

## HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM

- 1. REASON FOR ISSUE:** This Directive defines Department-wide policy, roles, and responsibilities for the creation and maintenance of an HSPD-12 Program necessary to implement Homeland Security Presidential Directive 12 (HSPD-12), "*Policy for a Common Identification Standard for Federal Employees and Contractors.*"
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This Directive sets forth policies, roles, and responsibilities for an HSPD-12 Program that integrates Personal Identity Verification (PIV), Physical Access Control System (PACS), and Logical Access Control System (LACS) capabilities within VA.
- 3. RESPONSIBLE OFFICE:** HSPD-12 Program Office, Office of Operations, Security, and Preparedness (007).
- 4. RELATED HANDBOOK:** VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program.*
- 5. RESCISSIONS:** None

**CERTIFIED BY:**

*/s/*

Roger W. Baker  
Assistant Secretary for  
Information and Technology

**BY DIRECTION OF THE SECRETARY OF  
VETERANS AFFAIRS:**

*/s/*

Jose D. Riojas  
Assistant Secretary for Operations,  
Security, and Preparedness

Distribution: Electronic Only



## HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM

### 1. PURPOSE

a. This Directive defines Department-wide policy, roles, and responsibilities necessary to implement Homeland Security Presidential Directive 12 (HSPD-12), "*Policy for a Common Identification Standard for Federal Employees and Contractors*" and establishes policy for the creation and use of the Federal government identification credentials within the Department of Veterans Affairs (VA).

b. The policies identified in this Directive apply to all VA administrations, staff offices, employees, contractors, and affiliates seeking access to VA facilities or information systems.

### 2. POLICY

a. The Personal Identity Verification (PIV), Non-PIV, and Flash badges, issued in accordance with HSPD-12 and Federal Information Processing Standards (FIPS) 201-1, are the sole credentials for Federal Identity Verification at VA. Credentials issued by VA organizations, such as those issued to VA Police, Office of the Inspector General (OIG) Inspectors and Healthcare Professionals establish the authority and rights of a position. These credentials must be used in combination with the PIV credential to verify the card holder's identity. Visitor passes are not governed by HSPD-12 policies. Issuance of visitor passes is the responsibility and at the discretion of each facility.

b. VA will establish:

(1) Standards, processes, and procedures for the creation, usage, and maintenance of identities and identity credentials for all VA employees, contractors, and affiliates accessing VA facilities, services, and/or information systems.

(2) Policies and procedures for requesting, sponsoring, identity proofing, registering, and adjudicating identities and issuing and re-issuing of identity credentials to VA employees, contractors, and affiliates based on access determinations.

(3) Policies and procedures to ensure only authorized personnel are permitted to issue identity credentials to sponsored individuals whose identities are validated and who possess an appropriate background investigation.

(4) An HSPD-12 Executive Committee lead by the HSPD-12 Program Office and comprised of Administration and Staff Offices representatives to set priorities, ensure privacy and information security requirements are met, align activities within the business line, and maximize the benefits realized by VA through the HSPD-12 Program.

c. To the extent that this Directive applies to Title 38 employees, the authority for implementing it is 38 U.S.C. 7421.

### 3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** The Secretary, or the Deputy Secretary, is responsible for the VA HSPD-12 Program. The Secretary delegates this authority as set forth below and makes other delegations as appropriate.

b. **Assistant Secretary for Operations, Security, and Preparedness (AS/OSP),** or designee, will:

(1) Establish, maintain, and monitor Department-wide HSPD-12 policies, procedures, training, oversight, compliance and inspection requirements of the VA HSPD-12 program.

(2) Issue directives and handbooks to provide direction for implementing the requesting, sponsoring, identity proofing, registering, adjudication of background investigations, issuing, and usage of identities and identity credentials as elements of the HSPD-12 program to all Department organizations.

(3) Develop technical and interoperability policies, procedures, and requirements for procurement and implementation of a VA national Physical Access Control Systems (PACS) program that use PIV and non-PIV cards for access in accordance with FIPS 201 and Office of Management and Budget (OMB) requirements.

(4) In cooperation with the Office of Information and Technology (OI&T), approve the policy, procedures, and requirements for a national Logical Access Control System (LACS) program that use PIV and non-PIV cards for access in accordance with FIPS 201 and OMB requirements.

(5) Develop and maintain the implementation plan for the Department's HSPD-12 Program to include PIV, PACS and LACS.

(6) Establish policies and procedures for the training of all roles in the HSPD-12 process.

(7) Develop policies and procedures for issuing VA PIV, non-PIV, and Flash badges.

(8) Develop policies and procedures for VA facilities to provide enrollment operations to support other VA staffs in the issuance of PIV cards.

(9) Assign access rights within PACS for physical access for all employees, contractors, and affiliates requiring access to VA facilities.

(10) Maintain the operations of VA Central Office (VACO) PACS.

(11) Establish VA personnel security and suitability directives and handbooks for all individuals requiring access to VA facilities and/or information systems.

(12) Ensure the initiation and adjudication of background investigations for all employees, contractors, and affiliates assigned to VA Central Office.

(13) Maintain a record of all background investigations for all employees, contractors, and affiliates.

c. **Assistant Secretary for Information and Technology (AS/OI&T), who serves as VA Chief Information Officer, or designee, will:**

(1) Ensure compliance with the responsibilities set forth in paragraph 3.e. of this Directive.

(2) Establish and operate a PIV help desk for the lifecycle of HSPD-12 related components.

(3) Ensure interoperability and conformance to applicable Federal standards for the lifecycle of HSPD-12 related components.

(4) Establish OI&T policies which clearly state IT processes, roles, and responsibilities in conformance with the VA HSPD-12 Program requirements.

(5) Assist OSP with developing and maintaining the infrastructure and connectivity for a PACS that complies with HSPD-12 technical and interoperability standards.

(6) In cooperation with OSP, establish and maintain an enterprise LACS infrastructure that complies with HSPD-12 technical and interoperability standards.

(7) Ensure the protection of personal privacy in accord with HSPD-12 and the requirements of FIPS 201, section 2.4. In accordance with those requirements, OI&T shall conduct a yearly, or as-needed based on changes to the system, review and update of the PIV System's Privacy Impact Assessment and System of Records Notice.

(8) Publish a quarterly report on the number of PIV credentials issued to employees, contractors, and affiliates as required by OMB.

d. **Executive Director, Office of Acquisition, Logistics, and Construction (OALC), or designee, will:**

(1) Ensure compliance with the responsibilities set forth in para. 3.e. of this Directive.

(2) Maintain design and building specifications in accordance with requirements defined by OSP and Office of Security and Law Enforcement (OSLE) as they relate to HSPD-12 and physical security.

(3) Ensure all VA contracts and exercised options adhere to Subpart 4.13 of the Federal Acquisition Regulation (FAR).

(4) Review and distribute relevant policies, procedures, and information to agency procurement operations as additional system requirements and operational procedures are defined by OSP.

(5) Determine, in cooperation with managers, Personnel Security and Suitability Service (PSSS), and the Office of Human Resources and Administration (OHR&A) position risk designations for all contractors, as needed.

(6) Evaluate and report, in collaboration with OSP, the status of background investigations for current contractor employees.

(7) Initiate, in collaboration with PSS and the SIC, required background investigations for all contractor employees who do not have a successfully adjudicated investigation on record or are undergoing a badge reissuance.

(8) Ensure that VA Contracting Officers appoint a Contracting Officer's Technical Representative (COTR) as the PIV Sponsor for each contract. The PIV Sponsor must be a Federal government employee and a COTR.

**e. Under Secretaries, Assistant Secretaries, Deputy Assistant Secretaries, and Other Key Officials will:**

(1) Ensure compliance with the policies, procedures, and guidance issued by OSP and established in this Directive and associated policies.

(2) Ensure that all products purchased for HSPD-12 related applications meet all applicable Federal standards and requirements, are listed on the FIPS Approved Products List (APL), and are tested to ensure interoperability with the current environment.

(3) Participate in the HSPD-12 Executive Committee.

(4) Ensure the accuracy, validity, and completeness of all information entered into data systems used to support the implementation of the HSPD-12 program such as the Personnel and Accounting Integrated Data (PAID), Personnel Information Processing System (PIPS), and the PIV System.

(5) Ensure training for individuals to fulfill the roles for PIV Card Issuer (PCI) Manager, Sponsor, Registrar, Issuer, and PIV Card Applicant Representatives.

(6) Ensure applicants travel to enrollment stations for enrollment and activation, renewal, reissuance, or PIN reset of their VA PIV, non-PIV or other appropriate badges.

(7) Ensure compatibility of the organization's Physical Access Control System (PACS) and Logical Access Control System (LACS) with VA requirements and compliance with VA PACS and LACS policies and procedures.

(8) Maintain all forms and records that will permit the audit of the organization's PIV programs in accordance with HSPD-12, FIPS 201-1, relevant Office of Management and Budget (OMB) guidance, and Office of Inspector General (OIG) requirements.

(9) Ensure personal information collected is handled in a manner consistent with the Privacy Act of 1974 (5 U.S.C. § 552a) and Federal Information Security Management Act (FISMA) requirements.

f. **Facility Directors/Regional Office Directors** will:

(1) Ensure compliance with the responsibilities set forth in para. 3.e. of this Directive.

(2) Appoint, in writing, a minimum of one and a maximum of three PCI Managers to be responsible for the following: appointing, in writing, registrars and issuers to support the badging office; managing the PIV operations and credential life cycle at the facility in accordance with this directive and associated handbook; ensuring initiation and completion of appropriate employee, contractor, and affiliate background checks prior to issuing a badge; managing the lifecycle of the badge to include creation, recovery, and destruction; and PACS management.

(3) Ensure the staffing of a full-time badging office during the normal operating hours of the facility comprised of a minimum of three staff to ensure continued operation. Waivers of full time operation will be reviewed on a case-by-case basis by the AS/OSP.

(4) Issue, upon deployment of the capability to do so, only PIV, non-PIV, or Flash Pass badges, based on access requirements, to all new and existing employees, contractors, and affiliates. Existing employees, contractors, and affiliates shall be issued the aforementioned badges for all cases of badge re-issuances to include lost, stolen, or defective badges and badge renewals.

(5) Report to the Program Management Office issuance status for all PIV, non-PIV, and Flash badge new issuances, renewals, and reissuances including lost, damaged, or stolen badges monthly.

(6) Ensure sustained operation of the PACS at the facility.

g. **Directors of Human Resources Management Offices** will:

(1) Ensure compliance with the responsibilities set forth in para. 3.e. of this Directive.

(2) Determine and assign in the Position Designation System and Automated Tool (PDAT), in cooperation with program managers, position risk designations for all VA employee positions.

(3) Ensure appropriate background investigations, commensurate with position risk designations in PDAT, are initiated and adjudicated within the allotted timeframes and recorded in PAID.

(4) Ensure appropriate administrative action is taken with regard to employment suitability in accordance with federal laws, Titles 5 and 38 of the United States Code, regulations, Code of Federal Regulations Parts 5 and 38, and VA policy and procedures.

h. **Directors of Voluntary Service** will:

(1) Ensure compliance with the responsibilities set forth in para. 3.e. of this Directive.

(2) Ensure the accuracy and completeness of all information entered into volunteer data systems used to support the implementation of the HSPD-12 Program.

(3) Determine and assign in the Position Designation System and Automated Tool (PDAT), in cooperation with program managers, position risk designations for all VA employee positions.

(4) Ensure appropriate background investigations, commensurate with position risk designations in PDAT, are initiated and adjudicated within local policy and timeframes.

i. **Identity Credential Holders.** Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

#### 4. REFERENCES

a. E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002), Titles I-III (the Federal Information Security Management Act (FISMA), codified at 44 U.S.C. Sections 3541-3549)

b. Executive Order 10450, Security Requirements for Government Employment, as amended

c. Federal Acquisition Regulation (FAR), Subpart 4.13

d. Federal Information Processing Standards Publication (FIPS) 199, Standards for the Security Categorization of Federal Information and Information Systems, February 2004

e. Federal Information Processing Standards Publication (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, issued February 25, 2005, and amended March 2006

f. Freedom of Information Act, 5 U.S.C. 552

g. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004

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

i. OMB Circular A-130, including its appendices

j. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008

k. OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 –Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005

l. OMB Memorandum M-08-01, HSPD-12 Implementation Status, October 23, 2007

- m. Privacy Act of 1974, 5 U.S.C. 552a
- n. VA Directive and Handbook 5005, Staffing.
- o. VA Directive and Handbook 5021, Employee/Management Relations.
- p. VA Directive and Handbook 0710, Personnel Suitability and Security Program.
- q. 5 C.F.R. Parts 731, 732, and 736, Suitability; National Security Positions; and Personnel Investigations, respectively
- r. 5 U.S.C. 301, Departmental Regulations
- s. 38 U.S.C. 7421, Personnel administration: in general

## 5. DEFINITIONS.

a. **Access Control:** The process of granting or denying specific requests to obtain and use information and/or related information processing services (that is, logical access to VA information and information systems) and to enter specific physical facilities (that is, physical access to VA owned or leased buildings and spaces).

b. **Affiliate:** Individuals who require logical access to VA information systems and/or physical access to VA facilities to perform their jobs and who do not fall under the category of Federal employee or contractor. Examples include but are not limited to: Veteran Service Organizations (VSO) representatives, Joint Commission Reviewers, childcare staff, credit union staff, Union Officials and union support staff.

c. **Applicant:** An individual applying for a VA PIV, non-PIV, or Flash Badge. An applicant may be a current or prospective Federal employee, contractor, or other individual requiring access to VA facilities, services, and/or information systems on a recurring basis.

d. **Background Investigation:** A process to ensure that a person is reliable, trustworthy, of good character and conduct, and loyal to the United States. The procedure includes verification and accuracy of an individual's identification, credentials, and employment history. May include screening consisting of fingerprint checks for criminal history records, validation of resume and/or education references, and checks of various databases for appropriate preliminary checks.

e. **Contractor:** A non-Federal employee who is under contract for furnishing supplies and/or services to VA who will have access to VA information systems and/or physical access to VA facilities regardless of frequency or length of time.

f. **Credential:** Documentary evidence that attests to an individual's identity used to grant authorization to access VA facilities, services, and/or VA information systems. In this directive a credential can be a PIV Card, Non-PIV Card, or Flash Badge.

g. **Employee:** Defined in title 5 U.S.C. 2105(a) as an individual who is appointed in the civil service and engaged in the performance of a Federal function under supervision by a Federal officer or employee.

h. **Federal Information Processing Standard (FIPS) 201 Approved Products List (APL):** A list of products and services that are in compliance with the current version of the Federal Information Processing Standard 201 and its supporting publications. The list may be found at <http://fips201ep.cio.gov/apl.php>. Only those products and services (service providers) listed on the FIPS 201 APL are recognized as being in compliance with HSPD-12.

i. **Flash Badge:** A VA identification (ID) card containing a photograph issued to an individual for infrequent access to VA public areas only (such as cafeterias, lobbies, libraries, credit unions) for a period not to exceed 12 months.

j. **Identification:** The process of discovering the true identity of a person, defined by known or recognized characteristics such as birth place, age, and residence of a person.

k. **Identity:** The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

l. **Identity Proofing:** The process of analyzing identity source documents provided by an applicant to determine if they are authentic, to contact sources of the documents to verify that they were issued to the applicant, and to perform background checks of the applicant to determine if the claim of identity is correct.

m. **Infrequent Access:** Accessing VA facilities and/or information systems for a period of less than 6 months in a year, or a period of less than 180 aggregate days in a 1 year period.

n. **Interoperability:** For the purposes of this Directive, interoperability allows any Federal government facility or information system, regardless of the PIV issuer, to verify a cardholder's identity using the credentials on the PIV card.

o. **Logical Access Control System (LACS):** Systems which authenticate and authorize an individual to access federally-controlled information systems.

p. **Non-PIV Badge:** A VA ID card containing a photograph issued to persons who do not require a PIV Badge but need unaccompanied, infrequent access to VA facilities or information systems for a period not to exceed six (6) months.

q. **Personal Identity Verification (PIV) Card Issuer (PCI):** An authorized HSPD-12 compliant PIV credential issuing organization that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.

r. **PCI Manager:** The individual or entity responsible for the operations required of identity proofing and PIV card issuance performed by a PIV Card Issuer.

s. **PIV Badge:** An identification card that complies with FIPS 201 and related guidance that contains a photograph and stored identity information so that the claimed identity of the cardholder can be verified by another person or an automated process. PIV badges are issued to persons requiring routine access to VA facilities or information systems.

t. **PIV Registrar:** The individual or entity who establishes and vouches for the identity of an applicant to a PIV Card Issuer. The PIV Registrar authenticates the applicant's identity by checking identity source documents, identity proofing, and ensures a proper background check has been completed before the credential or badge is issued.

u. **PIV Sponsor:** The individual who establishes the need for a relationship between VA and the applicant and requests that a credential be issued to an applicant pending appropriate identity proofing and background checks. This PIV official role must be performed by a Federal government employee.

v. **Physical Access Control System (PACS):** Systems which authenticate and authorize an individual to access Federally-controlled government facilities.

w. **Resource:** For purposes of this directive, the term "resource" refers to any physical or logical asset including but not limited to buildings, rooms, data (electronic and paper), and information technology.

x. **Routine Access:** Accessing VA facilities and/or information systems, without an escort and/or continuous monitoring by a VA official, for a period of more than 180 days in a 365 day period.

y. **Special Agreement Check (SAC):** A SAC is a fingerprint-only check. A successfully adjudicated SAC is required to obtain a non-PIV card.

z. **Visitor:** Any individual requiring escorted access and is on VA property fewer than fifteen (15) days in a 365 day period. Visitor Passes as stated in para. 2.a, are not governed by HSPD-12 policies. Issuance of visitor passes is the responsibility and at the discretion of each facility.