Department of Homeland Security
DHS Directives System
Directive Number: 121-03
Revision Number: 01
Issue Date: MAY 11 2017

Common Identification Standard for DHS Employees, Contractors, Visitors, and Affiliates

I. Purpose

This Directive establishes the Department of Homeland Security (DHS) framework for enterprise policy, responsibilities, and requirements regarding governance and implementation of Homeland Security Presidential Directive 12 (HSPD-12) and authorized authoritative credentials as the common identification standard for DHS employees, contractors supporting a DHS contract, and other affiliates supporting the Department. Authorized authoritative credentials include the DHS Personal Identity Verification (PIV) Card; the Derived PIV Credential (i.e., derived from the DHS PIV Card) as the common identification standard for secure mobile device management; and Temporary Credentials (e.g., identity credentials for facility and/or logical access, PIV Interoperable, etc.) as a common identification standard for other personnel, visitors, and affiliates.

II. Scope

This Directive is applicable throughout DHS with the exception of the U.S. Coast Guard, which uses the Common Access Card under the authorities of the Department of Defense.

This Directive applies to the lifecycle management of DHS-issued authoritative credentials to all DHS federal employees, contractor employees, temporary employees, internal and external detailees, foreign nationals, visitors, affiliates, and other authorized personnel with a need to access a DHS facility and/or a DHS network.

This Directive supersedes DHS Management Directive 11020.1, Issuance of Access Control Media and Chief Security Officer Memoranda, HSPD-12 Requirements for All DHS Personnel, October 19, 2006; Component Implementation of HSPD-12, December 2, 2008; Request to Designate a Component Primary Authority for HSPD-12, May 14, 2009; Required Review for HSPD-12 Related Plans and Acquisitions, August 21, 2009; One DHS PIV Card Issuance in the NCR, December 17, 2009; Required Actions to Fulfill HSPD-12 Mandate, January 22, 2010; Operations of DHS PIV Card Issuer Facility (PCIF) and PCIF Managers, July 10, 2012; and Updates and Clarifications to PCI Policies, Roles and Responsibilities, January 6, 2014. This Directive also supersedes the PIV Card Issuer Organization Identity Management Official issued memoranda, HSPD-12 Procedures Separation of Roles, April 1, 2009; and PCIF Managers and Enrollment Officials have Revocation Rights, August 23, 2013.

III. Authorities

A. Federal Acquisition Regulation Subpart 4.13, "Personal Identity Verification"

B. Federal Acquisition Regulation Subpart 52.204-9, "Personal Identity Verification of Contractor Personnel," January 2011

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

D. DHS Delegation 12000, "Delegation for Security Operations within the Department of Homeland Security," June 5, 2012

E. DHS Directive 121-01, Rev 01, "Office of the Chief Security Officer," February 6, 2014

F. DHS Under Secretary for Management Memorandum, "Implementation Plan Approval Request—Homeland Security Presidential Directive 12 (HSPD-12)," April 13, 2007

G. National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS) 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013

H. National Institute of Standards and Technology Special Publication 800-37 Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information systems: A Security Life Cycle Approach," February 2010

I. National Institute of Standards and Technology Special Publication 800-79-2, "Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)," July 30, 2015

J. National Institute of Standards and Technology Special Publication 800-157, "Guidelines for Derived Personal Identity Verification (PIV) Credentials," December 2014

K. Office of Management and Budget 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. Office of Management and Budget Memorandum M-07-06, "Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials," January 11, 2007

M. Office of Management and Budget Memorandum M-11-11, "Continued Implementation of HSPD-12—Policy for a Common Identification Standard for Federal Employees and Contractors," February 3, 2011

N. Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008

O. Office of Personnel Management Federal Investigations Notice 10-05, "Reminder to Agencies of the Standards for Issuing Identity Credentials Under HSPD-12," May 17, 2010

P. Department of Defense (DOD) Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," January 23, 2014

Q. Federal Chief Information Officer (CIO) Council, "Personal Identity Verification Interoperability for Non-Federal Issuers," May 2009

IV. Responsibilities

A. The ***Chief Security Officer (CSO), under the direction and authority of the Under Secretary for Management***, is responsible for all aspects of this Directive.

B. The ***CSO:***

1. Has Department-wide responsibility for all documented policies and requirements in DHS Delegation 12000 and DHS Directive 121-01 to specifically develop, implement, and oversee the DHS HSPD-12 Program for all DHS-issued authoritative credentials. The publications (e.g., the DHS PCI Operations Plan and DHS Derived PCI Operations Plan) managed by the DHS HSPD-12 Program for DHS-issued authoritative credentials detail the roles, responsibilities, acquisition, lifecycle management, and other related items for DHS-issued authoritative credentials.

2. Oversees the DHS Office of the Chief Security Officer (OCSO) program responsible for executing DHS issuance and lifecycle management activities and coordinating with the DHS Office of the Chief Information Officer programs responsible for the Identity, Credential, & Access Management (ICAM) activities and technical integration related to logical access through the use of public key infrastructure certificates applied to DHS-issued authoritative credentials.

3. Coordinates authorization activities with the Designated Authorizing Official and the Organization Identity Management Official within the DHS OCSO program responsible for executing DHS-issued authoritative credential management.

C. *The* ***Chief Information Officer (CIO)*** has Department-wide responsibility for all documented policies and requirements in DHS Delegation 04000, DHS Directive 140-01, and DHS Directive 142-02.

D. The ***Component Heads*** coordinate with the DHS CSO and DHS CIO to implement this Directive and other requirements related to HSPD-12 initiatives for the common identity standard for DHS employees, contractors, temporary employees, internal and external detailees, foreign nationals, visitors, affiliates, and other authorized personnel.

E. The ***Designated Authorizing Official, Organization Identity Management Official, and PIV Card Issuer Managers*** assume the responsibilities listed in the NIST Publication 800-79-2.

F. The ***DHS-Issued Authoritative Credential holders***:

1. Use DHS-issued authoritative credentials for official purposes only and maintain control at all times of the issued credential, not allowing anyone to use the issued credential for unauthorized purposes.

2. Do not alter or otherwise deface the DHS-issued authoritative credential to include punching a hole in, adhering decals to, or embossing the authoritative credential.

3. Report changes immediately to an appropriate authority for employee status, name, attributes, or if any DHS-issued authoritative credential is compromised, damaged, lost, or stolen.

4. Surrender a DHS-issued authoritative credential to an appropriate authority when employment or association with DHS is terminated, service is discontinued, or upon request by appropriate authority.

V. Policy and Requirements

A. ***Policy***:

1. The DHS HSPD-12 Program for DHS-issued authoritative credentials serves as a foundation for DHS Components to use in the issuance and management of DHS-issued authoritative credentials within their Components. The DHS HSPD-12 Program for DHS-issued authoritative credentials ensures compliance to the FIPS 201, NIST Special Publications, and DHS PIV Card program publications is followed by each DHS Component. The HSPD-12 Program clarifies DHS-issued authoritative credential policies, adapts them to specific circumstances, and imposes additional requirements when necessary.

2. All DHS Components ensure compliance with the FIPS 201 minimum requirements, NIST Special Publications, and the governance documented in the DHS PIV Card program publications.

3. All DHS employees, contractors, affiliates, and other eligible DHS authoritative credential applicants with a need to access a DHS facility and/or a DHS network meet the background investigation and other DHS requirements prior to DHS authoritative credential issuance.

B. ***Requirements***:

1. All PCIFs operated within the Department are within the authorization boundary of the DHS PCI and/or the DPCI and adhere to the governance documented in the DHS PIV Card program publications. All PCIFs within the DHS PCI authorization boundary are subject to assessments in compliance with NIST Special Publication 800-79-2.

2. DHS Headquarter (HQ) and Components operating a PCIF have a designated PCIF Manager executing the direction provided by the Organization Identity Management Official of the DHS HSPD-12 Program. An alternate PCIF

Manager may be designated if needed based on operational needs of DHS HQ or Components.

3. DHS HQ and Component personnel accepting DHS PCI or DPCI duties are accountable for tasks directed by the Organization Identity Management Official.

4. DHS HQ and Components operating a PCIF issue DHS authoritative credentials to other Components co-located in or near the same location within their operating capabilities.

5. All Enrollment and Issuance Workstations (EIWS) are DHS enterprisewide assets. DHS HQ and Components may be required to share EIWS equipment, other equipment, or supplies on an as-needed basis and within the operating capabilities of the Component. This ensures support to all DHS employees across the enterprise.

6. Prior to implementation, DHS HQ and Components align HSPD-12 planning efforts related to ICAM implementations with the DHS Organization Identity Management Official within the DHS HSPD-12 Program. This ensures ICAM products and services being implemented have been approved based on testing done by the General Services Administration's Federal Information Processing Standards 201 Evaluation Program.

7. Only one active DHS PIV Card is issued to any DHS PIV Card applicant or cardholder regardless of the DHS affiliation for which a DHS PIV Card applicant or cardholder is eligible (e.g., an individual who is both a federal employee and a contractor, etc.). The priority order of affiliation precedence is foreign national, federal employee, then contractor.

VI. Questions

Address any questions or concerns regarding this Directive to Management, OCSO, Chief Policy Advisor.

Chip Fulghum
Acting Under Secretary for Management

5/11/17
Date