

Department of Veterans Affairs



**DEPARTMENT OF VETERANS AFFAIRS (VA)
Office of Operations, Security, and Preparedness (OSP)
HSPD-12 Program Management Office (PMO)**

HSPD-12 Applicant Responsibilities

Version –3.0

September 15, 2008

**Department of Veterans Affairs
PIV Program Support**

Revision History Table

Date	Version	Description	Author
04/02/07	1.0	Initial	Nick Fadziejewicz
05/02/07	1.0	Edit/Format	Mary Ann Craig
05/30/07	1.0	Edits & Final Review	Seref Konur
04/07/08	1.0	Edits	Mark Chamberlain
06/04/08	1.0	Edits and Review	Lolie Kull
09/10/08	2.0	Updated Content	Sonya Weed
09/12/08	2.0	Review	Seref Konur
02/10/11	3.0	Revise/Edits	HSPD-12 PMO

Table of Contents

1 TRAINING OVERVIEW	1
2 BACKGROUND: HSPD-12 AND FIPS 201-1	1
3 PIV ROLES	1
3.1 <i>PIV Card Issuance (PCI) Manager</i>	2
3.2 <i>PIV Sponsor/Manager</i>	2
3.3 <i>PIV Registrar</i>	2
3.4 <i>PIV Issuer</i>	2
4 CARD TYPES AND ELIGIBILITY	2
4.1 <i>PIV Card</i>	2
4.2 <i>Non-PIV Card</i>	3
4.3 <i>FLASH BADGE</i>	3
5 PIV APPLICANT TRAINING TOPICS	3
6 PROCEDURES FOR CARD APPLICATION	4
7 APPLICANT RESPONSIBILITIES	4
8 SAFEGUARDING CREDENTIALS/CARD PROTECTION	5

1 Training Overview

This training focuses on the basic requirements and responsibilities of the PIV Applicant Role as it relates to the Department of Veterans Affairs (VA) implementation of Homeland Security Presidential Directive – 12 (HSPD-12). At the end of this course, Applicants will be able to:

- Discuss HSPD-12 and its purpose
- Describe the basic responsibilities of each PIV Official Role
- Demonstrate the procedures necessary for obtaining a card
- Recognize the importance of protecting the card and safeguarding credentials

2 Background: HSPD-12 and FIPS 201-1

On August 27, 2004, President George W. Bush signed [Homeland Security Presidential Directive 12 \(HSPD-12\), Policy for a Common Identification Standard for Federal Employees and Contractors](#) that requires the issuance of credentials that:

- Are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Can be utilized to control logical access to VA information systems
- Can be utilized to control physical access to VA facilities
- Are issued based on sound criteria for verifying an individual employee's identity
- Are issued only by providers whose reliability has been established by an official accreditation process

The National Institute for Standards and Technology (NIST), in response to this directive, developed [Federal Information Processing Standards Publication \(FIPS Pub\) 201-1](#). FIPS 201-1 describes the procedural and technical requirements for Federal PIV implementation. FIPS 201-1 directs the implementation of new procedural and technical requirements that standardize the credential issuance process in order to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification.

3 PIV Roles

FIPS 201-1 requires a separation of PIV Official Roles (functions) during the PIV card issuance process. A PIV Official cannot perform more than one role in the PIV issuance process for a single card applicant. For example, a PIV Sponsor cannot serve as a PIV Registrar or Issuer for an Applicant who he/she sponsored.

Any individual who serves in a PIV Official role as a PIV Sponsor, Registrar, Issuer, or PCI Manager must be appointed by his/her manager, successfully pass the Certification Training, and be certified for each PIV Official role he/she fulfills. Each of the PIV Official roles is defined in the following subsections.

3.1 PIV Card Issuance (PCI) Manager

The Facility PCI Manager oversees the PIV issuance process at a facility. This individual ensures all services specified in FIPS 201-1 are provided reliably and PIV cards are produced in accordance with requirements. He/she is responsible for certifying the PIV Officials (Sponsor, Registrar, and Issuer) at a given site and providing these role holders with access to the PIV Enrollment Portal. There should be at least one primary and one alternate PCI Manager for each facility with a badging office.

3.2 PIV Sponsor/Manager

The PIV Sponsor authorizes the request for the Applicant for a PIV, Non-PIV card, or Flash Badge. The Sponsor is a Federal employee who verifies the Applicant's need for a VA credential and the type of card the Applicant needs based on the access privileges required. The Sponsor ensures the data collected for card issuance is accurate and validates the need for a PIV card during the issuance and re-issuance/renewal process. PIV Sponsors must be federal employees. Contractors cannot serve as PIV Sponsors. There will be one or more PIV Sponsors at each facility. Sponsors are responsible for keeping the Applicant informed throughout the PIV process.

While the Sponsor authorizes the card request, it is important to note that initial Applicant data is entered by the Manager in the PIV Enrollment Portal. The Sponsor is responsible for verifying the accuracy of the data entered in the Manager section. The Manager and Sponsor may be, but are not required to be, the same individual. The Manager is not considered to be a PIV Official Role.

3.3 PIV Registrar

The PIV Registrar performs Applicant identity proofing (reviewing two approved forms of identification) and other enrollment functions that may include the collection of demographic and biometric data. The PIV Registrar is responsible for verifying the status of an Applicant's background investigation prior to card issuance. The Registrar also verifies the applicant data provided during Sponsorship. Each PIV card issuance facility should have at least one primary and one backup PIV Registrar.

3.4 PIV Issuer

The PIV Issuer produces credentials for Applicants and may perform other issuance functions to include biometric matching, PIN reset, and credential termination. The PIV Issuer is responsible for managing credential inventory and completing the Smart Card Inventory Report. Each PIV card issuance facility should have at least one primary and one backup PIV Issuer.

4 Card Types and Eligibility

VA issues three credential types that allow physical and/or logical access to VA facilities and information systems: PIV Cards, Non-PIV Cards, and Flash Badges.

4.1 PIV Card

PIV Cards are issued to employees, contractors, and affiliates who require access to a Federal facility or Federally-controlled information system for a continuous period of greater than 6 months

or more than 180 aggregated days for intermittent periods. Full-time employees can be issued only PIV cards. Two forms of identification, one of which must be a Federal or state government issued photo identification, must be provided in order to establish the identity of the Applicant. PIV cards are issued following the completion of, at a minimum, a successfully adjudicated Special Agreement Check (SAC) and the initiation of a National Agency Check with Written Inquiries (NACI).

PIV Cards are issued with physical access and may be issued with logical access. Applicants who receive PIV Cards with logical access must have a VA email address.

PIV Cards are valid for the lesser of 3 years or any existing contract plus extension years.

4.2 Non-PIV Card

Non-PIV Cards are issued to contractors and affiliates who require unsupervised, logical, and/or physical access for a continuous period of less than 6 months or less than 180 aggregated days within a one-year period. Two forms of identification, one of which must be a Federal or state government issued photo identification, must be provided in order to establish the identity of the Applicant. Non-PIV cards are issued following the completion of a successfully adjudicated Special Agreement Check (SAC).

Non-PIV Cards may be issued with physical and/or logical access and are valid for up to 6 months.

4.3 Flash Badge

Flash Badges are issued to contractors and affiliates who require common (public areas only) physical access only for less than 6 months or less or less than 180 aggregated days within a one-year period. One form of photo identification must be provided in order to establish the identity of the Applicant. No background investigation is required for a Flash Badge. Flash badges are valid for up to 1 year.

5 PIV Applicant Training Topics

A PIV Applicant is an individual to whom a card will be issued. To apply for a card, one of the following eligibility requirements must be met:

- The individual is a current Federal employee
- The individual is under contract to the Federal government
- The individual is an Affiliate. Affiliates include, but are not limited to, guest researchers, volunteers, VSO representatives, interns, residents, medical students, employees of on-site organizations providing services to VA employees such as childcare centers and credit unions.

PIV Sponsors will determine the eligibility of Card Applicants, identify the type of physical and logical access the Applicant requires, and the length of time the access is needed. Applicants and Sponsors can refer to the [PIV Card Access and Process Requirements](#) on the PIV Project website.

6 Procedures for Card Application

- Meet in person the Sponsor and provide the Sponsor with personal information
- Complete and submit background investigation forms/eQip application and fingerprints if necessary
- Obtain the requisite background investigation, dependent on card type
- Appear in person at the Registrar's workstation and provide required identification(s) in original format
- See [PIV Project](#) website for more details.
- Complete biometric capture with the Registrar (photo and/or fingerprint capture)
- Complete a biometric(e.g. photo and/or fingerprint) verification conducted by the Issuer

7 Applicant Responsibilities

Once issued a card, the Applicant is known as a Cardholder. During the acceptance of the credential, Cardholders will be presented with information about Cardholder responsibilities with respect to privacy, security, and protection of the card. Some Cardholder responsibilities include:

- Provide accurate information during the card application process
- Comply with the Certificate Practices Statement (CPS) governing the digital certificates on the card by not disclosing the user-assigned PIN that protects the private keys
- Use digital certificates and private keys for official purposes only
- Report any compromises of the card or associated PIN to the local Information Security Officer (ISO)

All Cardholders have a responsibility to contribute to the privacy, security, and protection of the PIV Program. By Title 18 of U.S. Code, it is a Federal offense to counterfeit, alter, or misuse a card produced in the card issuance system. All personnel issued a card are responsible for immediately reporting a lost, missing, stolen, or damaged card. All cardholders must protect the card and must replace the card when it becomes unusable. Specific Card Usage details can be found in the following section.

8 Safeguarding Credentials/Card Protection

It is the responsibility of all credential holders to safeguard their credentials from loss, theft, damage, and false use. Credentials and the PIN that securely authenticates identity to the credential must not be shared between individuals. Credentials should be visible at all times when at a VA facility and worn on the outermost garment, photo-side visible, when the cardholder is not sitting at his/her computer and using it for logical access. Credentials should be free of any visually altering elements such as stickers/decals, permanent or temporary symbols, or the affixing of any jewelry or pin such as a tenure or service pin.

PIV Cards are visual forms of employee identification as well as a device that can be used by VA personnel to access privileges and to conduct daily business operations such as accessing network system resources or entering approved VA facilities. Any Cardholder who does not follow the daily usage guidelines as listed in VA Handbook 0735 is in violation of the card usage agreement.

Complete procedural and usage details can be found in VA Handbook 0735. The primary Cardholder responsibilities and Card Usages are identified below:

- The Card must be protected. Cardholders are expected to protect the Card's physical integrity, operability, and data content accuracy as a normal part of their duties as an employee, contractor, or affiliate, and to alert the PIV Issuer if any of the following occurs:
 - The card begins to wear (e.g. laminate coming lose, ink rubbing off, cuts/rips/tears occur to the card)
 - The card is lost or stolen
 - The card does not operate properly when inserted into a logical or physical access reader
 - The Cardholder should notify the PIV issuer immediately if personal information changes (e.g. changes in affiliation, name change, or other information changes)
 - The card is scheduled to expire within 6 weeks (in order to maintain its operability without lapse).
- The card must not be left unattended. HSPD-12 and FIPS 201-1 require agencies to increase the protection of Government facility and systems access. The PIV Card is issued to securely and reliably provide the capability for physical and logical access. The PIV Cardholder plays a central role in this capability and must not leave the PIV Card unattended. The card must not be left in a smart card reader as doing so risks unauthorized access, tampering, or exploitation.
- The card, if not in its electromagnetic card holder, must be in a smart card reader. Electromagnetic card holders comply with FIPS 201.1 and mitigate risk of casual data capture. Only badge holders from the General Services Administration (GSA) Approved Products List (APL) shall be used to wear and display the PIV card. No pins, badges, decals, or similar items may be added to the badge or holder.