



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, DC 20240

**MAR 31 2011**

## Memorandum

To: Solicitor  
Inspector General  
Assistant Secretaries  
Heads of Bureaus and Offices

From: Rhea Suh, Assistant Secretary *Ch L to*  
Policy, Management and Budget

Bernard Mazer *[Signature]*  
Chief Information Officer

Subject: Policy for the Issuance, Management and Use of Federal Personal Identity  
Verification (PIV) Cards (DOI Access Cards)

This Memorandum prescribes the policy necessary to expedite full deployment and use of PIV credentials (DOI Access Cards) as the common means of authentication for access to facilities, networks, and information systems within the Department of the Interior. This implementation policy sustains Homeland Security Presidential Directive 12 (HSPD-12), a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy

This policy is issued in accordance with the authorities contained in HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, issued August 27, 2004; National Institute of Standards and Technology (NIST) Federal Information Processing Standard 201-1 (FIPS 201-1), Personal Identity Verification of Federal Employees and Contractors, dated March 6, 2006; NIST Special Publication 800-63; 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 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; 43 U.S.C. § 1453a.

The HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) credentials including a standardized background investigation to verify employees' and contractor's identities. The Cyberspace Policy Review, 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. DOI complied with HSPD-12 by issuing the "Personal Identity Verification (PIV) Policy and Guide for Federal Employees and Contractors", dated December 2005; the DOI HSPD-12 Charter, dated October 12, 2006, which established the DOI Executive Steering Committee (ESC) and Program Management Office (PMO) authorities and governance structure; and the Personnel Bulletin 09-06, dated June 1, 2009, policy for Issuance and Management of DOI Access Cards. DOI Acquisition Policy Release (DIAPR) 2010-04, outlines the responsibilities of the Head of the Contracting Activity, Procurement Chiefs, Contracting Officers and Contractor Officers Technical Representatives to implement the DOI Access Program in DOI contracts.

As of February 2011, DOI had issued 56,682 of 75,769 (roughly 75%) DOI Access Cards to federal employees and contractors and will deploy 500 Activation Stations to remote duty locations to activate the remaining 25%. Given that the majority of the DOI workforce has now received DOI Access Cards, DOI can aggressively step up efforts to expedite the full use of the electronic capabilities of the card. Specific benefits include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.

**Policy.** The following is effective immediately:

1. The Federal Personal Identity Verification smartcard (DOI Access Card) is the only recognized PIV credential for DOI employees and contractors and replaces all existing DOI Bureau/Office issued identity cards except for certain Law Enforcement credentials, temporary access badges, and visitor badges.
  - a. DOI Access Cards will be issued to:
    - (1) **Employees, as defined in Title 5 U.S.C. 2105.** This includes short-term employees (i.e., those serving fewer than 180 consecutive calendar days), personnel on detail assignment and others temporarily assigned to DOI, and affiliates such as, but not limited to, guest researchers, volunteers, tribal users, and intermittent, and temporary or seasonal employees who require physical or logical access to DOI facilities or information systems in accordance with HSPD-12 and NIST guidelines.
    - (2) **Contractors requiring logical access in accordance with current Office of the Chief Information Office (OCIO) logical access use policies, or routine physical access for more than 180 days in accordance with current Office of Law Enforcement and Security (OLES) physical access policies.**
  - b. DOI Access Cards are not required for:
    - (1) **Contractors and others requiring routine physical access for less than 180 days, or intermittent physical access.** These individuals will be issued a temporary access badge (TAB) in accordance with current Office of Law Enforcement and Security (OLES) guidance.

(2) **Occasional visitors requiring physical access.** These individuals will be issued a visitor badge in accordance with current OLES guidance.

2. All DOI bureaus/offices will initiate requests for network access and DOI Access Cards through the DOI Access System, which integrates access requests across Human Resources, Personnel Security and Information Technology work streams.
3. All new systems under development must be enabled to use the DOI Access Card to authenticate identity for logical access, including the combination of the DOI Access Card with other software solutions such as Active Directory, in accordance with NIST guidelines, prior to being made operational.
4. The beginning of FY2012 and in accordance with HSPD-12 and NIST guidelines, existing physical and logical access control systems must be upgraded to use DOI Access Cards prior to the agency using development and technology refresh funds to complete other activities.
5. Procurements for services and products involving facility or system access control must be in accordance with all applicable HSPD-12 policy and the Federal Acquisition Regulation, including OMB M-06-18, Acquisition of Products and Services for Implementation of HSPD-12.
6. DOI will initiate work to integrate its existing DOI Access Program into a complete identity, credential and access management architecture as prescribed in the Federal CIO Council's "Federal Identity, Credential and Access Management Roadmap and Implementation Guidance."

**Implementation.** To implement this policy, DOI bureaus/offices will continue to comply with Personnel Bulletin 09-06 and DOI Acquisition Policy Release (DIAPR) 2010-04. In addition, DOI will take the following actions to expedite full use of DOI Access Cards as the common means of authentication for access to facilities, networks and information systems:

1. Within 30 days of the issuance of this memorandum, DOI will establish an Identity, Credential, and Access Management (ICAM) Program Management Office (PMO) to manage all aspects of the ICAM Program through the planning, implementation and operational phases under the direction of the DOI Chief Information Officer (CIO), with the DOI Access Executive Steering Committee providing guidance to the CIO.
2. Within 30 days of issuance of this memorandum, bureaus/offices will identify subject matter experts in Physical Access and Logical Access to work with the ICAM PMO to complete and facilitate execution of the ICAM Transition Plan.

3. Within 120 days of issuance of this memorandum, the ICAM PMO and subject matter experts shall develop an ICAM compliant plan for logical access that fully integrates existing DOI Access components and will develop an ICAM Transition Plan in accordance with the Federal ICAM Framework, to enhance performance measurement and accountability within ICAM initiatives which will include:
  - a. A plan for accepting and electronically verifying PIV credentials issued by other federal agencies.
  - b. A process for streamlined collection and sharing of digital identity data.
  - c. An approach that fully leverages PIV and PIV-interoperable credentials.
  - d. A strategy to modernize the Physical Access Control infrastructure.
  - e. An approach to modernize the Logical Access Control infrastructure and to implement Logical Access Control as required to enable PIV smartcard use, according to NIST guidelines.
  - f. Guidance that facilitates implementation of a Federated identity capability.

**Point of Contact.** The point of contact for this policy is Mr. Bernard Mazer, Chief Information Officer at 202 208-6194 or Ms. Judith Snoich, HSPD12 Program Manager, at 202-219-0867 or email [Judith\\_Snoich@ios.doi.gov](mailto:Judith_Snoich@ios.doi.gov) .