Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 0735
Transmittal Sheet
October 26, 2015

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM

1. REASON FOR ISSUE: This Directive defines Department-wide policy, roles, and responsibilities for the creation, operation, and maintenance of an HSPD-12 Program necessary to ensure Department compliance of 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 defines Department-wide policies, roles, and responsibilities for aligning Personal Identity Verification (PIV), Logical Access Control System (LACS), and Physical Access Control System (PACS) with the Identity, Credential, and Access Management capabilities within VA.

3. RESPONSIBLE OFFICE: Office of Operations, Security, and Preparedness (007), Personnel Security and Identity Management, HSPD-12 Program Management Office.

4. RELATED HANDBOOK: VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*.

5. RESCISSIONS: VA Directive 0735, *Homeland Security Presidential Directive (HSPD-12) Program, issued February 17, 2011.*

CERTIFIED BY:

/s/

LaVerne H. Council
Assistant Secretary,
Office of Information and Technology,
and Chief Information Officer

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Kevin T. Hanretta
Assistant Secretary for Operations,
Security, and Preparedness

THIS PAGE LEFT INTENTIONALLY BLANK

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM

1. PURPOSE

a. This Directive establishes Department-wide requirements and responsibilities for VA's HSPD-12 program:

b. To provide a trusted framework and common identity infrastructure used to access VA facilities and information systems;

c. To reduce the identity, credential, and access management burden for individual Department employee, contractor, and affiliate organizations by fostering common interoperable approaches;

d. To align identity, credential, and access management policies and approaches;

e. To establish roles to enhance interoperability when collaborating with external identity management activities; and

f. To provide notification that these policies apply to all Department administrations, staff offices, employees, contractors, and affiliates requiring access to Department facilities and information systems.

2. POLICY

a. Department facilities and information systems must meet identity, credentialing, and access management requirements of HSPD-12 and Office of Management and Budget (OMB) Memorandum 11-11 *Continued Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011, which requires that agency implementations align with the Federal Chief Information Officers Council's Federal Identity Credential Access Management (FICAM) Roadmap and Implementation Guidance.

b. The Department must procure services and products that comply with HSPD-12 requirements in current Federal Acquisition Regulations (FAR) and, where applicable, are on the General Services Administration (GSA) Approved Products List.

c. The Department must issue and manage the lifecycle of the Personal Identity Verification (PIV) Credential, used in accordance with HSPD-12 and the current version of FIPS 201.

d. The VA PIV Credential is the sole identity credential for Department employees, contractors, and affiliates.

e. The Department will establish:

(1) Standards, processes, policies, and procedures for the creation, issuance, usage, maintenance, provisioning, and de-provisioning of identities and identity credentials for all Department employees, contractors, and affiliates accessing VA facilities and information systems.

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

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

(4) Policies and procedures for the use of identities and identity credentials for access to Department facilities and information systems.

(5) Policies and procedures to ensure that the proper identity verification is made when an individual attempts to access Department facilities and information systems.

(6) A Governance Board led by the PSIM (Personnel Security and Identity Management) Director, Assistant Secretary for Operations, Security, and Preparedness (AS/OSP), or designee, which is comprised of administration and staff office representatives to set priorities, to provide support, advice, and coordination among the various stakeholders on initiatives undertaken by the HSPD-12 Program Management Office (PMO) as set forth in the Governance Board Charter.

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. **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 products and services meet all applicable Federal standards and requirements, are listed on the GSA Approved Products List (APL), and are tested to ensure interoperability with the current environment.

(3) Participate in the Governance Board established by OSP.

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

(5) Ensure applicants travel for enrollment and activation, renewal, reissuance, or PIN reset of the Department Credential.

(6) Ensure compatibility and interoperability of the organization’s PACS and LACS with VA requirements.

(7) Ensure compliance with Department PACS and LACS policies and procedures.

(8) Maintain all forms and records that will permit the audit of the organization's compliance in accordance with HSPD-12, the current version of FIPS 201, Federal Information Security Management Act (FISMA), and relevant OMB guidance.

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

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

(1) Develop standards, processes, policies, and procedures for the creation, issuance, usage, maintenance, provisioning, and de-provisioning of identities and identity credentials for all Department employees, contractors, and affiliates accessing VA facilities and information systems.

(2) Develop policies and procedures for requesting, sponsoring, identity proofing, registering, and adjudicating identities and issuing and re-issuing of identity credentials to Department employees, contractors, and affiliates.

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

(4) Develop policies and procedures for the use of identities and identity credentials for access to Department facilities and information systems.

(5) Develop policies and procedures to ensure that the proper identity verification is made when an individual attempts to access Department facilities and information systems.

(6) Lead or designate a representative to lead a Governance Board, comprised of administration and staff office representatives to set priorities, to provide support, advice, and coordination among the various stakeholders on initiatives undertaken by the HSPD-12 PMO as set forth in the Governance Board Charter.

(7) Establish, maintain, and monitor Department-wide identity, credential, and access management policies, processes, procedures, training, oversight, compliance, and inspection requirements.

(8) Establish, maintain, and issue directives and handbooks that direct the implementation for requesting, sponsoring, identity proofing, registering, adjudication of background investigations, issuing, provisioning, de-provisioning, and usage of identities and identity credentials as elements of identity, credential, and access management.

(9) Develop policies, procedures, and procurement requirements for the Department-wide Physical Access Control System (PACS) program.

(10) Manage the implementation of the Departmental PACS program.

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

(12) Approve the policies, procedures, requirements, and implementation of the Departmental Logical Access Control System (LACS) program in cooperation with the Office of Information and Technology (OI&T).

(13) Approve the policies, procedures, requirements, and implementation of the Departmental Identity and Access Management (IAM) program in cooperation with OI&T.

(14) Develop and maintain Departmental implementation of identity, credential, and access management.

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

(16) Develop policies and procedures for issuing VA PIV, non-PIV, and Flash Credentials.

(17) Develop physical access policies for all employees, contractors, and affiliates requiring access to VA facilities.

(18) Develop policies and procedures for VA facilities to provide enrollment operations and issuance of HSPD-12 Credentials as specified in the current versions of FIPS 201 and NIST Special Publication 800-79, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs*). Such procedures include the designation of qualified individuals to the roles of Designated Accreditation Authority (DAA), Assessor, VA Official for Privacy (AOP), and other VA officials involved with identity management.

(19) Establish VA Personnel Security and Suitability directives and handbooks for all individuals requiring access to VA facilities and information systems.

(20) Determine position designations for all individuals requiring access to VA facilities and information systems.

(21) Ensure the initiation, adjudication, and reinvestigation of background investigations for all employees, contractors, and affiliates.

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

(23) Collaborate with OI&T to publish a quarterly report on the number of PIV credentials issued to employees, contractors, and affiliates as required by OMB and other reports as necessary.

d. **Executive in Charge, Office of Information and Technology, and Chief Information Officer,** or designee, will:

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

(2) Establish and operate a help desk to support identity, credential, and access management program related systems and operations.

(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 identity, credential, and access management program requirements as defined by OSP.

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

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

(7) Ensure the protection of personal privacy in accordance with HSPD-12 and the requirements of the appropriate sections of the current version of FIPS 201-2.

(8) 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 (PIA) and System of Records Notice (SORN).

(9) Assist OSP to publish a quarterly report on the number of PIV Credentials issued to employees, contractors, and affiliates as required by OMB and other reports as necessary.

(10) Approve the policies, procedures, requirements, and implementation of the Departmental LACS program in cooperation with the AS/OSP.

(11) Approve the policies, procedures, requirements, and implementation of the IAM program in cooperation with the AS/OSP.

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

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

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

(3) Ensure all VA contracts and exercised options adhere to Subpart 4.13 of the FAR and OMB Memorandum 11-11.

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

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

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

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

(2) Appoint, in writing, a minimum of one and a maximum of three PIV Credential Issuance Facility (PCIF) 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 credential; managing the lifecycle of the credential to include creation, recovery, and destruction; and PACS management.

(3) Ensure the staffing of a badging office, as they see fit to accommodate customers, during the normal operating hours of the facility. In order to meet separation of duty requirements, the badging office will be comprised of a minimum of three staff to ensure continued operation.

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

(5) Report to AS/OSP or designee issuance status for all PIV, non-PIV, and Flash Credential new issuances, renewals, and reissuances including lost, damaged, or stolen credentials monthly.

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

g. **Identity Credential Holders** will:

(1) Comply with all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with Department policies and procedures, displaying their credentials at all times, and returning the identity credentials upon termination of their relationship with VA.

(2) Comply with LACS and PACS usage policies.

4. REFERENCES

a. E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002);Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (Dec. 18, 2014), codified at 44 U.S.C. Sections 3551-3558

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, issued February 2004

e. Federal Information Processing Standards Publication (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, dated February 25, 2005, and amended October 2013

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 800-79-1, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, issued July 2005, amended June 2008

i. OMB Circular A-130, including its appendices

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

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

l. OMB Memorandum M-11-11, Continued Implementation of HSPD-12, dated February 3, 2011

m. Privacy Act of 1974, 5 U.S.C. 552a

n. Public Law 105-220, § 408(b) (Sec. 508, Electronic and Information Technology), codified at 29 U.S.C. § 794d

o. VA Directive and Handbook 5005, Staffing

p. VA Directive and Handbook 5021, Employee/Management Relations

q. VA Directive and Handbook 0710, Personnel Suitability and Security Program

r. VA Directive and Handbook 0730, Security and Law Enforcement

s. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program

t. 5 C.F.R. Parts 731, 732, and 736, Suitability; National Security Positions; and Personnel Investigations, respectively

u. 5 U.S.C. 301, Departmental Regulations

v. 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 Credential. 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. **Biometric:** A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

f. **Certification:** The formal process of assessing the attributes (e.g., knowledge, availability, accountability, trustworthy, security) of a process, role, or task using various methods of assessment (e.g., interviews, document reviews, test results, evaluations, validations reports) that support the assertion of reliability and capability to perform the process, role, or task.

g. **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.

h. **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 Credential.

i. **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.

j. **Federal information Processing Standards (FIPS):** A standard for Federal computer systems, for adoption and use by Federal agencies or a contractor or organization acting on behalf of a Federal agency, that has been developed and issued by the National Institute of Standards and Technology (NIST) and the Department of Commerce under 40 USC 11331.

k. **Flash Credential:** 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.

l. **General Services Administration (GSA) 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.

m. **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.

n. **Identity:** The set of physical and behavioral characteristics by which an individual is uniquely recognizable and may include a digital, electronic, or physical record.

o. **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.

p. **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.

q. **Initiated:** The formal acceptance of an investigation for processing by the Office of Personnel Management (OPM), denoted by a status of “scheduled” in the OPM PIPS.

r. **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.

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

t. **National Agency Check with Written Inquiries (NACI):** Conducted by OPM, this investigation covers a period of 5 years and consists of a review of current records in the OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and an FBI fingerprint check as well as written inquiries to previous employers and references listed on the application for employment. It is used for Non-sensitive or Low Risk positions in VA.

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

v. **Personal Identity Verification Card Applicant Representative (PCAR):** The PCAR represents the interests of current or prospective employees, contractors, and affiliates who are the applicants for PIV Credentials. They are responsible for assisting an applicant who is denied a PIV Credentials because of missing or incorrect information, and for ensuring that all applicants obtain useful information and assistance when needed.

w. **Personal Identity Verification Credential Issuing Facility (PCIF):** An installation that adequately houses and supports PCI personnel, storage of vital and sensitive records, test systems and associated components (hardware/software/firmware), and other operational components.

x. **Personal Identity Verification Credential Issuance Facility (PCIF) Manager:** The individual or entity responsible for the operations required of identity proofing and PIV card issuance performed by a PIV Card Issuer.

y. **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.

z. **Personal Identity Verification (PIV) Credential:** 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 credentials are issued to persons requiring routine access to VA facilities or information systems.

aa. **Personal Identity Verification (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 credential is issued.

bb. **Personal Identity Verification (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.

cc. **Physical Access:** Access to areas within or on a VA facility that may or may not be controlled by locks, card readers, guards, or other security devices.

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

ee. **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.

ff. **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.

gg. **Special Agreement Check (SAC):** A SAC is an automated records check conducted by the Federal Bureau of Investigation in collaboration with the Office of Personnel Management.

hh. **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 of VA Handbook 0735, are not governed by HSPD-12 policies. Issuance of visitor passes is the responsibility and at the discretion of each facility.