ORDER

1681.1

Effective Date: 4-12-2011

SUBJECT: Department of Transportation (DOT) Implementation Policy for Identity, Credential, and Access Management (ICAM) and Homeland Security Presidential Directive – 12 (HSPD-12)

Short Title: DOT ICAM/HSPD-12 Implementation Policy

---

1. PURPOSE

This order establishes the U.S. Department of Transportation's (DOT) policy for the implementation of Identity, Credential, and Access Management (ICAM) and Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors."

This order applies to all DOT Operating Administrations and Secretarial Offices (hereinafter referred to as "DOT components").

2. CANCELLATIONS.

None.

3. REFERENCES.

3.1 Federal Information Security Management Act (FISMA) of 2002.

3.2 Privacy Act of 1974.

3.3 Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004.

3.4 Office of Management and Budget (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. (OMB M-05-24)

3.5 OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12," dated June 30, 2006 (OMB M-06-18)

3.6 OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011.

3.7 National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," dated February 25, 2005, and all subsequent editions (FIPS 201).

3.8 NIST Special Publications (SP) 800-73, 800-76, 800-78, 800-79, 800-85, 800-87, 800-96, 800-103, 800-104, and 800-116, and all subsequent editions.

3.9 Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, dated November 10, 2009, and all subsequent editions (FICAM Roadmap).

3.10 DOT order 1680.3A, "Identification Media Program," dated January 12, 2005, and all subsequent editions (DOT order 1680.3).

3.11 DOT order 1681.2, "DOT HSPD-12 PIV Card Program," currently in draft, and all subsequent editions (DOT order 1681.2).

4. BACKGROUND

The *Cyberspace Policy Review*[1], adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal PIV credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to Federal facilities and disaster response sites, as well as multi-factor authentication, digital signature, and encryption capabilities.[2] Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry[3] and facilitates interoperability.

The Federal Chief Information Officer (CIO) Council established the Identity, Credential, and Access Management Subcommittee (ICAMSC) with the charter to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. Implementing ICAM will help the Federal government to address the cybersecurity threat and provide improved physical security at federally-owned and -leased facilities, while promoting data security, privacy, and collaboration through secure information sharing and transparency in

[1] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[2] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be justified by extenuating circumstances.

[3] Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at http://csrc.nist.gov/publications/PubsSPs.html .

government. The ICAMSC developed the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, which combines HSPD-12, electronic authentication (e-Authentication) and public key infrastructure (PKI) into one holistic program and provides a common architecture and implementation guidance for use by federal agencies.

In February 2011, OMB issued Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," which outlines a plan of action for agencies that will expedite the Executive Branch's full use of the PIV credentials for access to Federal facilities and information systems and includes a requirement that Federal agencies implement the FICAM Roadmap.

5. POLICY

5.1 The DOT must implement an ICAM segment architecture that aligns with the government-wide ICAM architecture and with the Federal CIO Council's FICAM Roadmap[4]

5.1.1 The DOT must complete the implementation of HSPD-12.

5.1.2 DOT processes must accept and electronically verify PIV credentials issued by other Federal agencies.

5.1.3 DOT processes must be able to accept and electronically verify credentials issued by third party Identity Providers that have gone through the Trust Framework Provider Adoption Process.[5]

5.2 The DOT must maintain a proactive management process for this initiative to address any requirements that cannot be achieved as specified in this policy to ensure that all identified activities are completed in a timely manner.

5.3 As PIV credentials are issued to DOT Federal and contractor employees, DOT components must require the use of these credentials as the common means of authentication for access to DOT networks and information systems and to facilities[6] owned, leased or managed by that DOT component.

5.3.1 Heads of DOT components may request the DOT CIO grant a waiver of compliance for critical infrastructure[7].

---

[4] Available at https://www.idmanagement.gov/

[5] Identity Providers that have gone through the Trust Framework Provider Adoption Process are listed at: http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

[6] This order does not require the installation of physical access control systems at facilities that do not meet the facility security level requirement to do so.

[7] Critical infrastructure as described in HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection and defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)).

5.3.1.1 The request must include: (a) justification, (b) a description of the measures or compensating controls that already exist, (c) risk acceptance, (d) risk mitigation measures, (e) length of time for which the waiver is requested, and (f) milestones to achieve compliance.

5.3.1.2 If a waiver is granted, upon the next technology refreshment the Head of the component must attempt to achieve compliance and request a new waiver only if necessary.

5.3.2 The DOT components that will not be able to upgrade physical or logical access control systems to use the PIV credential, in accordance with the applicable NIST standards and the DOT ICAM segment architecture, by September 30, 2011 must register Plans of Action and Milestones (POA&M) for doing so with the DOT Office of the CIO by August 31, 2011.

5.3.3 Effective the beginning of FY2012, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.

5.3.4 Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the DOT component that owns the system using development and technology refresh funds to complete other activities.

5.4 Procurements for services and products involving facility or logical access control must be in accordance with HSPD-12 policy[8] and the Federal Acquisition Regulation[9]. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards, and supporting technical specifications.[10]

5.5 The DOT must issue PIV credentials to all DOT Federal and contractor employees who meet the criteria described in DOT Order 1680.3.

5.5.1 Where compliance with paragraph 5.5 cannot be achieved, POA&Ms must be established for doing so and registered with the DOT Office of the CIO by August 31, 2011.

5.5.2 The PIV credentials must be issued in accordance with FIPS 201 and all related NIST Special Publications.

[8] OMB M-05-24 and OMB M-06-18

[9] To the extent that any acquisition related portions of this order conflict with 49 USC §§ 106(f)(2)(D), 106(l)(6), and 40110(d), and the FAA's Acquisition Management System and Procurement Toolbox, those authorities take precedence.

[10] The General Services Administration (GSA) maintains a list of products that have been tested for conformance to FIPS 201. The list is available at https://www.idmanagement.gov/ .

5.5.3 All DOT components must adequately plan and budget for PIV credential issuance before filling any Federal positions or awarding any contracts requiring personnel to access Federal facilities or information systems.[11]

5.5.4 The PIV credentials must be issued to all current DOT employees as soon as possible, but not later than June 30, 2012.

5.5.5 The PIV credentials must be issued by June 30, 2012 to all current contractor employees who have 6 months or more remaining on their contracts, including optional contract periods that result in the contract extending more than 6 months.

5.5.6 The PIV credentials must be issued to all newly hired DOT employees and all new contractor employees as part of the on-boarding process and no later than 4 weeks after boarding, with the following exceptions:

5.5.6.1 Federal employees on-boarding with DOT for a temporary (detail) assignment and who have a PIV[12] credential issued by their employing agency must not be issued a second PIV credential, unless authorized by the Director of Security, M-40, as long as the PIV credential has been electronically verified to be in good standing (i.e. has not been revoked or expired).

5.5.6.2 Contractor employees who have been issued a PIV credential from another Federal agency must not be issued a second PIV credential, unless authorized by the Director of Security, M-40, as long as the PIV credential has been electronically verified to be in good standing (i.e. has not been revoked or expired).

5.5.6.3 Contractor employees who possess a PIV-Interoperable (PIV-I) credential from an authorized PIV-I issuer may not be issued a PIV credential, unless authorized by the Director of Security, M-40, as long as the PIV-I credential has been electronically verified to be in good standing (i.e. has not been revoked or expired).

5.6 The only DOT Components authorized to issue orders or policies related to ICAM or HSPD-12 are the DOT Office of the CIO and the Office of the Assistant Secretary for Administration.

6. RESPONSIBILITIES.

6.1 The Office of the DOT Chief Information Officer (S-80) is the office of primary responsibility for the implementation of HSPD-12 and the implementation of the ICAM segment architecture. As such, the responsibilities of the **DOT Chief Information Officer** include, but are not limited to the following:

6.1.1 Providing leadership and support necessary to ensure implementation of this order.

[11] Since all personnel are required to have and use PIV credentials, hiring authorities and contracting officials must confirm availability of funding for PIV credentials (as well as computers, telephones, etc.) before bringing any personnel on board.

[12] This includes the Common Access Card (CAC) issued by the Department of Defense.

6.1.2 Coordinating with the Assistant Secretary for Administration, the Chief Financial Officer, and Heads of DOT Components.

6.1.3 Issuing policies, guidance, procedures, and standards as necessary to ensure implementation of this order. These include, but are not limited to:

6.1.3.1 Accessing information technology resources.

6.1.3.2 Enterprise architecture.

6.1.4 Ensuring ICAM is incorporated into the DOT enterprise architecture per the FICAM Roadmap.

6.1.5 Providing a list of all physical and logical access control systems to the DOT Chief Financial Officer that identifies which systems can use PIV credentials in accordance with NIST guidelines by September 30, 2011, and annually thereafter.

6.1.6 Providing recommendations to the DOT Investment Review Board (IRB) regarding the prioritization of physical and logical access control systems for PIV-enablement and the termination of investments that are underperforming in order to support ICAM.

6.1.7 Reporting the status of the implementation of HSPD-12 and ICAM to the Office of Management and Budget, the Department of Homeland Security, and the General Services Administration, as required.

6.2 Implementing HSPD-12 and ICAM heavily involves activities delegated to the Assistant Secretary for Administration (M-1). As such, the responsibilities of the **Assistant Secretary for Administration** include, but are not limited to the following:

6.2.1 Providing leadership and support necessary to ensure implementation of this order.

6.2.2 Coordinating with the Office of the Chief Information Officer, the Chief Financial Officer, and Heads of DOT Components.

6.2.3 Issuing policies, guidance, procedures, and standards as necessary to ensure implementation of this order. These include, but are not limited to the subjects of the following:

6.2.3.1 Personnel security.

6.2.3.2 Issuing and maintaining ID credentials.

6.2.3.3 Accessing physical resources.

6.2.3.4 Human resources.

6.2.3.5 Acquisitions.

6.2.4 Ensuring PIV credentials containing the certificates required for authentication to physical and logical access control systems are issued to DOT Federal and contractor employees.

6.3 The **DOT Senior Procurement Executive** (M-60) is responsible for ensuring procurements for services and products involving facility or logical access control are in accordance with Federal HSPD-12 policy and the Federal Acquisition Regulation.

6.4 The **DOT Chief Financial Officer** (B-1) is responsible for ensuring development and technology refresh funds are used to upgrade existing physical and logical access control systems to use PIV credentials, in accordance with NIST guidelines, before they are used to complete other activities.

6.5 **Heads of DOT Components** are responsible for the following:

6.5.1 Ensuring the compliance within their components with the policies stated in this order and related DOT orders.

6.5.2 Allocating all necessary resources to support PIV card issuance and maintenance for the federal and contractor employees within their component.

6.5.3 Allocating all necessary resources to upgrade physical and logical access control systems controlled by that component to use PIV credentials, in accordance with NIST guidelines.

6.5.4 Upgrading physical and logical access control systems controlled by that component to use PIV credentials, in accordance with NIST guidelines, before using development or technology refresh funds to complete other activities.

6.5.5 Appointing an ICAM Lead within 2 weeks of the date of this order to coordinate with the Offices of the DOT CIO and the Assistant Secretary for Administration.

6.6 **Component ICAM Leads** are responsible for the following:

6.6.1 Representing the component at department-level ICAM meetings.

6.6.2 Providing status reports on the implementation progress for that component.

6.6.3 Participating in working groups or locating experts within that component who can do so, depending on the focus of the specific working group. Not all working groups will require representation from all DOT components.

6.6.4 Assisting in communications regarding ICAM within their components.

6.7 **Federal and contractor employees** are responsible for the following :

6.7.1 Applying for and completing the process of being issued a PIV credential.

6.7.2 Protecting the PIV credential issued to them.

6.7.3 Using the PIV credential to access DOT facilities, networks, and information systems.

6.7.4 Immediately reporting lost, stolen, or damaged PIV cards per DOT order 1681.2.

6.7.5 Surrendering the PIV card issued to them upon separation from DOT for any reason, per DOT order 1681.2.

Ray LaHood
Secretary of Transportation