database (TSDB). FIPS 201-1 also requires PIV credential issuers to repeat the entire registration and issuance process, including capturing applicant fingerprints, when PIV credentials need to be reissued due to expired, lost, stolen, damaged, or compromised cards. In addition, Office of Management and Budget (OMB) guidance requires that PIV credential issuers take fingerprints concurrently with the enrollment action to issue new or subsequent PIV credentials.

Staff at the six Enrollment Centers visited did not ensure PIV applicant fingerprints were checked against the TSDB as part of the enrollment process for all 120 statistically selected PIV records before issuing the PIV credentials. Enrollment Centers issued three PIV credentials to applicants who were not screened against the TSDB because background investigations and fingerprints checks were not performed for these PIV credential holders.

Enrollment Centers also issued 39 PIV credentials to applicants who were not screened against the TSDB because these PIV credential holders' background investigations and fingerprints pre-dated the December 2003 establishment of the TSDB. In addition, 78 credential holders who had background investigations conducted and fingerprints taken after December 2003 were not fingerprinted and checked against the TSDB concurrent with the enrollment process as required, and averaged 2 years between the fingerprint check and receipt of the PIV credential.

This occurred because HSPD-12 Program Management and Enrollment Center personnel were unaware of the FIPS 201-1 requirement to verify an applicant is not a suspected terrorist concurrent with the enrollment process and prior to issuing a PIV credential. Furthermore, VA guidance issued in 2008 and updated as recently as February 2011 does not address this requirement and lacks critical information to ensure Registrars are aware of the specific steps to ensure an applicant is not a known or suspected terrorist.

Because the FBI updates the TSDB as information becomes available, fingerprint checks not conducted concurrently with the enrollment process may be based on outdated and possibly inaccurate information. Based on the results of our sample, we project that, as of January 2011, VA issued PIV credentials to at least 147,000 applicants without a concurrent TSDB screening, of which approximately 69,000 may never have been screened.

Status of Background Investigation Not Consistently Verified

FIPS 201-1 requires a completed and successfully adjudicated background investigation prior to issuing a PIV credential. However, FIPS 201-1 allows agencies to issue PIV credentials based on an initiated background investigation, but only after successful completion of a concurrent FBI fingerprint check.

Enrollment Centers visited did not verify the existence and results of a background investigation for each applicant prior to issuing a PIV credential for 25 (21 percent) of 120 statistically selected PIV records. Errors were identified at two of the six Enrollment Centers visited. For example, one Enrollment Center issued credentials to 16 applicants based on unsupported background investigation dates entered into the PIV System.

Of the 16, 2 PIV credential holders did not have any record of a background investigation initiated or completed. The remaining 14 applicants had completed background investigations, but the dates and information contained in the PIV System were inaccurate. In response to our concerns about inaccurate information, management at the Enrollment Center reviewed the personnel records of all 231 employees and identified an additional 38 PIV credential holders who did not have a background investigation either initiated or completed, including the Enrollment Center supervisor.

VA's PIV System requires Registrars to enter the initiation and completion dates of an applicant's background investigation to complete the registration process and issue a PIV credential. The Registrar and Enrollment Center supervisor could not provide a plausible explanation as to why the Registrar entered inaccurate background investigation information into the PIV System. In addition, program management and Enrollment Center staff stated that issuing all PIV credentials by the October 1, 2011, deadline was considered the highest priority. These factors appear to be the reason Enrollment Center staff entered inaccurate data into the PIV system to override the control that requires data fields to have information in order to issue credentials.

A second Enrollment Center issued PIV credentials to nine applicants based on inaccurate background investigation dates. All nine errors occurred because the Registrar entered incorrect data from spreadsheets provided by

the local Human Resources office. Of the nine, one PIV credential holder did not have an initiated or completed background investigation, and therefore, was not eligible to receive a PIV credential.

Significant lapses in controls designed to ensure that applicants have initiated or completed background investigations prior to PIV credential issuance occurred due to the lack of specific implementation guidance to Enrollment Centers and limitations in automated tools that support the credentialing process. Specific control problems identified included the following:

- VA guidance did not require Enrollment Centers to validate that PIV credential applicants had a successfully completed background investigation prior to issuing a PIV credential. In response to our concerns, on January 31, 2011, VA issued revised guidance that requires direct verification of background investigation information using the Office of Personnel Management's Personnel Investigations Processing System and the applicant's Electronic Official Personnel File.

- VA did not establish adequate controls to verify the accuracy of background investigation information in the PIV System. The Office of Inspector General (OIG) reported a similar situation at VACO that occurred almost 2 years ago.[3] Specifically, the VACO Enrollment Center, a pilot site for testing the credentialing process, issued PIV credentials to 1,278 VACO employees without verifying the existence and results of the employees' background investigations. Approximately 895 (70 percent) of the 1,278 VACO employees who received a PIV credential, including 7 SES-level employees, did not have an initiated or completed background investigation. We were advised that Enrollment Center personnel entered fictitious background investigation dates into the PIV System to facilitate the issuance of PIV credentials. Despite this report, program officials in VACO did not assess if the same vulnerability may exist at other Enrollment Centers. Thus, VA officials took no action to address and mitigate the problem nationwide.

- The PIV System does not automatically verify background investigation information. In March 2011, during the course of our audit, the PIV System Project Manager stated the Office of Information and Technology (OI&T) was developing an update to the PIV System that would allow automatic collection of initiated and completed dates of an applicant's background investigation. However, the PIV System Project Manager also stated the update would not include the PIV System automatically

[3] *VA Has Opportunities to Strengthen Program Implementation of Homeland Security Presidential Directive 12* (VA OIG Report No. 10-01575-262, September 30, 2010).

collecting background investigation results to ensure that Enrollment Centers issue PIV credentials only to suitable applicants.

Based on our results, VA potentially issued approximately 5,100 PIV credentials to applicants without verifying background investigation results and information, as of January 2011.

Identity Documents Not Authenticated

FIPS 201-1 requires the PIV Registrar to visually inspect applicant identification documents and authenticate that the documents are genuine and unaltered. Identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, *Employment Eligibility Verification*, and at least one document must be a valid State or Federal Government-issued picture identification such as a driver's license or U.S. passport. The Registrar should electronically verify the authenticity of the source document, when the issuer of the source document offers such services. When electronic verification is not available, the Registrar should use other available tools to authenticate the source and integrity of the identity source documents.

Enrollment Centers are not verifying the authenticity of identity source documents to prevent or detect the use of fraudulent documents prior to issuing PIV credentials. The Registrars at six Enrollment Centers accepted identity source documents as valid based on a visual inspection without performing additional steps to ensure the documents are valid.

These control weaknesses exist because VA guidance issued in 2008 and updated as recently as February 2011 lacks critical information to ensure Registrars understand how and where to authenticate the source and integrity of an applicant's identity source documents. Without proper guidance, Enrollment Centers are at risk of issuing PIV credentials to individuals based on fraudulent identity source documents.

Separation of Duties Requirements Circumvented

FIPS 201-1 states, "The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person." The standard specifically establishes that Sponsor, Registrar, and Issuer roles are mutually exclusive. This requirement is in place to ensure the identity of a PIV credential applicant and the integrity of PIV credentials.

At two of six Enrollment Centers visited, VA staff circumvented mandatory separation of duties by allowing a single person to complete multiple and mutually exclusive roles during the PIV credentialing process. At one Enrollment Center, staff exploited weak system controls to fulfill Registrar and Issuer roles in the PIV System for the same applicant. Enrollment

Center staff stated they routinely used this method for processing PIV applicants and issuing credentials because it saved time in the PIV credential issuance process. This occurred because the PIV System does not automatically enforce separation of duties for individual applicants. Our review of Enrollment Center staff user assignments in the PIV System revealed that staff are assigned multiple roles (that is, Sponsor, Registrar, and Issuer) in 175 (88 percent) of the approximately 200 Enrollment Centers.

In addition, staff shared PIV credentials and PIV System passwords at two Enrollment Centers, enabling one individual to improperly perform multiple roles in the PIV credentialing process. For 120 statistically selected PIV records, we identified 9 (8 percent) instances where staff at the two Enrollment Centers shared their PIV credentials and PIV System passwords that enabled an individual to perform multiple roles in the PIV credentialing process. As a result, Enrollment Center staff potentially circumvented separation of duty controls to issue approximately 5,600 PIV credentials, as of January 2011.

While VA guidance requires adherence to the principle of separation of duties during the credentialing process, Enrollment Center staff were able to successfully circumvent these requirements in the PIV credentialing process because:

- The PIV System lacks system controls to prevent Enrollment Center staff from acting as both Registrar and Issuer for individual PIV applicants.
- Enrollment Center management did not implement a mechanism to detect and prevent the sharing of credentials and PIV System passwords during the PIV credentialing process.

In 2009, HSPD-12 Program Management identified that staff at an unrelated Enrollment Center shared PIV credentials and PIV System passwords; however, Program Management failed to develop oversight procedures designed to detect and prevent Enrollment Centers from circumventing the FIPS 201-1 separation of duties requirements. In addition, VA advised that it identified 1 individual at another Enrollment Center who performed the Sponsor, Registrar, and Issuer roles to issue approximately 1,400 PIV credentials.

Operating Under Uncertified and Unaccredited Program

NIST requires PIV Credential Issuers (PCIs) to formally assess and make a determination as to whether their program's policies, procedures, and processes comply with HSPD-12 and FIPS 201-1 prior to issuing PIV credentials.[4] In June 2008, NIST issued SP 800-79-1 to provide a more

[4] NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

technically based approach to assure that PCIs reliably fulfill the requirements of FIPS 201-1. Under this guidance, PCIs who completed the assessment and certification of their PIV credentialing process under SP 800-79 were required to re-accredit their PIV credentialing process by June 2009. The outcome of the assessment and certification processes is a determination of whether the program has the Authority to Operate, Interim Authority to Operate, or a Denial of Authority to Operate.

After receiving an Authority to Operate, PCIs must re-accredit their process within 3 years, or when a significant change in structure, personnel, or operating procedures occurs. When assessment procedures disclose a noncompliance with HSPD-12 and FIPS 201-1, a PCI that has already started issuing cards must immediately halt operations, take action to address the deficiencies, and determine whether to revoke PIV credentials issued using a noncompliant process.

In addition, departments and agencies are required to establish formal monitoring procedures to provide continued oversight and inform the appropriate officials of changes that may adversely affect continued compliance with FIPS 201-1. Monitoring consists of operations plan maintenance and an annual life-cycle walkthrough. An operations plan is the primary description of what and how PIV credential issuing services are provided. Departments and agencies are required to keep the operations plan updated as changes occur in their PIV credentialing operations. The annual life-cycle walkthrough entails reviewing all the services and functions of a PCI and its facilities for continued reliability, and it must cover a PIV credential's life cycle from sponsorship to maintenance.

While VA completed the assessment and certification process and issued an Authority to Operate in September 2007, VA did not take required steps to formally assess whether its HSPD-12 Program's policies, procedures, and processes complied with HSPD-12 and FIPS 201-1 by June 2009, as required. Furthermore, after completing the deployment of approximately 200 Enrollment Centers in June 2010, VA did not perform the required re-accreditation of the program.

In addition, the HSPD-12 Program Manager did not establish required monitoring procedures to ensure the continued reliability of the PIV credentialing operations. Program management also did not conduct required annual assessments of Enrollment Center operations to ensure that the credentialing operations continue to meet HSPD-12 and FIPS 201-1 requirements.

If VA had performed the required evaluations and certification of its HSPD-12 Program and Enrollment Center operations, and put required

monitoring processes into place, HSPD-12 Program Management should have identified missing procedures and control lapses in Enrollment Center operations undermining the PIV credentialing process. Major deficiencies in PIV credentialing operations require an immediate halt to all Enrollment Center operations, taking corrective action, and re-assessing and re-accrediting the HSPD-12 Program in accordance with NIST SP 800-79-1. Additionally, VA must evaluate the suitability of all PIV credential holders to date and revoke credentials as necessary.

Conclusion

Because of missing procedures and significant control lapses in Enrollment Center operations, VA has compromised the integrity of all PIV credentials issued to date. Until VA corrects the identified deficiencies and formally accredits the HSPD-12 Program, the Department's PIV credentials cannot meet security requirements necessary for acceptance Government-wide. The costs to remediate these deficiencies are estimated at approximately $6.7 million, which will continue to increase with every additional credential issued through VA's existing PIV credentialing process.

Since Enrollment Centers continue to issue more than 17,500 deficient credentials monthly, we expect the cost of remediating these deficiencies to increase with the issuance of additional credentials. Accordingly, VA should immediately direct Enrollment Centers to stop issuing PIV credentials, while the Department assesses and accredits the adequacy of the existing processes in meeting FIPS 201-1 requirements.

Recommendations

1. We recommended the Assistant Secretary for Operations, Security, and Preparedness direct VA Enrollment Centers to stop issuing Personal Identity Verification credentials until the Department assesses and accredits the adequacy of the existing processes in meeting Federal Information Processing Standards 201-1 requirements.

2. We recommended the Assistant Secretary for Operations, Security, and Preparedness direct VA Enrollment Centers to evaluate information supporting the eligibility of Personal Identity Verification credential holders and take action to deactivate Personal Identity Verification credentials of individuals who did not satisfy processing requirements.

3. We recommended the Assistant Secretary for Operations, Security, and Preparedness implement Enrollment Center monitoring procedures, such as implementing operations plan maintenance and annual life-cycle walkthrough procedures in accordance with National Institute of Standards and Technology Special Publication 800-79-1.

4. We recommended the Assistant Secretary for Operations, Security, and Preparedness develop and issue guidance to ensure Registrars screen all

Personal Identity Verification credential applicants against the Terrorist Screening Database prior to issuing Personal Identity Verification credentials.

5. We recommended the Assistant Secretary for Operations, Security, and Preparedness issue procedures to ensure Registrars verify the existence and results of a background investigation for each applicant prior to issuing a Personal Identity Verification credential.

6. We recommended the Assistant Secretary for Operations, Security, and Preparedness issue guidance to ensure Registrars authenticate the source and integrity of identity documents used during the Personal Identity Verification credential enrollment process through official Federal and State databases.

7. We recommended the Assistant Secretary for Operations, Security, and Preparedness make appropriate changes to the Personal Identity Verification System to prevent Enrollment Center staff from performing more than one role in the Personal Identity Verification credential issuance process.

Management Comments and OIG Response

The Assistant Secretary for Operations, Security, and Preparedness concurred in principle with Recommendation 1 and fully concurred with the other recommendations. He advised us the Department has taken immediate actions to mitigate the risks associated with the VA PIV Program. OSP plans to take the following actions:

- Forwarded a list of all VA employees, contractors, and affiliates with PIV credentials to the Office of Personnel Management for a detailed by-name review against electronic records of background investigations to identify individuals who do not satisfy processing requirements.
- Scheduled all PIV Card Issuance facilities for assessment and accreditation in accordance with NIST 800-79-1 and FIPS 201-1 requirements.
- Directed personnel performing PIV duties to undergo retraining and recertification on PIV roles and responsibilities by December 2011.

OSP is also drafting policy guidance to require:

- Enrollment Centers to evaluate information supporting the eligibility of PIV credential holders and take action to deactivate PIV credentials of individuals who did not satisfy processing requirements.

- All VA organizations to a conduct a new Special Agency Check for each PIV enrollment action and for each employee who has not been subject to a Special Agency Check since implementation of HSPD-6 in 2003.
- All applicants to have at least a favorably adjudicated Special Agency Check and background investigation scheduled at the Office of Personnel Management prior to issuing PIV credential.
- Authentication of the source and integrity of identity documents used during the PIV credential enrollment process through official Federal and State databases.

As to maintaining the intergrity of individual roles and responsibilities in the Enrollment Centers, the Assistant Secretary advised that he will direct PIV System managers to investigate and report on options available to prevent Enrollment Center staff from performing more than one role for an individual applicant in the credential issuance process. The final completion date for corrective actions is expected to occur on or before March 31, 2012.

The Assistant Secretary provided responsive implementation plans to address our recommendations. We will monitor the Department's progress and follow up on its implementation until all proposed actions are completed. Appendix D provides the full text of the Assistant Secretary's comments.

Appendix A Background

National Strategy for Homeland Security

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: reduce America's vulnerability to terrorism, minimize the damage, and assist in the recovery from attacks that may occur. The President also issued 25 Homeland Security Presidential Directives through January 2009, providing additional guidance related to the mission areas outlined in the National Strategy.

Homeland Security Presidential Directive 12

HSPD-12, issued in August 2004, established a policy for creation, issuance, and use of personal identification credentials in the Federal Government. The Directive requires the development and use of a standard for a secure and reliable form of identification for Federal employees and contractors. Secure and reliable forms of identification are:

- Issued based on sound criteria for verifying an individual employee's identity
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Rapidly authenticated electronically
- Issued only by providers whose reliability has been established by an official accreditation process.

HSPD-12 required the Department of Commerce to promulgate a common standard for identification credentials, issued by Federal departments and agencies for gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

FIPS 201

In response to HSPD-12, NIST developed and published FIPS 201-1, *Personal Identity Verification of Federal Employees and Contractors,* which established the architecture and technical requirements for a common identification standard for Federal employees and contractors. FIPS 201-1 is composed of two parts, PIV-I and PIV-II. PIV-I describes the minimum requirements for a Federal Personal Identification System that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-II provides detailed technical specifications to support the control and security objectives in PIV-I, as well as interoperability of PIV credentials and systems among Federal departments and agencies.

FIPS 201-1 requires each agency's PIV implementation meet HSPD-12 control objectives such that:

- Credentials are issued to individuals whose true identity has been verified and after a proper authority has authorized issuance of the credential.
- Only an individual with a background investigation on record is issued a credential.
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State Government-issued picture ID.
- Fraudulent identity source documents are not accepted as genuine and unaltered.
- A person suspected or known to the Government as being a terrorist is not issued a credential.
- No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- No credential is issued unless requested by proper authority.
- A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
- A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential.
- An issued credential is not modified, duplicated, or forged.

Agencies using a system-based approach that incorporates an automated Identity Management System (IDMS) are required to follow the identity proofing and registration process defined in FIPS 201-1, Appendix A, Section 2. An IDMS is an information system that performs identity proofing, verification, and validation to establish identity claim validity.

Using Government-wide services, IDMS uses fingerprint information to perform a one-to-many search to validate the identity of the applicant, the authenticity of identification documents, and to confirm existence of suitability checks. Additionally, an IDMS supports verifying that no substitutions occur by facilitating a one-to-one fingerprint check of the applicant against the PIV enrollment record. Agencies that do not have an existing PIV System that incorporates IDMS functionality, such as VA, are required to use the role-based approach for identity proofing and registration as defined in FIPS 201-1, Appendix A, Section 1.

FIPS 201-1 defines the critical roles with the PIV identity proofing, registration, and issuance process:

- The **Sponsor** substantiates the need for a PIV credential, requests the issuance of a PIV credential, and submits the request to the Registrar.
- The **Registrar** is responsible for identity proofing of an applicant and ensuring the successful completion of the background checks, and provides the final approval for the issuance of a PIV credential.
- The **Issuer** performs credential personalization operations and issues the identity credential to the applicant after completing all identity proofing, background checks, and related approvals.

FIPS 201-1 requires that the roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive such that no individual shall hold more than one of these roles in the identity proofing and registration process for a single applicant.

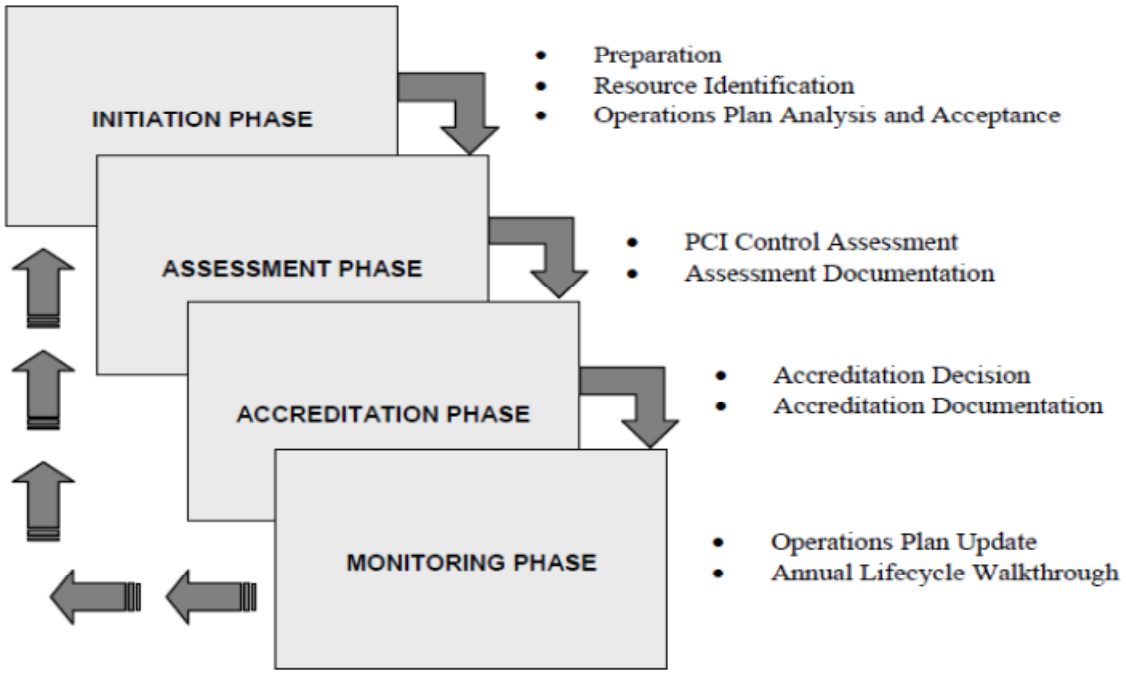
NIST SP 800-79

FIPS 201-1 specified that NIST "…establish a Government-wide program to accredit official issuers of PIV Cards…," of which led to the issuance of NIST SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, in July 2005. NIST updated the publication and issued SP 800-79-1 in June 2008. SP 800-79-1 establishes an assessment and accreditation methodology providers must use to document that their PIV credentialing process is reliably adhering to HSPD-12 and FIPS 201-1 standards and implementation directives.

Figure 1 depicts the assessment and accreditation process to assess and determine whether a PCI's policies, procedures, and processes comply with HSPD-12, FIPS 201-1, and their own policies, regulations, and standards prior to issuing PIV credentials.

Figure 1

Assessment and Accreditation Methodology

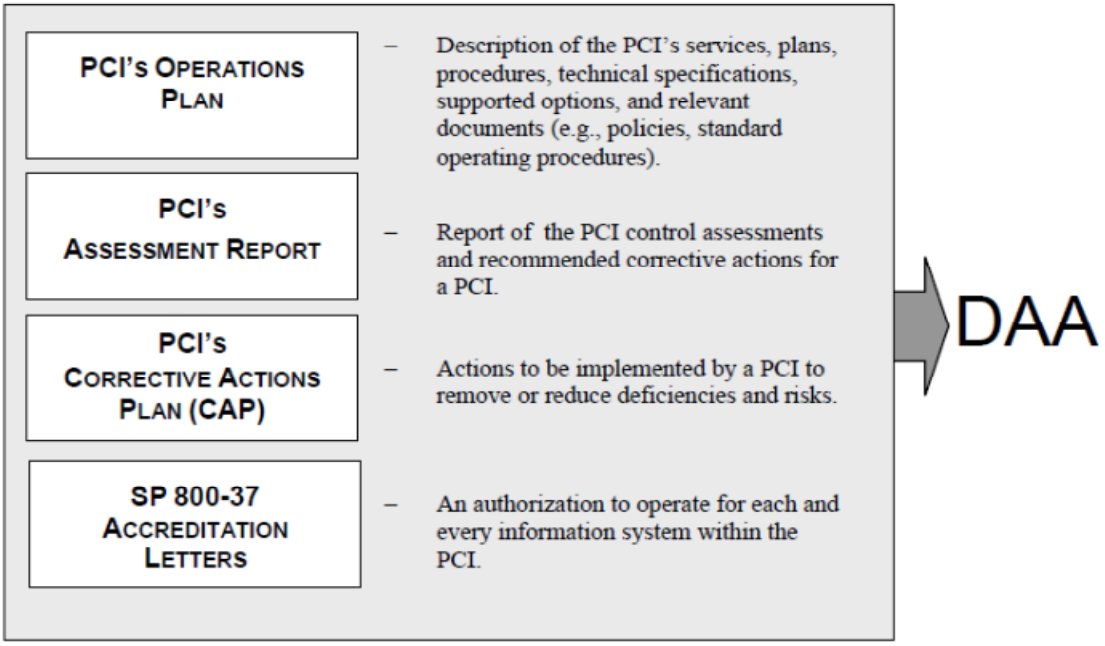


Source: NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008

An Assessment Team that is not involved in the development, day-to-day maintenance, and operations of the program, or in the removal, correction, or remediation of deficiencies, gathers evidence on how well the HSPD-12 Program satisfies the requirements of FIPS 201-1. The result of the assessment is a report that serves as the basis for an appropriate accreditation decision as well as developing corrective actions for removing or mitigating discovered deficiencies. The department or agency must appoint a Designated Accreditation Authority (DAA) who is independent of the Assessment Team and has the authority to review assessments of the HSPD-12 Program. The DAA relies on an Accreditation Submission Package similar to that depicted in Figure 2, to determine whether accreditation of the program is appropriate.

Figure 2

Accreditation Submission Package



Source: NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008

Based on the importance of reliably creating and issuing PIV credentials, SP 800-79-1 requires the accrediting agency to monitor the PCI to ensure that policies, procedures, and processes remain in effect as originally intended. Changes in a PCI's policies, management, operations personnel, and available technology must be monitored so that the organization minimizes exposing itself to security and privacy threats existing or arising in the PCI. For example, if there is a significant staff turnover in the PCI, the organization must be sure that the new PCI staff is enrolling applicants and issuing credentials using the same reliable processes that were previously approved.

Under SP 800-79-1, monitoring consists of operations plan maintenance and an annual life-cycle walkthrough. The latter entails reviewing all services and functions of a PCI and its facilities for continued reliability. The annual walkthrough must cover a PIV credential's life cycle from sponsorship to maintenance. Observation of the full life cycle of a credential ensures that all processes are still reliably operating as assessed during the accreditation.

VA's HSPD-12 Program

Designated in March 2009, OSP is the overall VA Business Sponsor providing 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. VA established a

Program Management Office in October 2009, led by the HSPD-12 Program Manager. OI&T is the Information Technology Program Management Office responsible for analysis, design, implementation, operations, and maintenance of the PIV System. OI&T is also responsible for help desk functions, field site deployment, full software development life cycle, and hardware/software procurement related to the HSPD-12 Program.

VA established and equipped approximately 200 Enrollment Centers at VA Medical Centers (VAMCs), VA Regional Offices (VAROs), and other locations, such as the VA Health Eligibility Center in Atlanta, GA. Enrollment Centers are responsible for processing and issuing PIV credentials to VA employees, contractors, and others at their assigned locations and geographic areas. Enrollment Center staff are trained to perform the PCI Manager, Registrar, and Issuer roles and use PIV System workstations. According to VA, the PIV System automates the enrollment and issuance processes for the PIV credential, manages the identities of PIV credential holders, manages the life cycle of the PIV credential, provides data management and provisioning services for interfacing systems, and provides audit and reporting data on PIV System transactions and events. Enrollment Centers issued approximately 147,000 PIV credentials to VA's workforce through January 28, 2011. Enrollment Centers issued approximately 81,000 during the course of our audit (through June 2011) or 228,000 in total.

Appendix B Scope and Methodology

Scope

Our audit focused on VA's Enrollment Center procedures for processing credential applicants and issuing PIV credentials from September 2007 through February 2011. We conducted our fieldwork from October 2010 through June 2011 at VA Central Offices, and Enrollment Centers located in the Oklahoma City, OK, VAMC; St. Louis, MO, VARO; Atlanta, GA, Health Eligibility Center; New York, NY, VARO; Kansas City, MO, VAMC; and Augusta, GA, VAMC.

Methodology

To assess the Department's progress in implementing the requirements of HSPD-12, we reviewed laws, regulations, and policies applicable to VA's HSPD-12 Program. We interviewed the HSPD-12 Program Manager, senior Veterans Health Administration and Veterans Benefits Administration officials, the PIV System Project Manager, and the Deputy Assistant Secretary for Emergency Management. We also interviewed the Acting Director of Personnel Security and Suitability Services, personnel from VA Human Resources and VACO Security and Suitability Services, and directors and Enrollment Center staff.

We reviewed the guidance provided to Enrollment Centers by VA and the Administrations. We observed and evaluated processes used by Registrars and Issuers as part of the PIV credentialing process, such as applicant identity proofing, validation of background investigation, and applicant fingerprinting at each of the six Enrollment Centers visited.

We tested a statistical sample of 120 PIV System records to determine whether Enrollment Centers were taking the necessary steps to:

- Ensure that applicants were screened against the TSDB
- Verify the existence of a background investigation supporting suitability to work for the Government
- Authenticate the source and integrity of identity documents with Federal and State-managed databases
- Ensure adherence to separation of duty during the credentialing process.

To estimate the $6.7 million cost to mitigate risks associated with existing PIV credentials, we applied an estimated average labor rate of $29.30 to the total estimated time to reevaluate the status of the approximately

228,000 PIV credentials issued as of June 19, 2011. Our average labor rate and time to reevaluate credential holders are based on:

- Average labor rate – Total salary and wages divided by total labor hours worked in VA's Personnel and Accounting Integrated Data System
- Time to reevaluate – Estimate of 1 hour per credential based on 30 minutes each for the Enrollment Center Registrar and PIV credential holder to complete the reevaluation processes

Reliability of Computer-Processed Data

We 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 traced a statistically selected sample of transactions to supporting source documentation. We determined the computer-generated data were sufficiently reliable to meet the audit objective and support our recommendations.

Compliance With Government Audit Standards

Our assessment of internal controls focused on those controls relating to our audit objective. 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 Statistical Sampling Methodology

To achieve our objective of determining whether Enrollment Centers are issuing PIV credentials to VA's workforce that meet critical HSPD-12 requirements, we selected a sample of PIV credential recipients from the PIV System.

Population

The population consisted of 147,247 records in the PIV System of applicants who received PIV credentials from September 7, 2007, through January 28, 2011.

Sampling Design

We used a two-stage cluster sample. In the first stage of the sample, we selected six Enrollment Centers using simple random sampling without replacement. We used this methodology to ensure each Enrollment Center had an equal probability of selection as each sampling unit was drawn. In the second stage of the sample, we sampled 20 PIV credential holders within each Enrollment Center selected in the first stage using simple random sampling without replacement.

Weights

We calculated sampling weights as a product of the probability of selection at each stage of sampling. The weights were post-stratified in the analysis to ensure that sample totals equaled the known population of 147,247 PIV credential holders.

Projections and Margins of Error

The margin of error and confidence interval are indicators of the precision of the estimate. Repeated statistical sampling of this universe would result in an estimate approximately between the lower and upper limits in 90 percent of the samples.

Table 1

Credentials Issued With Concurrent TSDB Screening
Projections and Margins of Error

Finding	Projection	Margin of Error	Lower 90%	Upper 90%	Sample
Number					
Screened	0	7,701	0	7,701	0
Not Screened	147,247	7,701	139,546	147,274	120
Total	**147,247**	**N/A**	**N/A**	**N/A**	**120**
Percent					
Screened	0%	5.2%	0%	5.2%	0
Not Screened	100%	5.2%	94.8%	100%	120
Total	**100%**	**N/A**	**N/A**	**N/A**	**120**

Source: VA OIG

Table 2

Credential Applicants Screened Against TSDB Projections and Margins of Error

Finding	Projection	Margin of Error	Lower 90%	Upper 90%	Sample
Number					
Never Screened	68,740	19,537	49,203	88,277	42
Not Concurrent	78,207	19,537	58,970	98,044	78
Total	**147,247**	**N/A**	**N/A**	**N/A**	**120**
Percent					
Never Screened	46.7%	13.3%	33.4%	60.0%	42
Not Concurrent	53.3%	13.3%	40.1%	66.6%	78
Total	**100%**	**N/A**	**N/A**	**N/A**	**120**

Source: VA OIG

Table 3

Credentials Issued With Verified Background Investigations (BI) Projections and Margins of Error

Finding	Projection	Margin of Error	Lower 90%	Upper 90%	Sample
Number					
BI Verified	142,139	1,220	140,918	143,359	95
BI Not Verified	5,108	1,220	3,888	6,629	25
Total	**147,247**	**N/A**	**N/A**	**N/A**	**120**
Percent					
BI Verified	96.5%	0.8%	95.7%	97.4%	95
BI Not Verified	3.5%	0.8%	2.6%	4.3%	25
Total	**100%**	**N/A**	**N/A**	**N/A**	**120**

Source: VA OIG

Table 4

Credentials Issued With Required Separation of Duties (SOD) Projections and Margins of Error

Finding	Projection	Margin of Error	Lower 90%	Upper 90%	Sample
Number					
With SOD	141,639	7,695	133,944	149,334	111
Without SOD	5,608	7,695	9	13,303	9
Total	**147,247**	**N/A**	**N/A**	**N/A**	**120**
Percent					
With SOD	96.2%	5.2%	91.0%	100%	111
Without SOD	3.8%	5.2%	0.01%	9.0%	9
Total	**100%**	**N/A**	**N/A**	**N/A**	**120**

Source: VA OIG

Appendix D Assistant Secretary for Operations, Security, and Preparedness Comments

Department of Veterans Affairs

Memorandum

Date: September 19, 2011

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

Subj: Response to Draft Report – Audit of Enrollment Centers' Implementation of Personal Identity Verification Requirements

To: Inspector General (50/52)

1. This memorandum provides ***revised*** comments from the Office of Operations, Security, and Preparedness on the Draft Audit Report: *Audit of Enrollment Centers' Implementation of Personal Identity Verification Requirements*, as directed. The audit assessed the Department of Veterans Affairs progress in field implementation of 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. My POC for this matter is Mr. Thomas Muir, Director, Personnel Security and Identity Management at 202-461-7531. Thank you for your efforts to ensure the safety and security of our Nation's Veterans, our dedicated VA workforce, our workplaces, and for identifying areas for improvement in VA's HSPD-12 Program.

(original signed by:)

Jose D. Riojas

Attachment

Attachment

Audit of Enrollment Centers' Implementation of Personal Identity Verification

Recommendation 1:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness direct VA Enrollment Centers to stop issuing Personal Identity Verification credentials until the Department assesses and accredits the adequacy of the existing processes in meeting Federal Information Processing Standards 201-1 requirements.**
VA Response:	Concur in principle. The Department of Veterans Affairs is taking immediate actions to mitigate risk associated with the VA Personal Identity Verification (PIV) card program. VA has scheduled all PIV Card Issuance (PCI) facilities for assessment and accreditation in accordance with NIST 800-79-1 and FIPS 201-1 requirements. Additionally, in order to ensure the integrity of the VA PIV card issuance program, VA has forwarded to the Office of Personnel Management (OPM) a listing of all VA employees, contractors, and affiliates with a PIV card and requested a detailed by-name review against electronic records of background investigations. Finally, VA has required that personnel performing PIV duties retrain and recertify their training on PIV roles and responsibilities by December 2011. These immediate actions, briefed to the Office of Management and Budget (OMB) and coordinated with NIST, enable VA to mitigate the immediate risks to the integrity of VA the PIV card system while ensuring long-term compliance with FIPS 201-1.
Supporting Documentation:	
Status:	Target Dates: Assessment & Accreditation: March 31, 2012 Name by name PSS review: October 15, 2011 Role-based Training: December 2, 2011

Recommendation 2:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness direct VA Enrollment Centers to evaluate information supporting the eligibility of Personal Identity Verification credential holders and take action to deactivate Personal Identity Verification credentials of individuals who did not satisfy processing requirements.**
VA Response:	Concur. The Assistant Secretary for Operations, Security, and Preparedness will issue policy guidance requiring all VA PIV Enrollment Stations to evaluate information supporting the eligibility of Personal Identity Verification credential holders and take action to deactivate Personal Identity Verification credentials of individuals who did not satisfy processing requirements. OI&T has generated a listing of all individuals with PIV badges, which OSP will verify against OPM's security investigations index file to identify individuals who do not satisfy processing requirements. Once the list is received, VA organizations will review this information and take appropriate action for employees, contractors, and affiliates (which may include a check of hard copy employee Official Personnel Files).
Supporting Documentation:	OSP Draft Memo 11-002 and 11-004
Status:	Pending Assistant Secretary for OSP and General Counsel review. Target Dates: Policy Issuance: October 15, 2011 Name by name review - Electronic: October 15, 2011 Name by name review - OPFs: Plan from Administrations and Staff Offices: December 31, 2011
Recommendation 3:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness implement Enrollment Center monitoring procedures, such as implementing operations plan maintenance and annual life-cycle walkthrough procedures in accordance with National Institute of Standards and Technology Special Publication 800-79-1.**

VA Response:	Concur. The Assistant Secretary for OSP has established an Assessment and Accreditation (A&A) program for accrediting the reliability of all VA PIV Enrollment Stations by March 31, 2012. In accordance with NIST SP 800-79-1, all PIV Enrollment Stations will be assessed and VA's Designated Accreditation Authority will issue, as appropriate, certificates of authority to operate (re-accreditation within 3 years), interim authority to operation (3 months), or denial of authority to operate (halt of all PCI operations). Follow-up program assessments and oversight for existing and proposed PIV Enrollment Stations will be conducted in accordance with SP 800-79-1.
Supporting Documentation:	Pending Assistant Secretary for OSP and General Counsel review. OSP Draft Memo 11-001
Status:	The OI&T Office of Information Security is current conducting Assessment and Accreditation surveys of all 284 PIV Enrollment units. Target Dates: Policy Issuance: October 15, 2011 Assessments & Accreditations: March 31, 2012
Recommendation 4:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness develop and issue guidance to ensure Registrars screen all Personal Identity Verification credential applicants against the Terrorist Screening Database prior to issuing Personal Identity Verification credentials.**
VA Response:	Concur. OIG stated that this requirement exists in FIPS 201-1, Section 2.1 and 2.2. Review of this document showed requirement that: [HSPD-12] establish control objectives for secure and reliable identification of Federal employees and contractors. These control objectives, provided in paragraph 3 of the directive, state: (3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose

	reliability has been established by an official accreditation process. [Including] a person suspected or known to the government as being a terrorist is not issued a credential; The Assistant Secretary for OSP will issue policy guidance requiring all VA organizations to a conduct a new Special Agreement Check (SAC) for each PIV enrollment action (new issuance or renewal) and for each employee who has not been subject to a SAC since implementation of HSPD-6 (2003) to screen applicants against the Terrorist Screening Database prior to issuing Personal Identity Verification credentials.
Supporting Documentation:	OSP Draft Memo 11-004
Status:	Policy memorandum pending Assistant Secretary for OSP and General Counsel review. Target Dates: Policy Issuance: October 15, 2011 SAC Screening Plan: Develop Plan by November 30, 2011 SAC Screening Completed: To Be Determined
Recommendation 5:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness issue procedures to ensure Registrars verify the existence and results of a background investigation for each applicant prior to issuing a Personal Identity Verification credential.**
VA Response:	Concur. The Assistant Secretary for OSP will issue policy guidance that requires all Registrars ensure applicants have at least a favorably adjudicated SAC and background investigation scheduled at OPM prior to issuing Personal Identity Verification credential; or a favorably adjudicated National Agency Check with Written Inquiries (NACI) prior to issuing a 3-year Personal Identity Verification credential for each applicant.
Supporting Documentation:	OSP Draft Memo 11-004

Status:	Pending Assistant Secretary for OSP and General Counsel review. Target Dates: Policy Issuance: October 15, 2011
Recommendation 6:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness issue guidance to ensure Registrars authenticate the source and integrity of identity documents used during the Personal Identity Verification credential enrollment process through official Federal and State databases.**
VA Response:	Concur. OIG referenced FIPS 201-1 as the guiding document that must be adhered to ensure compliance. Review of document indicated: VA is required to establish control objectives for secure and reliable identification of Federal employees and contractors. Furthermore that "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; and that fraudulent identity source documents are not accepted as genuine and unaltered; and finally, that an issued credential is not modified, duplicated, or forged. With those requirements in highlighted, VA concurs in principle. The Assistant Secretary for OSP will issue guidance requiring all PIV Enrollment Stations to authenticate the source and integrity of identity documents used during the Personal Identity Verification credential enrollment process through official Federal and State databases. In support of this initiative, the Office of Personnel Security and Identity Management initiated a market survey to determine the availability of stand-alone ID validation software for use at each PIV Enrollment Station and is developing requirements for an open source procurement.
Supporting Documentation:	OSP Draft Memo 11-002

Status:	Include competitive acquisition in FY12 IT Acquisition Plan Target Dates: Policy Issuance: October 15, 2011 Acquisition: March 31, 2012
Recommendation 7:	**We recommend the Assistant Secretary for Operations, Security, and Preparedness make appropriate changes to the Personal Identity Verification System to prevent Enrollment Center staff from performing more than one role in the Personal Identity Verification credential issuance process.**
VA Response:	Concur. The PIV System currently prohibits PIV Enrollment Staff from performing more than one role for an individual applicant. However, the audit team identified sharing of PIV cards and PINS among PIV Enrollment Staff. Assistant Secretary for OSP will direct VA's OI&T Personal Identity Verification System managers to investigate and report back with PIV System options that would prevent Enrollment Center staff from performing more than one role for an individual applicant in the Personal Identity Verification credential issuance process. In the interim, the Assistant Secretary for OSP will issue policy guidance to Under Secretaries, Assistant Secretaries, and Other Key Officials reiterating Federal and VA policy that prohibits PIV Enrollment staff from sharing PIV credentials and PINS in the PIV Enrollment process.
Supporting Documentation:	OSP Draft Memo 11-003
Status:	Pending Assistant Secretary for OSP and General Counsel review. Target Dates: Policy Issuance: October 15, 2011 OI&T PIV System Assessment: November 30, 2011

Appendix E Office of Inspector General Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Timothy J. Crowe, Director Alan Brecese Brandon Guadalupe Charles Chiarenza Debra Cato Dennis Capps Lee Giesbrecht Mark Mullery Thomas McPherson

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.