

Agency Responses to NCIL Comments on the Implementation of HSPD-12 and New Badging Process:

(1) Re: Prior to the beginning of the new badging process, an applicant (includes a current employee, a prospective employee, a contractor, or other individual who requires access to a NASA facility and/or computer system) will be assigned a **sponsor/representative** who must verify the need for a badge and who will be involved in any decisions regarding the denial or revocation of a badge.

Request confirmation that the sponsor/representative will have successfully completed the same requirements as the applicant(s) being sponsored.

RESPONSE: Yes.

Provide schedule for badging the sponsors and representatives.

RESPONSE: A separate schedule for badging sponsors and representatives varies depending on the Center.

What is the ratio of sponsors/representatives to applicants at each Center?

RESPONSE: The Sponsor role can be fulfilled by any NASA Center employee. Prior to acting as such, a Sponsor must have successfully undergone the HSPD-12 badging process. "The Sponsor is the designated government official who establishes and approves the request for the Applicant's physical or logical access to NASA facilities... Generally, the Sponsor role is held by an HR specialist for NASA employees." Please refer to NASA Interim Directive NPR 1600.1. Thus, the ratio of sponsors and representatives to applicants will vary depending on the Center.

(2) Provide specific details regarding data and information to be stored on the badge chip;

RESPONSE: The PIV Card must contain the following mandatory Personally Identifiable Information:

- *Personal Identification Number (PIN)-this data is used to authenticate the cardholder to the card--in the same way a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card.*
- *A Cardholder Unique Identifier (CHUID)-this number uniquely identifies the individual within the PIV system.*
- *Two fingerprint biometrics that are PIN protected.*
- *One asymmetric cryptographic key pair used to authenticate the card to the PIV system.*

(see OPM idmanagement HSPD FAQ website)

Who will be able to read this chip?

RESPONSE: The chip imbedded in the badge can only be read by certain systems with the ability to read multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels.

If the chip is lost or stolen, is the badge holder at risk for identity theft?

RESPONSE: The visible aspects of the badge consist of:

- *Photograph*
- *Name*
- *Employee affiliation employment identifier*
- *Expiration date*
- *Agency card serial number (back of card)*
- *Issuer identification (back of card).*

As noted, the chip imbedded in the badge contains limited information, which is encrypted, and can only be read by certain systems. Any loss or theft should be immediately reported to management or the cognizant badging office, but no additional risk of identity theft has been identified.

(3) In Shana Dale's blog of June 25, 2007, she advised that Bob Hopkins, NASA, Chief of Strategic Communications, would be developing a plan for communicating the directive's requirements to the NASA employees. Please advise regarding status and what employees can expect.

RESPONSE: A plan has been developed to communicate to both our civil servants and contractor employees the purpose, goals and benefits of HSPD-12 and its badging process. These messages will be communicated by various methods and media, and may include, but is not necessarily limited to posters, fact sheets, newsletter articles and other support products at the Centers. The communications plan, also, focuses on maintaining employee awareness during all phases of the implementation process.

(4) What is the projected cost of this implementation?

RESPONSE: Like many security projects, HSPD-12 implementation was not tracked as a separate budget or cost item. All federal agencies have existing background investigation, access control, and identification credential activities. It is anticipated that these activities, and the funding used to support them will be used in support of activities compliant with FIPS 201. Any additional funding needs for implementing FIPS 201 will have to be requested by agencies through the normal federal budget process.

What is the schedule for full implementation?

RESPONSE: The Office of Management and Budget (OMB), the Executive Office of the President, has established a schedule for implementing HSPD-12. This schedule states that by October 27, 2007, all covered agencies shall complete the action of verifying and completing "background investigations for all current employees and contractors." (OMB M-05-24 pertains).

Will any employees be exempt, e.g., if they are planning to depart the Agency prior to a certain time?

RESPONSE: No. There is no provision for waivers or exemptions in HSPD-12 or in its implementing standards.

(5) What are the consequences if an employee is not issued a new badge?

RESPONSE: Centers' security offices will notify each individual when they are to begin the HSPD-12 badging process. Without a proper and current badge, employees would be treated as a visitor when entering a federal building, including not being able to access certain Federal resources. If using a badge and/or access is a condition of that employee's position, not providing the information may affect placement or employment prospects.

Please refer to NASA Interim Directive (NPR 1600.1) Section 13.1.1.

(6) What measures exist or are planned to safeguard an employee's private and personal data and information?

RESPONSE: All information gathered is subject to the Privacy Act OF 1974 (5 U.S.Code 552a.). The full system of records notice, with complete description of routine uses, was published in the Federal Register at Volume 71, Number 154 of August 10, 2006, and can be viewed at <http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/E6-13009.pdf>. A Privacy Impact Assessment was submitted on July 20, 2006, and can be reviewed at http://www.nasa.gov/privacy/PIA_NASA_Security_Records_System.html. These items set forth the information retained and how it is safeguarded.

(7) How are the classifications for Non-sensitive positions and Public Trust positions determined?

RESPONSE: The classification of a position as being Non-sensitive or Public Trust is based on the standards set out at length at 5 Code of Federal Regulations (CFR) Part 731.

What are the requirements for each?

RESPONSE: See 5 CFR 731.

Are there additional classifications?

RESPONSE: See 5 CFR 731.

May an employee appeal his/her position classification?

RESPONSE: Yes; an employee may appeal the grade, occupational series, and sometimes the title of the position. An employee may not appeal the content or accuracy of the official position description, the accuracy of the classification standard, the Agency's proposed classification decision, the classification of a position to which the employee is not officially assigned, or the classification of a position to which the employee is detailed or temporarily promoted to for a period of less than two years.

May an employee transfer into a lower risk position?

RESPONSE: An employee may apply for any position vacancy.

The Agency has previously shared with you information regarding the implementation of Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors (<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>), which calls for a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. The Agency may issue such identification only once the reliability of its issuance procedures has been established by an official accreditation process. The identification (i.e., badge) is necessary for Federal employees and contractors to have physical access to Federally-controlled facilities and logical access to Federally-controlled information technology (IT) systems. Additional information regarding HSPD-12 can be found at <http://hspd12.nasa.gov/hspddoc.htm>.

NASA will soon begin issuing new badges to replace all current badges to all individuals needing physical and/or logical access for greater than six (6) months. The new HSPD-12 badge will contain a chip that stores a Personal Identification Number (PIN); a digital certificate; a unique cardholder identification number; a digital authentication key; and the key attributes, called electronic minutiae, of two fingerprints that will authenticate users and allow access to IT resources and area locations. Some advantages of this badge to an employee are:

- Minimizes the number of passwords to remember (Note: This is a future capability (within approximately two years) which requires other IT infrastructure systems to be implemented);
- Reduces the risk of identity theft by increasing protection of personal privacy; and

Interoperability across the Agency for access to facilities and IT systems.

Additional information regarding how HSPD-12 will affect an employee can be found at <https://tdjbosc.ksc.nasa.gov/servlet/dm.web.Fetch/HSPDI-REF-121r1.pdf?gid=65743>.

Prior to the beginning of the new badging process, an applicant (includes a current employee, a prospective employee, a contractor, or other individual who requires access to a NASA facility and/or computer system) will be assigned a sponsor/representative who must verify the need for a badge and who will be involved in any decisions regarding the denial or revocation of a badge. In order to obtain the new badge, an applicant must meet the following requirements:

Identity proofing – must provide two forms of approved, unexpired identification from the list on Form I-9, Employment Eligibility Verification one of which must be a State or Federal Government issued photo ID.

The sole exception to the requirement for unexpired documents is that a U.S. passport is acceptable. I-9 information may be obtained at

<http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=31b3ab0a43b5d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=db029c7755cb9010VgnVCM10000045f3d6a1RCRD>

<http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=31b3ab0a43b5d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=db029c7755cb9010VgnVCM10000045f3d6a1RCRD>.

Background investigation – must have had an Agency request for a Federal background investigation submitted and an FBI fingerprint check completed, followed by a subsequent suitability for access determination.

Issuance of new badge – once 1 and 2 above are successfully completed, will be issued a new badge with a printed picture of his/her face, name, agency, organization, expiration date, badge serial number, and an issuer identification number.

The information on the badge will be used by NASA and other Government agencies to verify an individual's identity and right of access when he/she attempts to gain access to a Federal facility, computer, application, or data. This information will be maintained in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a(b))

(http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552a <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552a>)

and NASA's Privacy Act system of records titled, Security Records System

(<http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/E6-13009.pdf>).

Upon the individual's separation from the Agency, NASA will retain this information consistent

with NASA Procedural Requirements (NPR) 1441.1, NASA Records Retention Schedules (<http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=1441&s=1D> <<http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=1441&s=1D>>). After that time, if the information is no longer needed for safety or security reasons, it will be destroyed.

Prior to the issuance of the HSPD-12 badge, each applicant will be informed of his/her rights and responsibilities and will be required to sign a statement indicating that he/she has read and understands his/her rights and agrees to abide by the responsibilities while in possession of the badge. These rights and responsibilities include the following:

To cooperate fully in the new badging process, including submitting unaltered forms;

To use the badge only in the manner intended to gain access to NASA or other Government facilities and/or systems;

To protect the badge and its contents;

To appropriately display and secure the badge;

To report the loss of the badge within 24 hours; and

To return the badge upon expiration, demand, or termination of need or employment.

Failure, on the part of an applicant, to provide the necessary forms and information in a timely manner or to pass the background investigation and/or fingerprint check will result in the denial of the issuance of a badge. In addition, a badge may be revoked should the individual mismanage his/her responsibilities. The denial or revocation of a badge and the appeal of such will be handled in accordance with NASA Interim Directive (NID) to NASA Procedural Requirements (NPR) 1600.1, NASA Security Program Procedural Requirements (http://nodis-dms.gsfc.nasa.gov/restricted_directives/policy_letters/NM_1600-52.pdf).

Additional information regarding the implementation of HSPD-12 is available on the Agency's web site at <http://hspd12.nasa.gov>.