

HSPD-12 FAQs – October 1, 2009

GENERAL

1. What is HSPD-12?

[HSPD 12](#) is a presidential directive requiring all Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.

2. Does HSPD-12 apply to all agencies including the smaller agencies (e.g. micro-agencies)?

For the most part, yes. The Directive applies to all "Executive departments" and agencies listed in title 5 U.S.C. § 101, and the Department of Homeland Security; "independent establishments" as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201). The exceptions are as follows: "Government corporations" as defined by title 5 U.S.C. § 103(1) are encouraged, but not required to implement this Directive. (Ref: OMB M-05-024 Section 1.A.)

3. What is FIPS 201?

[FIPS 201](#) is the Standard identified in HSPD-12 that sets out the requirements for a Federal government-wide identity credential for employees and contractors.

4. Why is the standard divided into 2 parts?

The standard is divided into two parts so agencies can make an orderly migration-in terms of both technology and "identity proofing" from their current systems to the requirements established by the standard and meet the deadlines established by the President in HSPD 12. Part 1 deals with the security objectives as they apply to uniform personnel identity proofing and vetting activities, while Part 2 focuses on the technical interoperability requirements, including the issuance of compliant identity badges and the implementation of the government-wide infrastructure to support the effective use of the badges.

5. What are the primary requirements for an agency to implement FIPS 201?

Revise the identity proofing and identity card issuance process of the agency to meet FIPS-201 requirements and implement access control mechanisms for facilities and IT systems that utilize the capabilities of the compliant identity credential. Establish control measures that mandate privacy protections with information assurance that is auditable. FIPS 201 requirements include the issuance of an identity badge that utilizes smart card technology, both contact and contactless, and incorporates a standardized Card Holder Unique Identifier (CHUID), digital credentials, and biometric templates.

6. Can federal agencies use the standard for other purposes beyond the scope of the standard to include national security applications?

Yes. The Directive specifically tasks agencies to identify additional applications important to security for which the standard might be employed. Such wider use must conform to Office of Management and Budget (OMB) policy (including the relevant privacy provisions) and, if national security systems are involved, the applicable requirements to protect national security information and systems.

7. What will the card look like?

Card topology is described and pictured in the Standard. Each card will contain a required set of information: a printed picture of the cardholder, name, expiration date, and agency affiliation. Additional optional information (e.g., signature, agency seal, issue date, etc.) may be selected by each agency within the parameters set by the Standard and further refined by OMB, where applicable.

8. Which agencies are responsible for government-wide activities associated with implementing the directive?

Four federal agencies have specific responsibilities for implementing this directive: Department of Commerce (DOC) for development of the Standard, OMB for oversight of agency implementation and development of policy, General Services Administration (GSA) for acquisition assistance, FBI for National Criminal History (Fingerprint) checks, and Office of Personnel Management (OPM) for assisting agencies with required background investigations.

9. What implementation solution is recommended for agencies?

Both large and small agencies will benefit from the government-wide strategy. Interested agencies should make their interest in a shared solution known to the GSA Managed Service Office. Once a decision has been made to participate, agencies will need to sign an MOU with GSA, as appropriate, and prepare to transfer funds.

10. What does "logical access" mean in FIPS 201?

Logical access, as used in FIPS 201, refers to use of the credential as part of identification and authentication processes that are used by automated information systems access-control processes (e.g., log on actions and digital signatures).

11. How can agencies assess their existing infrastructure to tell if they are FIPS 201 compliant? Do you have any specific publication (like 800-53)?

FIPS 201 is the governing Standard for HSPD-12 compliance. FIPS 201 contains normative references to additional documents. Enrollment and Card Issuance organizations and processes must be accredited in accordance with SP 800-79. Data objects produced by Card Issuance systems are tested according to SP 800-85B, assisted by the 800-85B test toolkit. Implementation of infrastructure for utilizing the cards is covered by FISMA reporting and SP 800-53. (Ref: <http://csrc.nist.gov/publications/nistpubs/index.html>).