



HSPD-12 Update

Security Awareness
SIG Conference

Ceil Rogers
Office of Personnel Security
April 18, 2007



HSPD–12 Refresher



- On August 27, 2004, a Homeland Security Presidential Directive was issued entitled HSPD–12, “Policy for a Common Identification Standard for Federal Employees and Contractors.”
- In response to HSPD–12, the National Institute of Standards and Technology (NIST) published the Federal Information Processing Standards Publication 201 (FIPS 201) on February 25, 2005. This Standard has had one revision, so FIPS 201–1 is the current Standard. NIST is considering a new more comprehensive revision in the near future.



Covered Population



- October 13, 2005, Clay Sell memo
 - All DOE Federal employees
 - All L- or Q-cleared contractors
 - All uncleared contractors servicing DOE HQ
 - Program offices may opt in additional uncleared contractors at their discretion
- Excluded (per DOE N 206.3)
 - Navy Nucs
 - Contractors working 6 months or less



Shared Service Provider Implementation



- General Services Administration (GSA) formed a Managed Service Office (MSO) to be an HSPD-12 Shared Service Provider
- Awarded contract to meet October '06 deadline
 - Did not exercise option for full scale deployment
- Issued new RFP
- Award of new contract scheduled for mid-April
- Deployment scheduled to begin in Washington in mid-June



(Preliminary)

SSP Responsibilities



- Enrollment services
- SSP enrollment locations
- C&A of enrollment stations
- Card printing
- Card management infrastructure
- Identity management infrastructure
- PKI infrastructure



(Preliminary)

DOE Responsibilities



- DOE site security
- Operation of enrollment stations at DOE facilities
- Candidate sponsorship
- Background investigations (BI)
- Adjudication of BI
- Badge issuance and most activations
- Internet access for system
- C&A of system connections
- Access authorization
- Physical/logical card readers
- Integration w/ existing physical and logical access control systems



Implementation Timeline



- October 27, 2005
 - Compliance w/ FIPS 201–1, Pt 1
- October 27, 2006
 - Issued first DOE smart cards
 - “Interim Compliance w/ FIPS 201–1, Pt 2”
- October 27, 2007
 - Verify and/or complete BIs on current workers
- October 27, 2008
 - Verify and/or complete BIs on Federal employees w/ > 15 years service



Implementation Timeline (cont.)



- April 2007
 - New PIV-II SSP contract to be awarded
- July 2007
 - PIV-II Badge issuance expected to begin in earnest
- October 2008 and beyond
 - DOE Federal and contractor employees begin to use smartcard for routine access to buildings and computer systems
 - Interoperability with other Federal agencies to improve and expand



Why PIV-I?



- Mandated by HSPD-12 and FIPS 201–1
- A Federal identity proofing standard provides the basis for trust among agencies
- DOE will know that a person from another agency with a PIV Card has had—
 - fingerprints checked by the FBI
 - a successfully adjudicated BI (NACI or higher)
 - identity source documents verified



Personal Identity Verification



- Identity Proofing
 - Credentials/documents (I–9s)
 - Identity history (BI)

 - ??To establish an identity
 - ??Suitability



I-9 Documents



- OMB Form I-9, Employment Eligibility Verification
 - Documents that establish identity
 - Drivers license; Federal, State, or local ID card, school ID, military card, Native American tribal document, etc.
 - Documents that establish employment eligibility
 - Social security card, birth certificate, certif of birth abroad (issued by Dept of State), Native American tribal document, etc.
 - Documents that establish both
 - Passport, certif of US citizenship, certif of naturalization, unexpired foreign passport + unexpired employment auth., permanent resident card, unexpired temporary resident card, etc.
- <http://www.uscis.gov/files/form/i-9.pdf>



Background Investigations



- NACI
- Any BI used to grant a clearance
- Reciprocity



PIV Reciprocity



- A PIV badge can be issued under reciprocity if an individual has had a prior, favorably adjudicated Federal agency BI
- Documentation of the results of the BI must be kept in the PIV file
- Reciprocity verification, if possible, reduces wait time



FBI Fingerprint Check



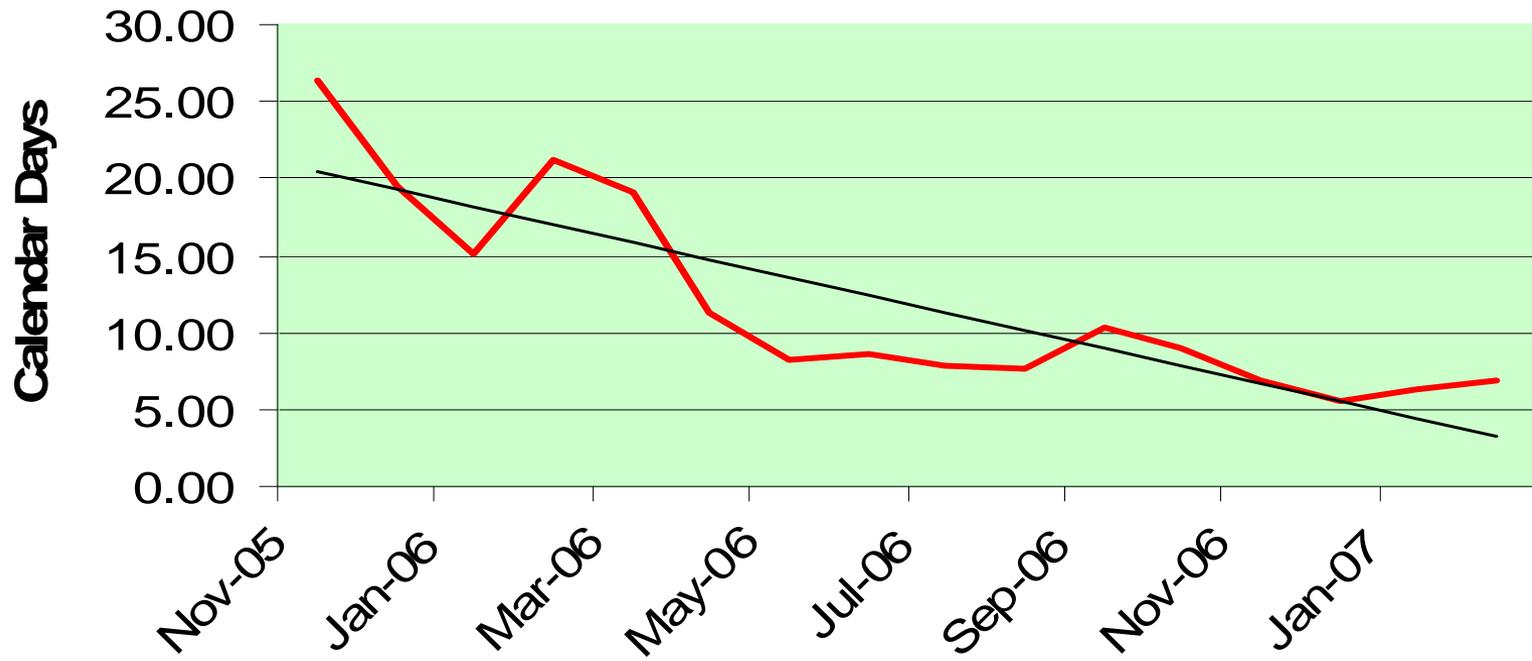
- PIV credentials can be issued after fingerprint check results have been returned and favorably adjudicated
- Fingerprints are submitted to OPM, which forwards them to the FBI
- Average turnaround time (since May 2006) is < 8 calendar days for HQ
- **Electronic submission of fingerprints and electronic reports have reduced turnaround time**



FBI Fingerprint Check



Fingerprint Turnaround Time





Incumbent Workers



- OMB Implementation Memo 05–24
 - “verify and/or complete background investigations for all current employees and contractors” by October 27, 2007
 - Federal employees with > 15 years of service have until October 27, 2008
 - For uncleared Feds, look for proof of “suitability” NACI in OPF



Other Aspects of HSPD-12



- PIV-II (“smart”) Cards
- Logical Credentials
- Policy Developments
- PMO



PIV-II Card Physical Attributes



- **Physical PIV-II Smart Card**
 - Common 'look and feel' across Federal government
 - Areas set aside for agency specific information
 - Common color coding scheme for employee affiliation
 - Blue- foreign nationals
 - Red – emergency responder officials
 - Green – contractors
- Must meet ANSI and ISO standards for physical durability
- Tamper resistant security features (e.g., optical varying structures)
- Magnetic stripe to be provided for legacy support
- A bar code may be provided (additional cost) for legacy support
- Contact and contactless interface provided

Ray Holmer



PIV-II Logical Credentials



- CHUID (Card Holder Unique Identifier)
 - Designed for Federal interoperability
 - Read through contact or contactless interface
 - Contains the element, Federal Agency Smart Card Number (FASC-N), which uniquely identifies each card.
- PIV Authentication Certificate (and associated public/private keys)
 - PKI certificate issued from Federally certified PKI provider
 - Read through contact interface
- PIN
 - Personal Identification Number to unlock the PIV Card
- Biometrics
 - Electronic template generated from fingerprint minutiae (on card)
 - Read through contact interface only after PIN unlock

Paul Aaron



Policy Developments



- DOE N 206.3, Personal Identity Verification, revised to 206.4
 - Grants authority to obtain additional information in the adjudication process
 - New policy to recognize PIV–II and the GSA SSP is being developed
- HQ is using a standard PIV request form 
 - Field use of this form is optional
- Privacy Act System of Records Notice has been published
 - SOR should be final by the time of this briefing



HSPD-12 Pgm Mgmt Office (PMO)



- Operating for more than 2 years
- Co-chaired by the CIO & HSS
- Supported by
 - Office of Management
 - Office of General Council
 - Office of Human Resources
 - NNSA
 - FOIA
 - EM
- Stakeholder field calls held by PMO as information and program developments warrant
- Public Web site
<http://www.hss.energy.gov/HSPD12/index.html>
 - An updated FAQs is to be posted soon
- Contact the PMO at HSPD12PMO@hq.doe.gov

Fred Catoe
Tim Gaines



HSPD-12



Questions?



Resources



- DOE HSPD-12 webpage
<http://www.hss.energy.gov/HSPD12/index.html>
- DOE N 206.4, “Personal Identity Verification”
 - Expect to be posted very soon
- Ask HSPD12PMO@hq.doe.gov about Stakeholders teleconference meetings
- Ask Raymond.Holmer@hq.doe.gov about the Physical Security Working Group
- Ask Cecellia.Rogers@hq.doe.gov about DOE Registrars teleconference meetings