

# Homeland Security Presidential Directive 12

---

## Policy for a Common Identification Standard for Federal Employees and Contractors

Thomas J. Schlagel

Presented at the 2005 RHIC/AGS Annual User's Meeting  
Open Forum

June 23, 2005

# HSPD-12

---

- Homeland Security Presidential Directive 12 (HSPD-12) was issued by the White House on August 27, 2004. Motivated by the need to secure access to Federal and other facilities where there is potential for terrorist attacks, HSPD-12 requires the development and deployment of a common and reliable ID system for Federal employees and contractors that is interoperable across government agencies.
- Requires secure and reliable forms of personal identification:
  - Based on sound criteria to verify an individual employee's identity
  - Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
  - Rapid electronic verification of personal identity
  - Identity tokens issued only by providers whose reliability has been established by an official accreditation process
- HSPD-12 Information <http://csrc.nist.gov/piv-project>

# HSPD-12 Applicability

---

According to draft OMB guidance, HSPD-12 applies to:

- Executive departments and agencies (including DOE)
- Federal employees and contractors (both foreign and domestic). Applicability to others (e.g. guest researchers) is an agency decision. (Does not apply to short term guests and occasional visitors.)
- Federally owned buildings or leased space
- Information technology systems. Applicability for remote access is an agency decision

# FIPS 201

## Personal Identity Verification (PIV)

---

- NIST Computer Security Division was tasked with developing standards, guidelines, recommendations, and/or technical specifications. Federal Information Processing Standard (FIPS) 201 *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.
- FIPS 201 defines the standards to:
  - properly protect the personal privacy of all subscribers of the PIV system;
  - authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card";
  - electronically obtain and store appropriate biometric data (e.g., fingerprints, facial images) from the PIV system subscriber;
  - create a PIV "card" that is "personalized" with data needed to grant access to the subscriber to Federal facilities and information systems;
  - assure appropriate levels of security for applications; and
  - provide interoperability among Federal organizations

# Personal Identity Proofing Requirement (FIPS 201)

---

- Applicant must present two government-issued identity documents. One must be a photo ID.
- Applicant must pass a background investigation process equivalent to at least OPM Form 85.
- Full fingerprinting of the applicant is a part of the background investigation process.

# Implementation Timelines

---

- Agencies submit implementation plan to OMB
  - Completion: **June 27, 2005**
- Comply with FIPS 201 Part 1 (Policies and Procedures)
  - Common Identification, Security and Privacy Requirements
    - Minimum requirements for identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance process
  - Completion: **October 27, 2005.**
- Comply with FIPS 201 Part 2 (Technical Interoperability)
  - Government-wide uniformity and interoperability
    - Detailed specifications for technical interoperability among departments and agencies required to implement PIV card system
    - New employees and contractors must be using the new system
  - Completion: **October 27, 2006.**
  - By **September 30, 2007**, identity proofing should be on record for all current employees and contractors

# DOE Implementation of HSPD-12

---

- DOE Project Team staffed by Office of Chief Information Officer, Office of Security and Safety Performance will manage implementation. Effort led by Bruce Brody, Associate CIO for Cyber Security.
- Project Team staffed by Program Offices – representatives from the Laboratories highly encouraged
- Project Team will have primary responsibility for engineering, design, procurement, coordination, deployment and support of common solution for all DOE elements (including M&O contractors)
- Project Team issued data call to gather data on current environment – due May 9.

# Some Issues

---

- This is a unfunded mandate. Costs across the DOE complex are expected to run in to \$100's M
  - Background checks and replacement ID's on all existing employees/guests
  - Ongoing costs for background checks and ID cards for new employees/guests.
  - Badge scanners for buildings and individual computers will be required. Will have to upgrade systems and modify applications to handle the cards
- Broad implementation of the directive could have adverse effects to the Science mission which is a low risk area. Graded implementation approach needs to be taken
- Background checks will cause a delay in bringing in employees/guests if directive applies to them
- Not clear how foreign nationals and remote users will be handled
- No process for handling negative results of background checks
- Potential loss of users and employees because of perceived invasion of privacy issues

# Current status

---

- BNL established working group on PIV: representatives from IT, Safeguards and Securities, CI, HR and S&T
- SLCCC (SC lab CIO's) having regular discussions on PIV and impact to science labs
  - SLCCC drafted briefing for Laboratory Directors meeting
  - SLCCC has submitted comments to NIST on FIPS 201 and DOE OCIO on potential negative impacts with implementation.
- RHIC/AGS UEC submitted memo to DOE OCIO on potential negative impacts of PIV for access to facilities.
- Waiting to see the DOE PIV Implementation Plan due to OMB on June 27.