United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

PERSONNEL BULLETIN NO. 09-06

SUBJECT: Policy for the Issuance and Management of DOI Access Cards

1. Purpose

a. This Personnel Bulletin prescribes the policies, roles, and responsibilities necessary to issue and manage the Department of the Interior (DOI) personal identity verification (PIV) credentials, DOI Access Cards, to comply with Homeland Security Presidential Directive 12 (HSPD-12).

b. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, issued August 27, 2004, mandates the use of secure and reliable forms of identification for Federal employees and contractors for authenticating to/accessing federally controlled facilities (physical access) and federally controlled information systems (logical access).

c. The National Institute of Standards and Technology (NIST) promulgated Federal Information Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors on February 25, 2005. FIPS 201 and associated NIST publications establish standards and requirements for the personal identity verification of federal employees and contractors and for PIV credentials to be issued. FIPS 201 was updated to FIPS 201-1 on March 6, 2006.

2. Authorities

a. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004.

b. NIST Federal Information Processing Standard 201-1 (FIPS 201-1), Personal Identity Verification of Federal Employees and Contractors, dated March 6, 2006.

c. 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.

d. DOI HSPD-12 Charter dated October 12, 2006, established the DOI Executive Steering Committee (ESC) and Program Management Office (PMO) authorities and governance structure.

e. DOI Acquisition Policy Release (DIAPR) 2006-03, requires all contracts to include language requiring background investigations for contractors.

3. Policy

a. Effective immediately, bureaus/offices must implement the FIPS 201-1 standard process for personal identity verification and PIV credential (DOI Access Card) issuance for DOI employees and contractors as outlined in Section 5 below. The DOI Access Card is the only authorized PIV credential for these individuals and replaces all existing DOI Bureau/Office issued identity cards. This policy does not apply to the issuance and management of Law Enforcement, Security or Emergency Management credentials.

DOI uses the GSA Managed Services Office (MSO) Shared Services solution (USAccess) to provide the accredited FIPS 201-1 system for PIV and DOI Access Card issuance and management. Standard procedures to execute this process are outlined in the GSA USAccess PIV Card Issuer (PCI) Operations Plan and the DOI Access PCI Operations Plan.

b. This policy applies to:

(1) **Employees, as defined in Title 5 U.S.C. 2105.** This includes other DOI specific categories of employees (e.g., short-term (i.e., less than 180 calendar days), detailed or assigned to DOI); and all other affiliates such as, but not limited to, guest researchers; volunteers: tribal users; or intermittent, temporary or seasonal employees) that require logical access.

(2) **Contractors requiring routine physical access or logical access in accordance with current Office of the Chief Information Office (OCIO) logical access use policies.**

c. This policy does not apply to:

(1) **Contractors and others requiring 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.

4. DOI Access Card Issuance and Management

a. DOI Access Card issuance will follow the schedule outlined in the current OMB approved DOI Access Implementation Plan and in accordance with the DOI Access PCI Operations Plan.

b. DOI Access Cards will be managed (e.g., reissuance, renewal, replacement of lost cards, transfers from bureau to bureau) in accordance with the DOI Access PCI Operations Plan.

5. Roles, Responsibilities, and Requirements

a. **Departmental DOI Access Executive Steering Committee (ESC) will:**

(1) Assign the following program executives to provide cooperation, collaboration and consensus-driven direction, and oversight to achieve compliance with HSPD-12:

- Deputy Assistant Secretary for Human Capital, Performance, and Partnerships (HCPP)
- Deputy Assistant Secretary, Law Enforcement, Security and Emergency Management (LESEM)
- Deputy Assistant Secretary, Budget and Business Management (BBM)
- Department Chief Information Officer (CIO).

(2) Manage the scope of the DOI Access Program by approving changes in scope, resources or schedule with a formal vote, and provide strategic input on future program requirements, as outlined in the DOI Access Program Charter.

(3) Provide direction and oversight to complete integration of the DOI Access Card with Department-wide Logical Access Control Systems (LACS) and Physical Access Control Systems (PACS) to establish a Department-wide identity management solution.

(4) Designate a DOI Access Program Manager to:

- Manage all aspects of the DOI Access Program through the planning, implementation and operational stages of the program, under the direction of the DOI Access ESC.
- Prepare and submit a quarterly report on the number of PIV credentials issued to employees and contractors as required by OMB.
- Develop the DOI HSPD-12 Implementation Plan required by OMB.
- Develop the DOI Access PCI Operations Plan required by FIPS 201-1.
- Lead the DOI Access Integrated Project Team (IPT), which includes the DOI Access System Project Manager, PACS Project Manager, and LACS Project Manager to identify and resolve integration issues.
- Lead the DOI Access Implementation Team (I-Team) comprised of Bureau and Office DOI Access Leads to issue DOI Access Cards.

(5) Designate a PACS Project Manager to:

- Participate in the DOI Access IPT.
- Recommend an enterprise PACS (ePACS) solution and implementation schedule for ESC approval.
- Implement approved ePACS solution in accordance with NIST SP 800-116 and LESEM policy.
- Establish and lead the ePACS Implementation Team with bureaus/offices
- Report status of the ePACS Implemenation Plan to DOI Access Program Manager to support OMB reporting.

(6) Designate a LACS Project Manager to:

- Participate in the DOI Access IPT.
- Recommend a LACS solution and implementation schedule for ESC approval.
- Implement approved LACS solution in accordance with OCIO policy.
- Establish and lead the LACS Implementation Team with Bureaus/offices.
- Report status of the LACS Implementation Plan to the DOI Access Program Manager to support OMB reporting.

b. **Deputy Assistant Secretary for Human Capital, Performance, and Partnerships will:**

(1) Establish policies and procedures in consultation with the CIO and LESEM for implementing and administering the DOI Access Program in compliance with FIPS 201-1 and DOI Security and Privacy policies throughout the department to:

- Ensure minimum background investigations, National Agency Check with Inquiries (NACI), have been initiated and successfully adjudicated for each employee.
- Ensure Federal Personnel and Payroll System (FPPS) data required by DOI Access are current, accurate, and available.
- Ensure Emergency Response Official (ERO) designation is included in position descriptions and recorded in FPPS.

c. **Deputy Assistant Secretary, Law Enforcement, Security, and Emergency Management (LESEM) will:**

(1) Establish policies and procedures in consultation with the HCPP and CIO for implementing and administering the DOI Access Program in compliance with FIPS 201-1 throughout the department to:

- Require designation of Bureau/Office ERO Managing Officials responsible for approving and maintaining ERO designation assignments.
- Identify the minimum background investigation required for non-U.S. citizens and contract employees.
- Require use of DOI Access Cards in Physical Access Control Systems (PACS) as outlined in the Interagency Security Committee Standard, Facility Security Level Determinations for Federal Facilities.

d. **Chief Information Officer (CIO) will:**

(1) Establish policies and procedures in consultation with HCPP and LESEM for implementing and administering the DOI Access Program in compliance with FIPS 201-1 throughout DOI to:

- Implement the use of DOI Access cards for logical access control.
- Ensure Active Directory (AD) and e-mail system data required by DOI Access are current, accurate, and available.
- Support deployment and operation of USAccess enrollment and activation stations on DOI networks.

(2) Assign a DOI Access System Project Manager to develop the DOI Access identity management system in accordance with requirements from the DOI Access PMO. Maintain the DOI Access System as the system of record for DOI identity credential information submitted to USAccess.

(3) Assign a Privacy Officer to ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a) and all OMB and FISMA requirements.

(4) Assist the ePACS Project Manager with implementing and maintaining the ePACS infrastructure and connectivity.

e. **Deputy Assistant Secretary, Budget and Business Management will:**

(1) Establish policies and procedures in consultation with HCPP, CIO, and LESEM for implementing and administering the DOI Access Program in compliance with FIPS 201-1 and DOI Security and Privacy policies throughout DOI to:

- Manage the DOI Access Program budget.
- Review and distribute procurement and contracting guidance related to the DOI Access Program to Bureaus/offices.
- Verify compliance with Acquisition regulations.

(2) Assign all Contracting Officer Representatives (CORs) to:

- Maintain current data required to issue and manage DOI Access Cards for contractors in the DOI Access system.
- Request the initiation and adjudication of contract employee background checks (NACI), in accordance with the DIAPR 2006-03.
- Maintain signed confidentiality agreements for all contractors.

f. **Departmental Bureaus/Offices will:**

(1) Assign the DOI Access Executive (SES level) responsible for the successful implementation and management of bureau/office DOI Access program, complying with program goals outlined in the current OMB-approved DOI Access Implementation Plan and procedures defined in the DOI Access PCI Operations Plan.

(2) Assign resources to fund, administer, implement and maintain the DOI Access Program:

- Designate and certify DOI Access role holders, and maintain records for audit purposes
- Complete DOI Access Card issuance for existing employees and contractors
- Issue DOI Access Cards during on-boarding for new employees and contractors
- Perform DOI Access Card Management, which includes updating USAccess identity accounts to complete bureau to bureau transfers, card reissuance, card reprinting, and card or certificate renewal; maintaining a chain of custody for all cards until activation; and the collection and destruction of DOI Access Cards upon termination of employment or suspension) in accordance with the DOI PCI Operations Plan.

(3) Maintain a current list of Emergency Response Officials by name and position, to ensure DOI Access Cards are issued with the "Emergency Response Official" red stripe designation, in accordance with LESEM guidance.

(4) Host and operate mobile and fixed USAccess Enrollment and Activation Stations

(5) Align bureau/office PACS and LACS with DOI enterprise PACS and LACS solutions, and comply with DOI physical and logical access control policies and procedures.

(6) Maintain records that will permit the audit of bureau/office PIV programs in accordance with HSPD-12, FIPS 201-1, relevant OMB guidance and any OIG requirements.

g. **DOI Access Card Holders will:**

(1) Create and maintain a 6-8 digit numeric Personal Identification Number (PIN) required for the DOI Access Card

(2) Secure the DOI Access card in a FIPS 201 approved shielded badge holder (Electromagnetically Opaque Sleeve), listed on the FIPS 201 Evaluation Program website: http://fips201ep.cio.gov/apl.php.

(3) Immediately report a lost or stolen card in accordance with their Bureau's card management procedures.

(4) Surrender their DOI Access Card and badge holder upon termination of employment, contract, or other affiliation with DOI.

6. Cancellations/Special Instructions

a. Existing DOI and bureau/office issued identification cards will be obsolete upon issuance of the DOI Access Card.

b. This Personnel Bulletin replaces the Office of Law Enforcement and Security memorandum, Definition of Card Issuance and Facility Guidance, dated July 14, 2005.

c. The 2002 Federal Information Security Management Act (FISMA) does not permit waivers to the FIPS 201-1 standards.

7. Personnel Bulletin Contact

The Departmental point of contact for this policy is Judith Snoich at 202-219-0867 or email Judith_Snoich@ios.doi.gov .

PERSONNEL BULLETIN NO. 09-06

SUBJECT: Policy for the Issuance and Management of DOI Access Cards

Kathleen J.H. Wheeler

Kathleen J.H. Wheeler
Acting Deputy Assistant Secretary
Human Capital, Performance and Partnerships

May 26, 2009
Date

Larry R. Parkinson

Larry Parkinson
Deputy Assistant Secretary
Law Enforcement, Security and Emergency Management

5-29-09
Date

Pamela Haze

Pamela K. Haze
Deputy Assistant Secretary
Budget and Business Management

6-1-09
Date

Sanjeev (Sonny) Bhagowalia
Chief Information Officer

6.1.09
Date

Appendix A. Definitions

Access control. The process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also "logical access control system" and "physical access control system."

Contractor. An individual under contract to perform work for or provide services to DOI.

Credential. Data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

DOI Access Card (PIV Credential). An identity card issued to an individual that contains stored credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person or by an automated process.

Federal Facility or Information System Access. Authorization granted to an individual to physically enter federally controlled facilities, and/or electronically (logically) access federally controlled information systems for approved purposes.

Logical Access Control System (LACS). Protection mechanisms that limit a user's access to information and restrict their forms of access on the system to only what is appropriate for them. These systems may be built in to an operating system, network or application.

National Agency Check with Inquiries (NACI). The basic and minimum background investigation required of all new Federal employees and contractors by FIPS 201-1 consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the FBI Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS). Protection mechanisms that limit users' access to physical facilities or areas to only what is appropriate for them. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

Personal Identity Verification (PIV) The process of providing sufficient information to verify legal name (e.g., driver's license, legal documents, proof of current address) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other.

PIV Credential. See DOI Access Card

Routine access. A person that is accessing the facility without an escort and/or continuous monitoring by a DOI official. The agency's determination should be based upon the support to successfully complete DOI's mission critical functions/missions. This type of access requires issuance of a DOI-Access Card.

Shielded Card Holder. A FIPS 201-1 Approved Product List (APL) electromagnetically opaque sleeve to protect against any unauthorized contactless access to information stored on a DOI-Access Card.

Appendix B. References

Computer Security Act of 1987 (Public Law 100-235).

DOI Access PCI Operations Plan (in progress).

DOI Departmental Manual Series Administrative Services, Part 310 General, Chapter 3: Identification Cards. February 2, 2009.

DOI Departmental Manual Series Law Enforcement and Security, Part 441 Personnel Security and Suitability Requirements.

DOI HSPD-12 Implementation Plan, submitted to OMB on November 17, 2008.

DOI Memorandum Mandatory Use of the Electronic Questionnaires for Investigations Processing System and Clearance Verification System, Oct 23. 2008

DOI Memorandum Guidance – Requirements for the U.S. Department of the Interior Personal Identity Verification Card (Smart Card) Visual Card Topography, April 18, 2007.

DOI Memorandum HSPD-12 Temporary Physical Access Badge Guidance, August 3. 2006.

DOI Memorandum HSPD-12 Non-U.S. Citizen Background Investigation Guidance, April 18. 2007.

DOI Memorandum Updated HSPD-12 Emergency Response Official Guidance, October 21, 2008.

Executive Order (EO) 12968, Access to Classified Information, August 1995.

Form I-9 (Rev. 10/4/00) – Department of Justice (OMB No. 1115-0136).

Interagency Security Committee Facility Security Level Determinations for Federal Facilities Standard, February 21, 2008.

CIO 2006-015 Controlled Logical Access Policy, June 1, 2006.

CIO Directive 2004-08.

OLES Guidance 5/25/05-Requirements for the DOI Personal Identity Verification Card (Smart Card) Visual Card Topography.

OLES Guidance 5/25/05-Installation of Smart Card Readers at DOI Facilities.

OMB Memorandum, Acquisition of Products and Services for Implementation of HSPD-12, M-06-18, June 30, 2006.

OMB Memorandum for CIOs – Guidance for HSPD-12 Implementation dated May, 23, 2008.

OMB Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials. M-07-06. January 11, 2007.

Privacy Act. 1974 (5USC 552a) and Electronic Privacy Act, 1986 (USC 2701).

USAccess Program PIV Credential Issuer Operations Plan, Version 2.1, GSA. February 17, 2009.

U.S. Department of Commerce, National Institute of Standards and Technology. Special Publications (SP):

(1) 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004

(2) 800-53, Recommended Security Controls for Federal Information Systems, September 2004 (2PD).

(3) 800-63, Electronic Authentication Guideline, Appendix A, June 2004.

(4) 800-73-1, Interfaces with Personal Identity Verification, April 2006.

(5) 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007.

(6) 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, July 2006.

(7) 800-85A, PIV Card Application and Middleware Interface Test Guidelines, April 2006.

(8) 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations, December 2006.

(9) 800-104, A Scheme for PIV Visual Card Topology, January 2007.

(10) 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), November 2008.