

PERSONAL IDENTIFICATION VERIFICATION (PIV) PROJECT

On August 27, 2004, President Bush signed Homeland Security Presidential Directive 12 (HSPD-12), which requires all federal employees, contractors and affiliates to have a Personal Identity Verification (PIV) identification card that complies with Federal Information Processing Standard 201 (FIPS 201). The PIV card will provide both physical access to government facilities and logical access to government information systems. Additionally, this card will facilitate interoperability among Federal agencies and departments.

HSPD-12 requires Federal agencies and departments to begin issuing PIV cards by October 26, 2006 and to complete a national roll-out of PIV cards by October 2008.

Bay Pines VA Healthcare System will begin implementation on the PIV-Phase 1 project on October 15, 2006.

Implementation of the PIV-I process will affect the following personnel ONLY:

-New Employees, Students, Contractors, Volunteers and Residents and anyone requiring a NEW VA Identification card.

THE PROCESS: All Applicants for a PIV card must be sponsored by a certified PIV Sponsor. Multiple Sponsors have already been appointed and received training at Bay Pines. The Applicant (New Employees, Students, Contractors, Volunteers and Residents) will complete VA Form 0711 and forward to their Sponsor. The Sponsor will complete their requirements on the VA Form 0711 and send to the Registrar. Fingerprints and a photograph will then be taken. A background check will be completed and the Applicant will be notified when they can receive their facility ID badge. During PIV-Phase 1, Bay Pines will continue to issue the same facility identification card you are currently using. We are expecting to move into PIV-Phase II in approximately June, 2007.

If you have questions, please contact any of the following individuals: Bo Barella ext. 7771, Kim Hansen, ext. 5648, David Jones ext. 4113

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(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. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

PERSONAL IDENTITY VERIFICATION (PIV) APPLICANT COURSE

Federal Personal Identity (PIV) Training

This course provides one hour of mandatory training on one of the four core components of the new PIV system: PIV Applicant

You must review all the pages in this course and complete the post course survey to obtain a Certificate of Completion.

PIV APPLICANT OBJECTIVES

At the end of this course, you will be able to:

- Describe Homeland Security Presidential Directive (HSPD-12) and its purpose
- Describe the Personal Identity Verification (PIV) subsystem
- Describe the different types of PIV standards
- Describe the PIV Roles and Issuance Process
- Describe the privacy requirements of the PIV process
- Describe the procedures for ID Proofing a PIV card applicant

FIPS-201 and HSPD -12 Overview

- Why a FIPS-201 Compliant Personal Identity Verification (PIV) System?
- What is HSPD-12?
- What is FIPS-201?
- What are PIV-I and PIV-II?

On August 27, 2004, President Bush signed Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. Based upon this directive, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication (FIPS Pub) 201 including a description of the minimum requirements for a Federal Personal Identity verification (PIV) system. FIPS 201 directs the implementation of a new standardized card issuance process, which is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification

PIV-I & PIV- II

The PIV standard consists of two parts:

PIV-I: PIV-I satisfies the control objectives and security requirements of HSPD-12

PIV-II: PIV-II specifies implementation and use of identity credentials on integrated circuit cards (Smart Cards) for use in a Federal personal identity verification system .

What is Personal Identity Verification (PIV)

The PIV process provides a commonly accepted, reliable and secure form of identification for all Federal employees that:

- Is issued based on sound criteria for verifying an individual's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation
- Is only issued by providers whose reliability has been established
- Will provide physical and logical access to VA facilities

PIV Roles

FIPS 201 requires a separation of roles (jobs) during the PIV issuance process.

An employee cannot perform more than one role (except for Facility PIV Card Applicant Representative and Facility Privacy Official)

Prior to start of the PIV-I process at a facility, employees or contractors must be appointed and certified for each role

Facility PIV Card Issuance (PCI) Manager

PIV REGISTRAR

PIV Registrar

PIV ISSUER

Facility PIV Card Applicant Representative

Facility Privacy Official

PIV- I& PIV- II

The VA will implement the PIV card in a two phased approach.

- Started at VACO on Dec 2006
- Other VA sites will implement PIV-I Sep-Oct 2006.
- Phase II begins in Oct 2006.

PIV APPLICANT Role, Description and Requirements

- A PIV Applicant is an individual to whom a PIV card will be issued. To apply for a PIV card, one of the following eligibility requirements must be met:
 - The individual must be a prospective or current Federal employee
 - The individual must be (or will be) under contract to the Federal government, to whom the Veterans Administration would normally issue a long-term (greater than six months) Federal identity card, consistent with existing security policies
 - The individual must be a guest researcher, volunteer, intern, or intermittent, temporary, or seasonal employee who has been authorized to receive a PIV card

PIV APPLICANT Procedures

- As an Applicant, you will be required to:
 - Appear in person (at the location indicated by your Sponsor) with two forms of valid identification, one of which must be a Federal or State-issued photo identification Be fingerprinted
 - Have a passport-quality photo taken for placement on your PIV card
 - Sign for your PIV card and acknowledge understanding of your rights and responsibilities
 - Your Sponsor will notify you of any other supporting documents or additional information that may be required to receive a PIV card

PIV APPLICANT Rights and Responsibilities

- You will be presented with information about your rights and responsibilities with respect to privacy, security, and protection of your PIV card. Some of your rights include:
 - Notification of how your personal Information in Identifiable Form (IIF) will be protected while being stored or processed, both manually and electronically
 - Correction of errors in the identity source documents and all decisions based on them
 - Notification of the disposition of your application status
 - Notification of the steps required to re-apply for a PIV card if you are denied initially

PIV Applicant Privacy, Protection and Security

All Federal employees and contractors have a responsibility to contribute to the privacy, security, and protection of the PIV Program.

- By *Title 18* of the U.S. Code, it is a Federal offense to counterfeit, alter, or misuse the PIV card and system.
- All personnel issued a PIV card are responsible for:
 - Immediately reporting a lost/missing/stolen card

- Replacing the card when it has become unusable or worn Protecting the card

PIV Applicant Instructions

Bring to the Registrar (VA Police; Building 11):

- **Two** completed fingerprint cards (unless the Registrar indicates they are unnecessary) and your background investigation forms
- **Two** IDs – one must be a Federal or State issued photo ID. Both IDs must meet the requirements set forth in the ID Proofing Criteria List ([http://vaww.va.gov/PIVPROJECT/docs/PIV_ID_Proofing_Criteria%20\(2\).doc](http://vaww.va.gov/PIVPROJECT/docs/PIV_ID_Proofing_Criteria%20(2).doc))
- Your Applicant PIV training certificate

PIV APPLICANT SUMMARY

As a PIV Applicant, your responsibilities include:

- Working with your Sponsor to complete appropriate documentation
- Submitting forms and providing identity source documents in person
- Learning about and acknowledging your rights and responsibilities in the system
- Protecting your PIV card

PIV APPLICANT FULL NAME (PLEASE PRINT)

SIGNATURE

SERVICE (WHERE YOU ARE DOING YOUR CLINICAL ROTATION)

DATE