+ Expiration date
+ Agency card serial number (back of card)
+ Issuer identification (back of card).

The PIV Card may also bear the following optional components:

+ Agency name and/or department
+ Department or agency seal
+ PIV cardholder's physical characteristics
+ Applicant's Signature.

When a cardholder attempts to pass through an access control point for a Federally controlled facility, a human guard shall perform visual identity verification of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that shall be applied in the visual authentication process are as follows:

1. The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way.
2. The guard compares the cardholder's facial features with the picture on the card to ensure that they match.
3. The guard checks the expiration date on the card to ensure that the card has not expired.
4. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)
5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)
6. One or more of the other data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some of the characteristics of the visual authentication mechanism are as follows:

+ Human inspection of card, which is not amenable for rapid or high volume access control
+ Resistant to use of unaltered card by non-owner of card
+ Low resistance to tampering and forgery
+ Applicable in environments with and without card readers.

6.2.2 Authentication Using the PIV CHUID

The PIV Card provides a mandatory logical credential called the CHUID. As described in Section 4.2, the CHUID contains numerous data elements.

The CHUID shall be used for PIV cardholder authentication using the following sequence:

1. The CHUID is read electronically from the PIV Card.

2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. (Optional)

3. The expiration date is checked to ensure that the card has not expired.

4. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are used as input to the authorization check to determine whether the cardholder should be granted access.

Some of the characteristics of the CHUID-based authentication mechanism are as follows:

+ Can be used for rapid authentication for high volume access control

+ Low resistance to use of unaltered card by non-owner of card

+ Applicable with contact-based and contactless readers.

6.2.3 Authentication Using PIV Biometric

The PIV Card hosts a mandatory signed biometric that can be read from the card following cardholder-to-card (CTC) authentication using a PIN supplied by the cardholder. The PIV biometric is designed to support a cardholder-to-external system (CTE) authentication mechanism through a match-off-card scheme. The following subsections define two authentication schemes that make use of the PIV biometric.

Some of the characteristics of the PIV Biometric authentication mechanisms (described below) are as follows:

+ Slower mechanism, because it requires two interactions with the cardholder

+ Strong resistance to use of unaltered card by non-owner since PIN is required to activate card

+ Digital signature on biometric, which can be checked to further strengthen the mechanism

+ Applicable only with contact-based card readers.

6.2.3.1 Unattended Authentication Using PIV Biometric (BIO)

The following sequence shall be followed for unattended authentication of the PIV biometric:

1. The CHUID is read from the card.

2. The Expiration Date in the CHUID is checked to ensure the card has not expired.

3. The cardholder is prompted to submit a PIN, activating the PIV Card.

4. The PIV biometric is read from the card.

5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional)

6. The cardholder is prompted to submit a live biometric sample.

7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.3.2 Attended Authentication of PIV Biometric (BIO-A)

The following sequence shall be followed for attended authentication of the PIV biometric:

1. The CHUID is read from the card.

2. The Expiration Date in the CHUID is checked to ensure that the card has not expired.

3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant.

4. The submitted PIN is used to activate the card. The PIV biometric is read from the card.

5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional)

6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant.

7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

This authentication mechanism is similar to the unattended biometric credential check; the only difference is that an attendant (e.g. security guard) supervises the use of the PIV Card and the submission of the PIN and the biometric by the cardholder.

6.2.4 Authentication Using PIV Asymmetric Cryptography (PKI)

The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4. The following steps shall be used to perform authentication using the PIV asymmetric authentication key:

1. The cardholder is prompted to submit a PIN.

2. The submitted PIN is used to activate the card.

3. The reader issues a challenge string to the card and requests an asymmetric operation in response.

4. The card responds to the previously issued challenge by signing it using the PIV authentication private key and attaching the associated certificate.

5. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.

6. The response is validated as the expected response to the issued challenge.

7. The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.

Some of the characteristics of the PKI-based authentication mechanism are as follows:

+ Requires the use of online certificate status checking infrastructure

+ Highly resistant to credential forgery

+ Strong resistance to use of unaltered card by non-owner since PIN is required to activate card

+ Applicable with contact-based card readers.

6.3 PIV Support of Graduated Assurance Levels for Identity Authentication

The PIV Card supports a set of authentication mechanisms that can be used to implement graduated assurance levels for identity authentication. The following subsections specify the basic PIV authentication mechanisms that may be used to support the various levels of identity authentication assurance as defined in Section 6.1. Two or more of the basic identity authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder.

6.3.1 Physical Access

The PIV Card can be used to authenticate the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or may have electronic access control points. The PIV-supported authentication mechanisms for physical access control systems are summarized in Table 6-2. It is implicit that an authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Each authentication mechanism described in the table can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the department or agency's network infrastructure.

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI

6.3.2 Logical Access

The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to logical information resources. For example, a cardholder may log in to his or her department or agency network using the PIV Card; the identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.

Table 6-3 describes the authentication mechanisms defined for this standard to support logical access control. It is implicit that an authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Table 6-3. Authentication for Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
SOME confidence	CHUID	PKI
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, PKI	

Appendix A—PIV Processes

Sections 2.2 and 5.2 of this standard require the adoption and use an approved identity proofing and registration process. All identity proofing and registration systems must satisfy the PIV objectives and requirements stated in Sections 2.2 and 5.2 in order to be approved.

Section 2.3 and 5.3 of this standard requires the adoption and use of an approved credential issuance and management process. All credential issuance and management systems must satisfy the PIV objectives and requirements stated in Sections 2.3 and 5.3 in order to be approved. The heads of Federal departments and agencies may approve other identity proofing, registration and issuance process sets that are accredited as satisfying the requisite PIV objectives and requirements.

Two examples of PIV identity proofing, registration and issuance process sets that satisfy the requisite PIV control objectives and requirements are provided in this Appendix. Wherever appropriate, additional PIV-II requirements have been specified in order to meet the objectives of PIV-II.

A.1 Role Based Model

The role based identity proofing, registration and issuance process set is recommended for organizations not having a pre-existing PIV system.

A.1.1 PIV Identity Proofing and Registration

Departments and agencies that employ the generic process set for issuing PIV credentials shall follow the identity proofing and registration process defined in this section.

A.1.1.1 Roles and Responsibilities

The critical roles associated with the PIV identity proofing, registration and issuance process are defined below. These roles may be ancillary roles assigned to personnel who have other primary duties. The following roles shall be employed for identity proofing and issuance:

+ **Applicant**—The individual to whom a PIV credential needs to be issued.

+ **PIV Sponsor**—The individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.

+ **PIV Registrar**—The entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant.

+ **PIV Issuer**—The entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

+ **PIV Digital Signatory**—The entity that digitally signs the PIV biometrics and CHUID. This role only applies for PIV-II.

+ **PIV Authentication Certification Authority (CA)**—The CA that signs and issues the PIV Authentication Certificate. This role only applies to PIV-II.

The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity. The PIV Authentication CA is a CA accredited to issue certificates under the Common Policy as specified in Section 5.4.1.

Individuals and entities assigned to the PIV Registrar, Issuer, or Digital Signatory roles shall meet the applicable requirements established by an official accreditation process.

A.1.1.2 Identity Proofing and Registration of New Employees and Contractors

An Applicant applies for a PIV credential as a part of the vetting process for Federal employment, or to seek access to Federally controlled physical facilities or information resources. This section of the document defines a process that uses identity source document inspection and background checks to establish assurance of identity. The process provides the minimal functional and security requirements for achieving a uniform level of assurance for PIV identity credentials; issuing organizations may enhance or expand upon the process to meet their organizational requirements as long as the resulting process meets the requirements set forth in this section. The identity proofing and registration requirements shall include the following:

+ The PIV Sponsor shall complete a PIV Request for a particular Applicant, and submit the PIV Request to the PIV Registrar and the PIV Issuer. The PIV Request shall include the following:

  – Name, organization, and contact information of the PIV Sponsor, including the address of the sponsoring organization

  – Name, date of birth, position, and contact information of the Applicant

  – Name and contact information of the designated PIV Registrar

  – Name and contact information of the designated PIV Issuer

  – Signature of the PIV Sponsor.

  The PIV Registrar shall confirm the validity of the PIV Request prior to acceptance.

+ The Applicant shall complete Standard Form (SF) 85, OPM Questionnaire for Non-Sensitive Positions, or an equivalent, to provide the required background information. The Applicant shall then submit the completed background information form to the PIV Registrar.

+ The Applicant shall appear in person and provide two forms of identity source documents in original form to the PIV Registrar. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID). The PIV Registrar shall visually inspect the identification documents and authenticate them as being genuine and unaltered. In addition, the PIV Registrar shall electronically verify the authenticity of the source document, when such services are offered by the issuer of the source document. When electronic verification is not offered, the PIV Registrar shall use other available tools to authenticate the source and integrity of the identity source documents. The PIV Registrar shall subsequently compare the picture on the source document with the Applicant to confirm that the Applicant is the holder of the identity source document. If all of the above checks are deemed to be successful, the PIV Registrar shall record the following types of data for each of the two identity source documents presented, sign the record, and keep it on file:

  - Document title
  - Document issuing authority
  - Document number
  - Document expiration date (if any)
  - Any other information used to confirm the identity of the Applicant.

+ The PIV Registrar shall compare the Applicant's information contained in the PIV Request (e.g., full name, date of birth, contact information) with the corresponding information provided by the Applicant.

+ The PIV Registrar shall capture a facial image of the Applicant and retain a file copy of the image. In PIV-II, if an electronic facial image is captured, it shall conform to the facial image specifications in [SP800-76].

+ The PIV Registrar shall fingerprint the Applicant, obtaining all the Applicant's fingerprints as defined in Section 4.4, and retain a copy. Additionally in PIV-II, two of the Applicant's fingerprints shall be collected in an electronic format compliant with Section 4.4.

+ The PIV Registrar shall initiate a National Agency Check with Inquiries (NACI) on the Applicant as required by Executive Order 10450 [EO10450]. Appendix C provides further detail on NACI and National Agency Check (NAC). Any unfavorable results of the investigation shall be adjudicated to determine the suitability of the Applicant for obtaining a PIV credential.

+ When all of the above requirements are completed, the PIV Registrar shall notify the Sponsor and the designated PIV Issuer that the Applicant has been approved for the issuance of a PIV credential. Conversely, if any of the required steps are unsuccessful, the PIV Registrar shall send appropriate notifications to the same authorities.

+ The PIV Registrar shall make available the following information to the PIV Issuer through a secure process:

  - Applicant's facial image
  - Copy of the results of the Applicant's background investigation
  - Other data associated with the Applicant (e.g., employee affiliation).

+ In PIV-II, the PIV Registrar shall make available the following information to the PIV Digital Signatory through a secure process:

  - Electronic biometric data for card personalization
  - Other data associated with the Applicant that is required for the generation of signed objects for card personalization.

+ The PIV Registrar shall be responsible for maintaining the following:

  - Completed and signed PIV Request
  - Completed and signed SF 85 (or equivalent) form received from the Applicant

- Information related to the identity source documents checked
- Results of the required background check
- Copies of the facial image and fingerprints
- Any other materials used to prove the identity of the Applicant.

All applicable Federal regulations for security, privacy, and records archival shall be followed in the implementation of the storage and access control mechanisms used to maintain the above data, including the privacy policies specified in Section 2.3.

A.1.1.3 Identity Proofing and Registration of Current Employees and Contractors

The identity proofing process described in Section A.1.1.2 shall be followed to issue or reissue PIV credentials to current employees and contractors. However, background checks are not required if the background check results can be referenced in the application process and verified by the PIV Registrar.

A.1.2 PIV Issuance

The PIV credential issuance process shall meet the functional and security requirements defined below. Departments and agencies may enhance the issuance process to meet their local constraints and requirements; however, the resulting process shall meet the requirements below.

+ The PIV Issuer shall confirm the validity of the PIV Request received from the Sponsor, and the approval notification received from the PIV Registrar. The PIV Issuer shall also confirm that the approval notification is consistent with the results of the background investigation.
+ The PIV Issuer shall control the creation and personalization of a new PIV credential using the information provided by the PIV Registrar. In PIV-II, the PIV Issuer shall initiate the creation of a CHUID for the new PIV credential. This CHUID shall be made available to the PIV Digital Signatory through a secure mechanism.
+ In PIV-II, the Digital Signatory shall create digitally signed credential elements (biometric and CHUID) needed for the card personalization process, using the data supplied by the PIV Registrar and the newly assigned CHUID. The digitally signed credential elements shall comply with the relevant specifications in Sections 4.2.2 and 4.4.2. The signed credential elements shall be made available to the PIV Issuer.
+ The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential. Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:
  - The individual shall present a state or Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.
  - In PIV-II, the PIV Issuer (or their authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.

- In PIV-II, the Applicant may be asked to provide a PIN, or the PIV Issuer may generate a PIN on their behalf.
- The PIV Issuer shall personalize the PIV credential. The personalized PIV credential shall meet all of the technical and interoperability specifications in Section 4 for compliance with PIV-II requirements.
- In PIV-II, the Applicant may generate cryptographic key pair(s) for the PIV credential and obtain the corresponding certificates from the PIV Authentication CA at this time. Alternatively, the Applicant may be supplied a one-time authenticator[7] for use in a subsequent certificate request to the PIV Authentication CA. In the latter case, the Applicant will generate their key pair(s) at a local workstation[8] rather than at the PIV Issuer location.
- In PIV-II, the recipient's name, issuer identity, card number, and possibly PKI certificate identification information shall be enrolled and registered with back-end data stores that support the PIV system. Depending on the infrastructure design, the back-end data stores may be centralized or decentralized.
- The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.
- When all of the above requirements are completed, the PIV Issuer shall notify the PIV Sponsor and the designated PIV Registrar signifying that the personalization and issuance process has been completed. Conversely, if any of the required steps are unsuccessful, the PIV Registrar shall send appropriate notifications to the same authorities.
- The PIV Issuer shall be responsible for maintaining the following:
  - Completed and formally authorized PIV Request
  - The approval notice from the PIV Registrar
  - The name of the PIV credential holder (Applicant)
  - The credential identifier. In PIV-II, this identifier is the Agency Card Serial Number
  - The expiration date of the PIV credential
  - The signed acceptance form from the PIV credential holder

All applicable Federal regulations for security, privacy, and records archival shall be followed in the implementation of the storage and access control mechanisms used to maintain the above data, including the privacy policies specified in Section 2.4.

[7] The issuing agency must ensure the necessary PKI management functions are supported and implemented in conformance with the security policy objectives mandated in [COMMON].

[8] The issuing agency is responsible for the necessary PKI certificate management.

A.2 System-Based Model

Organizations that possess an automated identity management system may choose to employ the system based identity proofing, registration and issuance process set. This section is provided by the Government Smart Card Interagency Advisory Board.

A.2.1 PIV Identity Proofing and Registration

For compliance to the PIV control objectives in Sections 2.2 and 5.2 of this standard, at a minimum, agencies employing the system-based identity proofing, registration and issuance process set using an Automated Identity Management System shall follow the identity proofing and registration process defined in Sections A.2.1- A.2.4 when issuing PIV credentials. Figure A-1, PIV Identity Verification and Issuance, shows the logical components that comprise a PIV identity proofing and credential issuance process. This diagram illustrates the minimum mandatory components and roles required to support PIV control objectives and requirements.

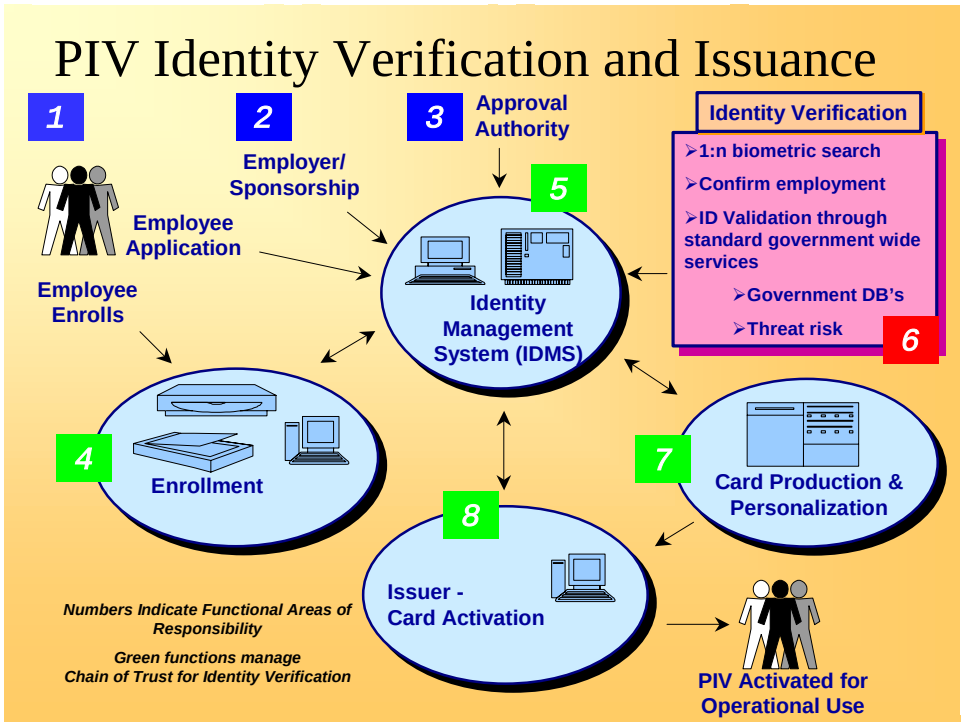


Figure A-1. PIV Identity Verification and Issuance

A.2.2 Roles and Responsibilities

The roles associated with the system-based PIV identity proofing, registration and issuance process are defined below:

+ Applicant—The individual to whom a PIV credential is to be issued. Individuals shall provide the necessary supporting identity-source documents to prove the claimed identity.

+ Employer/Sponsor— The individual who substantiates the relationship to the Applicant and provides sponsorship to Applicant. The employer/sponsor shall authorize the request for a PIV credential.

+ Enrollment Official— The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate the identity-source documentation. The Enrollment Official delivers a secured enrollment package to the IDMS for adjudication.

+ Approval Authority—The entity that establishes organizational chain of command within the Identity Management System (IDMS) for PIV application approvals. This includes establishing approved Employer/Sponsors. May designate automated or manual approval processes for completed PIV applications. Shall manage the total scope of the chain of trust established in functional process. Shall manage appropriate privacy and security controls.

+ Issuing Authority (Issuer) —The entity that issues the PIV credential to the Applicant after all identity proofing, background checks, and related approvals have been completed.

The issuer shall complete the chain of trust by performing 1:1 biometric check of the applicant against the PIV enrollment record. Upon confirmation of correct individual, the issuer shall activate the card. The issuer shall then release the credential to the individual.

Roles are not defined to mandate that a single individual within an organization must fulfill any given role. All roles and processes may be provided by accredited service providers compliant with this standard.

The Approval Authority shall practice best practices for separation of roles and responsibilities according to risk. The Approval Authority shall ensure the system has at least two persons performing different functions in the chain of trust processes. The principle of separation of duties shall be enforced to ensure that no single individual has the capability to issue a PIV credential without the participation of another authorized person. Card production may be accomplished either centrally or at a distributed issuer facility, provided security and quality control objectives for card stock management are fully met. The Applicant must appear in-person at least once before the issuance of a PIV card.

The components associated with the PIV identity proofing and issuance are:

+ Identity Management System—The Approval Authority shall maintain the IDMS that shall be the system of records for PIV credentials issued. It performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a 1:many search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.

+ Enrollment System—Initiates the chain of trust for identity proofing. Enrollment shall be provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.

+ Card Production and Personalization System—Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to

track status, control inventory, and protect blank card stock and personalized/printed card stock prior to activation.

PIV Identity Proofing and Issuance Requirements and Workflow are:

+ Applicant—The individual to whom an identity credential is to be issued. Individual shall provide supporting enrollment documentation for claimed identity.

+ Employers/Sponsors—Shall substantiate the relationship to the Applicant and provide sponsorship of Applicant. Shall authorize the request for a PIV credential.

+ Approval Authority—Is responsible for and shall manage the total scope of the chain of trust established in functional process areas 4 through 8 in *Figure A-2*.

+ Enrollment—Initiates the chain of trust for identity proofing. Enrollment shall provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.

+ Identity Management System—The Approval Authority shall maintain an IDMS that shall be the system of records for PIV credentials issued by that Approval Authority. The IDMS performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.

+ Card Production and Personalization—Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to protect blank card stock, consumable supplies, and personalized/printed card stock prior to activation.

+ Issuer—The entity that issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The issuer shall complete the chain of trust by: performing 1:1 biometric check of applicant against PIV enrollment record, verifying photograph in enrollment record matches the individual. Upon confirmation of correct individual, the issuer shall activate the card. Upon activation, the issuer shall close the chain of trust by having the individual verify their biometrics against the PIV credential. The issuer shall then release the credential to the individual.

A.2.3 Identity Proofing and Enrollment

All actions taken for approval/denial of requests by all participants in this process shall have an auditable trail that can support both forensic and system management capabilities. This audit trail shall provide a critical control component for the chain of trust for PIV issuance and management.

A.2.4 Employer/Sponsor

Employer/Sponsors must be pre-registered in the IDMS. The Approval Authority must establish roles for Employer/Sponsors. These may be government organizations or contractor organizations. The Approval Authority shall establish appropriate delegation of authority to Employer/Sponsors to approve PIV applications of Applicants.

A.2.5 PIV Application Process

The PIV Application Process has four components:

1. The Applicant request and claimed identity documentation,
2. The Employer/Sponsor approval of Applicant request,
3. The approval authority confirms and approves PIV application, appropriate sponsorship, and shall approve the PIV request,
4. The enrollment to bind the submissions from (1), (2) and (3) for formal submission to the IDMS initiating the identity verification and validation process.

The Applicant shall provide a formal request for a PIV.

The Employer/Sponsor shall approve the Applicant request.

Once the Applicant has gained the sponsorship and approval of the Employer, the Applicant shall appear for Enrollment. The Applicant shall provide a minimum of two forms of identification from the list of acceptable documents included in the *Form 1-9, OMB No. 1115-0136, Employment Eligibility Verification* to the PIV Registration Authority. At least one of the documents shall be a valid State or Federal Government-issued picture ID.

A.2.6 PIV Enrollment Process

The PIV Enrollment process shall provide the following minimum steps:

1. Applicant shall appear for enrollment with supporting documentation;
2. Enrollment shall inspect and confirm all supporting documents using automated means if available;
3. Enrollment shall establish that the individual present matches the supporting documents;
4. Enrollment shall confirm Employer/Sponsor approval for PIV; and
5. Enrollment shall scan all supporting documents.

The PIV Binding process shall provide the following minimum steps:

1. Enrollment shall take biometric samples and photograph of the Applicant;
2. Enrollment shall manage the quality assurance process of the biometric and photographic capture. The biometric samples shall be verified to ensure proper performance; and
3. Enrollment shall bind the completed electronic enrollment package with a digital signature and forward the enrollment application to the IDMS for identity verification and validation.

The completed PIV enrollment package shall include:

+ Scanned documents supporting identity claim;

+ Biometric samples and digital photograph;
+ Personal biographic and organizational information; and
+ Digital signature of Enrollment Official.

A.2.7 Identity Verification Process

The IDMS shall receive the completed package for PIV from Enrollment. The IDMS shall verify the integrity of that package by confirming completeness, accuracy, and digital signatures.

The IDMS shall provide a means to confirm employment and sponsorship as identified in the package.

The IDMS shall perform a 1:many search to assure that the individual identified in the package has not applied previously under a different name.

The IDMS shall conduct the appropriate identity verification and validation using government-wide databases and services in accordance with HSPD-11.

The Approval Authority shall provide adjudication of identity claim should any of these three core checks identify a potential risk.

After successful completion of the appropriate identity verification process, the Approval Authority shall approve card production for the credential. The Approval Authority may approve issuance of a PIV credential prior to completion of all core checks for identity verification and validation if these processes exceed ten days.

The IDMS shall be responsible to maintain:

1. Completed and signed PIV enrollment package;
2. Copies of the identity source documents;
3. Completed and signed background form received from the Applicant;
4. Results of the required background check;
5. Any other materials used to prove the identity of the Applicant;
6. The credential identifier such as an identity credential serial number;
7. The expiration date of the identity credential;
8. Unique minimal identity record for each approved Applicant;
9. Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and
10. Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking.

The IDMS shall provide services that:

1. Notify the Employee/Contractor Applicant of status of the PIV;

2. Notify the Employer of status of the PIV; and

3. Enable validation by anyone inquiring if an issued credential is still valid.

The IDMS shall provide complete personalization and printing information for card production for all approved PIV credentials as required by the supporting card production facility's requirements. This information shall be provided to enable the full chain of trust between the individual, the issuer, the identity verification performed, the credential and the biometric.

A.2.8 Card Production, Activation and Issuance

Card production may be performed either centrally or in a distributed location. The IDMS shall track the status of a PIV credential throughout its life cycle, from initial production request, personalization and printing, activation and issuance, suspension, revocation and destruction.

Card production services shall—

1. Maintain full inventory control of blank initialized or pre-issued (e.g. with the manufacturers keys) stock, consumables and manufacturing materials;

2. Maintain a list of approved IDMS systems that can submit PIV requests for card production,

3. Provide acknowledgement of IDMS request to produce a PIV;

4. Notify the IDMS upon completion of PIV credential production;

5. Maintain a list of approved Issuers that can activate and issue PIV credentials;

6. Only send information regarding production of PIV credentials to approved authorities;

7. Only send fully completed and personalized PIV credentials to approved Issuing Agents; and

8. Document, implement, and maintain a Card Production, Activation and Issuance Security Policy.

At time of activation, the Issuer shall establish that the individual seeking to activate their PIV credential is the individual who applied for the PIV with a 1:1 biometric verification to the IDMS. Once confirmed, the Issuer shall activate the credential.

A.2.9 Suspension, Revocation and Destruction

It is important to keep track of active cards as well as lost, stolen and expired cards. A card registry for all cards issued shall be established and maintained.

A.2.10 Re-issuance to Current PIV Credential Holders

When issuing or re-issuing identity credentials to current employees, the Issuing Authority shall—

1. Insure the IDMS record for this individual states the credential is not expired;

2. Verify the individual with a 1:1 biometric match against the IDMS record;

3. Verify the individual against the IDMS record digital photograph;

4. Recapture biometrics;

5. Issue a new credential and update the IDMS record; and
6. The recaptured biometrics and new credential record shall be digitally signed by the Issuing Authority.

Appendix B—PIV Validation, Certification, and Accreditation

B.1 Accreditation of PIV Service Providers

[HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. Funding permitting, NIST will establish detailed criteria that PIV Card issues must meet for accreditation. Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until such time as these are completed, agencies must self-certify their own issuers of PIV Cards.

B.2 Security Certification and Accreditation of IT System(s)

In order to accomplish the accreditation of PIV service providers as described above, and to be compliant with the provisions of OMB Circular A-130, App. III, the IT system(s) used by PIV service providers must also be certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. NIST SP 800-37 provides a formal framework for certification, along with specific requirements for validating and obtaining certificates for the PIV modules described below. [SP800-37]

B.3 Conformance of PIV Components to this Standard

NIST plans to develop a PIV validation program that will test implementations for conformance with this standard. Note that the following is not requirements until NIST establishes a program. Information on this program will be published at http://csrc.nist.gov/npivp as it becomes available.

A PIV system is FIPS 201-compliant after each of its constituent components (card, reader, issuer software, and registration database) has met its individual validation requirements. Because these individual validation requirements are based on different standards and no single test laboratory is accredited for validating products built to all these standards, a PIV system has to undergo testing and consequent validation through multiple validation facilities. The PIV components and currently available validation requirements are summarized in Table B-1.

Table B-1. PIV System Components and Validation Requirements

PIV Component	Validation Requirement(s)
PIV ICC	ISO/IEC 7816, ISO/IEC 10373 (Parts 1 and 3) ISO/IEC 14443 (Parts 1-4), ISO/IEC 10373 (Part 6) Crypto Modules—FIPS 140-2
PIV Reader	PC/SC
Card Issuance and Maintenance System	Crypto Modules—FIPS 140-2

B.4 Cryptographic Testing and Validation (FIPS 140-2 and algorithm standards)

All the cryptographic modules in the PIV system (both on-card and issuer software) shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher). [FIPS140-2] The facilities for FIPS 140-2 testing are the Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) program of NIST. Vendors wanting to supply

cryptographic modules for the PIV system can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP), a joint program run by NIST and Communications Security Establishment (CSE) of the Government of Canada. The details of the CMVP and NVLAP programs and the list of CMT laboratories can be found at the CMVP Web site at http://csrc.ncsl.nist.gov/cryptval.

Appendix C—Background Check Descriptions

The following describes the details of a National Agency Check (NAC) and a National Agency Check with Inquiries (NACI).

+ **NAC.** The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.

+ **NACI.** The basic and minimum investigation required on all new Federal employees consisting of a NAC with 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). Coverage includes:

  – Employment, 5 years

  – Education, 5 years and highest degree verified

  – Residence, 3 years

  – References

  – Law Enforcement, 5 years

  – NACs

Appendix D—PIV Object Identifiers and Certificate Extension

D.1 PIV Object Identifiers

Table D-1 lists details for PIV object identifiers.

Table D-1. PIV Object Identifiers

ID	Object Identifier	Description
PIV eContent Types		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.6.2	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
PIV Attributes		
pivCardholder-Name	2.16.840.1.101.3.6.3	The attribute value is of type DirectoryString and specifies the PIV cardholder's name.
pivCardholder-DN	2.16.840.1.101.3.6.4	The attribute value is an X.501 type Name and specifies the DN associated with the PIV cardholder in the PIV certificate(s).
pivSigner-DN	2.16.840.1.101.3.6.5	The attribute value is an X.501 type Name and specifies the subject name that appears in the PKI certificate for the entity that signed the biometric or CHUID.
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV card.
PIV Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.
id-PIV-cardAuth	2.16.840.1.101.3.6.8	This specifies that the public key is used to authenticate the PIV card rather than the PIV cardholder.

D.2 PIV Certificate Extension

The PIV NACI indicator extension indicates the status of the subject's background investigation at the time of credential issuance. The PIV NACI indicator extension is always non-critical, and SHALL appear in all PIV authentication certificates. The value of this extension is asserted as follows:

+ TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed.

+ FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.

Note that PIV authentication certificates MUST NOT be issued to a subject if —

+ a NACI has been completed unsuccessfully;

+ the FBI National Criminal History Fingerprint Check has not completed; or

+ a NACI has not yet been initiated.

The PIV NACI indicator extension is identified by the id-piv-NACI object identifier. The syntax for this extension is defined by the following ASN.1 module. See an important change notice at the end of this document.

```
PIV_Cert_Extensions { 2 16 840 1 101 3 6 10 1  }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NONE --

id-piv-NACI  OBJECT IDENTIFIER  ::= { 2 16 840 1 101 3 6 9 1 }

NACI_indicator ::= BOOLEAN DEFAULT FALSE

END
```

Appendix E—Physical Access Control Mechanisms

The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group publication *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS) provides guidance on physical access for various assurance profiles. Table C-1 describes the relationship between the PACS assurance levels and the PIV identity authentication levels defined in Section 6.1.

Table E-1. PIV Support of PACS Assurance Profiles

PACS Assurance Profile	PIV Identity Authentication Assurance Levels
PACS Low	SOME confidence
PACS Medium	SOME confidence
PACS High (without PIN)	SOME confidence
PACS High (with PIN)	VERY HIGH confidence

Appendix F—Glossary of Terms, Acronyms, and Notations

F.1 Glossary of Terms

The following terms are used throughout this standard.

Access Control: The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Applicant: An individual applying for a PIV Card/credential. The Applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.

Application: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Approved: FIPS approved or NIST recommended. An algorithm or technique that is either (1) specified in a FIPS or a NIST recommendation or (2) adopted in a FIPS or NIST recommendation.

Architecture: A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).

Asymmetric Keys: Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication: The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iriscan samples are all examples of biometrics.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

Biometric System: An automated system capable of the following:

+ Capturing a biometric sample from an end user
+ Extracting biometric data from that sample
+ Comparing the extracted biometric data with data contained in one or more references
+ Deciding how well they match
+ Indicating whether or not an identification or verification of identity has been achieved.

Capture: The method of taking a biometric sample from an end user. [INCITS/M1-040211]

Cardholder: An individual possessing an issued PIV Card.

Certificate Revocation List: A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 3280]

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification Authority: A trusted entity that issues and revokes public key certificates.

Claimant: A party whose identity is to be verified using an authentication protocol.

Comparison: The process of comparing a biometric with a previously stored reference. See also "Identification" and "Identity Verification". [INCITS/M1-040211]

Component: An element of a large system, such as an identity card, PIV Issuer, PIV Registrar, card reader, or identity verification support, within the PIV system.

Conformance Testing: A process established by NIST within its responsibilities of developing, promulgating, and supporting FIPS for testing specific characteristics of components, products, and services, as well as people and organizations for compliance with a FIPS.

Credential: Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

Cryptographic Key (Key): A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Federal Information Processing Standards (FIPS): A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Framework: A structured description of a topic of interest, including a detailed statement of the problem(s) to be solved and the goal(s) to be achieved. An annotated outline of all the issues that must be addressed while developing acceptable solutions to the problem(s). A description and analysis of the constraints that must be satisfied by an acceptable solution and detailed specifications of acceptable approaches to solving the problems(s).

Graduated Security: A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Hash-Based Message Authentication Code (HMAC): A message authentication code that uses a cryptographic key in conjunction with a hash function.

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. **One-Way.** It is computationally infeasible to find any input that maps to any pre-specified output.
2. **Collision Resistant.** It is computationally infeasible to find any two distinct inputs that map to the same output.

Identification: The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier: Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Binding – Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority. Represented by an identity assertion from the issuer that is carried by a *PIV credential*.

Identity Management System (IDMS) – Identity management system comprised of one or more systems or applications that manages the identity verification, validation and issuance process.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.

Identity Registration: The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

Information in Identifiable Form (IIF): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. [E-Gov]

Interoperability: For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.

Issuer: The organization that is issuing the PIV Card to an Applicant. Typically this is an organization for which the Applicant is working.

JPEG: A standardized image compression function originally established by the Joint Photographic Experts Group.

Key: See "Cryptographic Key".

Match/Matching: The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity.

Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.

Model: A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.

Off-Card: Refers to data that is not stored within the PIV Card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the PIV Card.

On-Card: Refers to data that is stored within the PIV Card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the PIV Card.

One-to-Many: Synonym for "Identification". [INCITS/M1-040211]

Online Certificate Status Protocol (OCSP): An online protocol used to determine the status of a public key certificate. [RFC 2560]

Personal Identification Number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

PIV Issuer: An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.

PIV Registrar: An entity that establishes and vouches for the identity of an Applicant to a PIV Issuer. The PIV Registrar authenticates the Applicant's identity by checking identity source documents and identity proofing, and ensures a proper background check has been completed, before the credential is issued.

PIV Sponsor: An individual who can act on behalf of a department or agency to request a PIV Card for an Applicant.

Population: The set of users for the application. [INCITS/M1-040211]

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI): A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

Recommendation: A special publication of the ITL stipulating specific characteristics of technology to use or procedures to follow to achieve a common level of quality or level of interoperability.

Reference Implementation: An implementation of a FIPS or a recommendation available from NIST/ITL for demonstrating proof of concept, implementation methods, technology utilization, and operational feasibility.

Registration: See "Identity Registration".

Secret Key: A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution.

Standard: A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.

Trustworthiness – Security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Verification: See "Identity Verification".

F.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

ACL	Access Control List
AES	Advanced Encryption Standard
AIA	Authority Information Access
AIM	Association for Automatic Identification and Mobility
ANSI	American National Standards Institute
CA	Certification Authority
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Cardholder Unique Identifier
CIA	Cryptographic Information Application
CMS	Cryptographic Message Syntax
CMT	Cryptographic Module Testing
CMTC	Card Management System to the Card
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CSE	Communication Security Establishment
CTC	Cardholder to Card
CTE	Cardholder to External System
DCII	Defense Clearance and Investigation Index
DN	Distinguished Name

dpi	Dots Per Inch
DUNS	Data Universal Numbering System
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ERT	Emergency Response Team
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certificate Authority
FBI	Federal Bureau of Investigation
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standards
FIPS PUB	FIPS Publication
FISMA	Federal Information Security Management Act
HMAC	Hash-Based Message Authentication Code
HR	House of Representatives
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IAB	Interagency Advisory Board
ICC	Integrated Circuit Chip
ID	Identification
IDMS	Identity Management System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIF	Information in Identifiable Form
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MQV	Menezes-Qu-Vanstone
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NVLAP	National Voluntary Laboratory Accreditation Program
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management

PACS	Physical Access Control System
PC/SC	Personal Computer/Smart Card
PDF	Portable Data File
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
pt	Point
RFC	Request for Comment
RSA	Rivest Shamir Adleman
SF	Standard Form
SHA	Secure Hash Algorithm
SII	Security/Suitability Investigations Index
SP	Special Publication
SSP REP	Shared Service Provider Repository Service Requirement
URI	Uniform Resource Identifier

F.3 Notations

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this standard are to be interpreted as described in IETF RFC 2119.

Additionally, this standard uses the following typographical conventions in text:

+ Terms (word or concatenated words) in *Italics* represent ASN.1 data types. For example, *SignedData or SignerInfo* are data types defined for digital signatures.

+ Letters or words in CAPITALS separated with underscore represent CBEFF-compliant data structures. For example, CBEFF_HEADER is a header field in the CBEFF structure.

Appendix G—References

[ANSI322] ANSI INCITS 322 Information Technology, *Card Durability Test Methods*, ANSI, 2002.

[CBEFF] NISTIR 6529-A, *Common Biometric Exchange Formats Framework (CBEFF)*, NIST, 2003.

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 2.0, November 1, 2004. Available at http://www.cio.gov/ficc/documents/CommonPolicy.pdf.

[E-Gov] *E-Government Act of 2002*, U.S. Public Law 107-347, 2002.

[EO10450] Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953. Available at http://www.dss.mil/nf/adr/10450/eo10450T.htm.

[FIPS140-2] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001. Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[G155-00] ASTM G155-00, *Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials*, Vol. 14.04, ASTM, July 2000.

[G90-98] ASTM G90-98, *Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight*, Vol. 14.04, ASTM, 2003.

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

[INCITS/M1-040211] ANSI/INCITS M1-040211, *Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers*, ANSI, April 2004.

[ISO10373] ISO/IEC 10373, *Identification Cards—Test Methods*. Part 1—*Standard for General Characteristic Test of Identification Cards*, ISO, 1998. Part 3—*Standard for Integrated Circuit Cards with Contacts and Related Interface Devices*, ISO, 2001. Part 6—*Standard for Proximity Card Support in Identification Cards*, ISO, 2001.

[ISO14443] ISO/IEC 14443-1:2000, *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*, ISO, 2000.

[ISO7810] ISO/IEC 7810:2003, *Identification Cards—Physical Characteristics*, ISO, 2003.

[ISO7816] ISO/IEC 7816, *Identification Cards—Integrated Circuits with Contacts*, Parts 1-6, ISO.

[NISTIR7123] NISTIR 7123, *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report*, NIST, June 2004.

[OMB322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.

[OMB404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[PACS] PACS v2.2, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004.

[PCSC] Personal Computer/Smart Card Workgroup Specifications. Available at http://www.pcscworkgroup.com.

[PRIVACY] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

[PROF] *X.509 Certificate and CRL Profile for the Common Policy*, Version 1.1, July 8, 2004. Available at http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf.

[RFC2560] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)*, Internet Engineering Task Force (IETF), June 1999. Available at http://www.ietf.org/rfc/rfc2560.txt.

[RFC3280] RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, April 2002. Available at http://www.ietf.org/rfc/rfc3280.txt.

[RFC3852] RFC 3852, *Cryptographic Message Syntax (CMS)*, IETF, July 2004. Available at http://www.ietf.org/rfc/rfc3852.txt.

[SP800-37] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST, May 2004.

[SP800-53] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, NIST, September 2004 (2PD).

[SP800-63] NIST Special Publication 800-63, *Electronic Authentication Guideline*, Appendix A, NIST, June 2004.

[SP800-73] NIST Special Publication 800-73, *Integrated Circuit Card for Personal Identity Verification*, NIST, February 2005.

[SP800-76] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, February 2006.

[SP800-78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, March 2005.

[SSP REP] Shared Service Provider Repository Service Requirements, January 23, 2004. Available at http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf.

FIPS 201-1, PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS
CHANGE NOTICE 1

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

DATE OF CHANGE: June 23, 2006

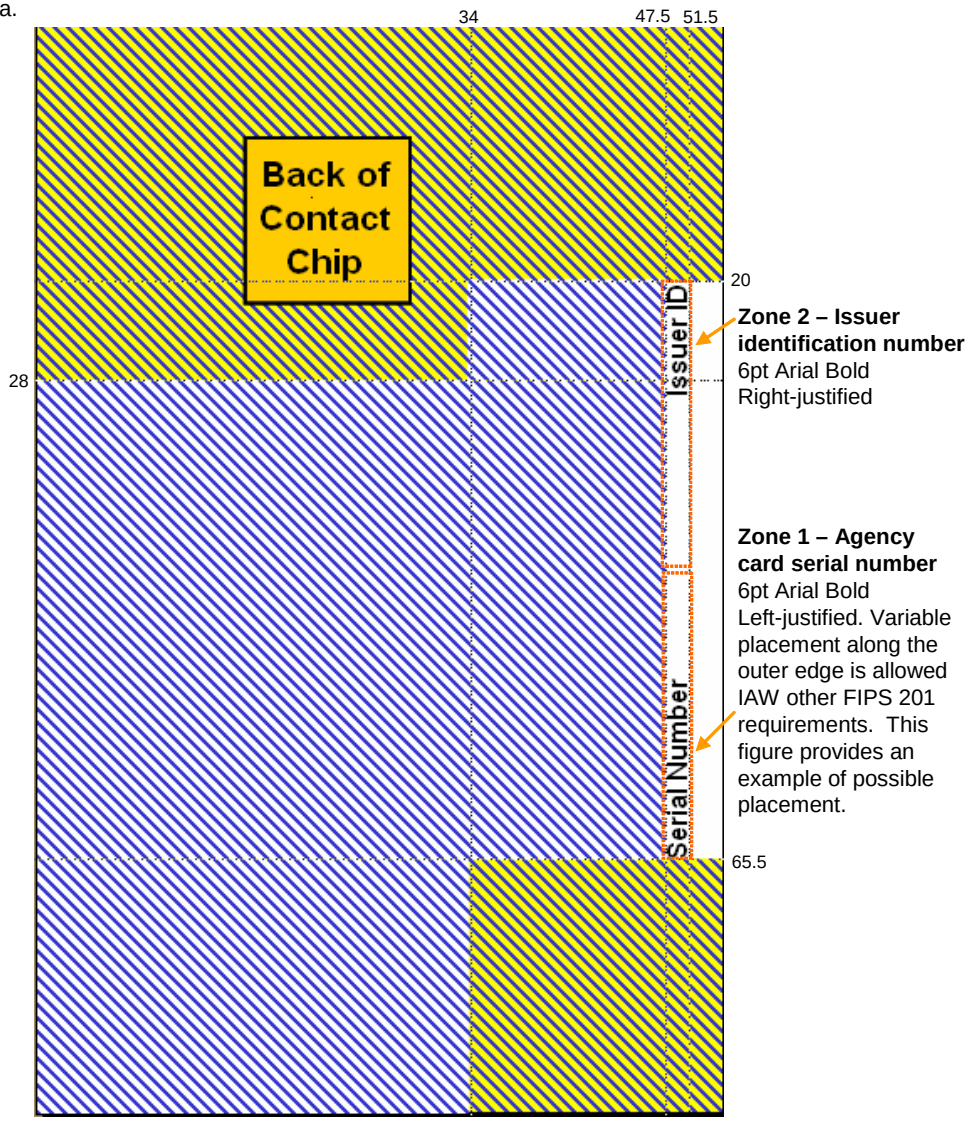
Questions regarding this change notice may be directed to piv_comments@nist.gov or to William MacGregor (william.macgregor@nist.gov, 301-975-8721).

The Homeland Security Presidential Directive HSPD-12 called for a common identification standard to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201 (FIPS 201-1) was developed to establish standards for identity credentials. This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

FIPS 201-1 was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on March 2006. This change notice provides changes to the graphics on the back of the PIV card and the ASN.1 encoding of NACI indicator as follows:

Date	Section, Page	Clarification
6/23/06	4.1.4.2, Pg. 18	Variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card is allowed. Revised Figure 4-6 and Figure 4-8 below further clarifies the placement of Agency Card Serial Number.
6/23/06	D.2, Pg. 68	Delete “DEFAULT FALSE” to the ASN.1 module for the NACI indicator extension and replace underscores with dashes as follows: PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1 } DEFINITIONS EXPLICIT TAGS ::= BEGIN -- EXPORTS ALL -- -- IMPORTS NONE -- Id-piv-NACI OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 6 9 1 } NACI-indicator ::= BOOLEAN END

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



Optional data area. Agency-specific data may be printed in this area. See examples for required placement of optional data elements.

Optional data area likely to be needed by card manufacturer. Optional data may be printed in this area, but will likely be subject to restrictions imposed by card and/or printer manufacturers.

Figure 4-6. Card Back—Printable Areas and Required Data

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

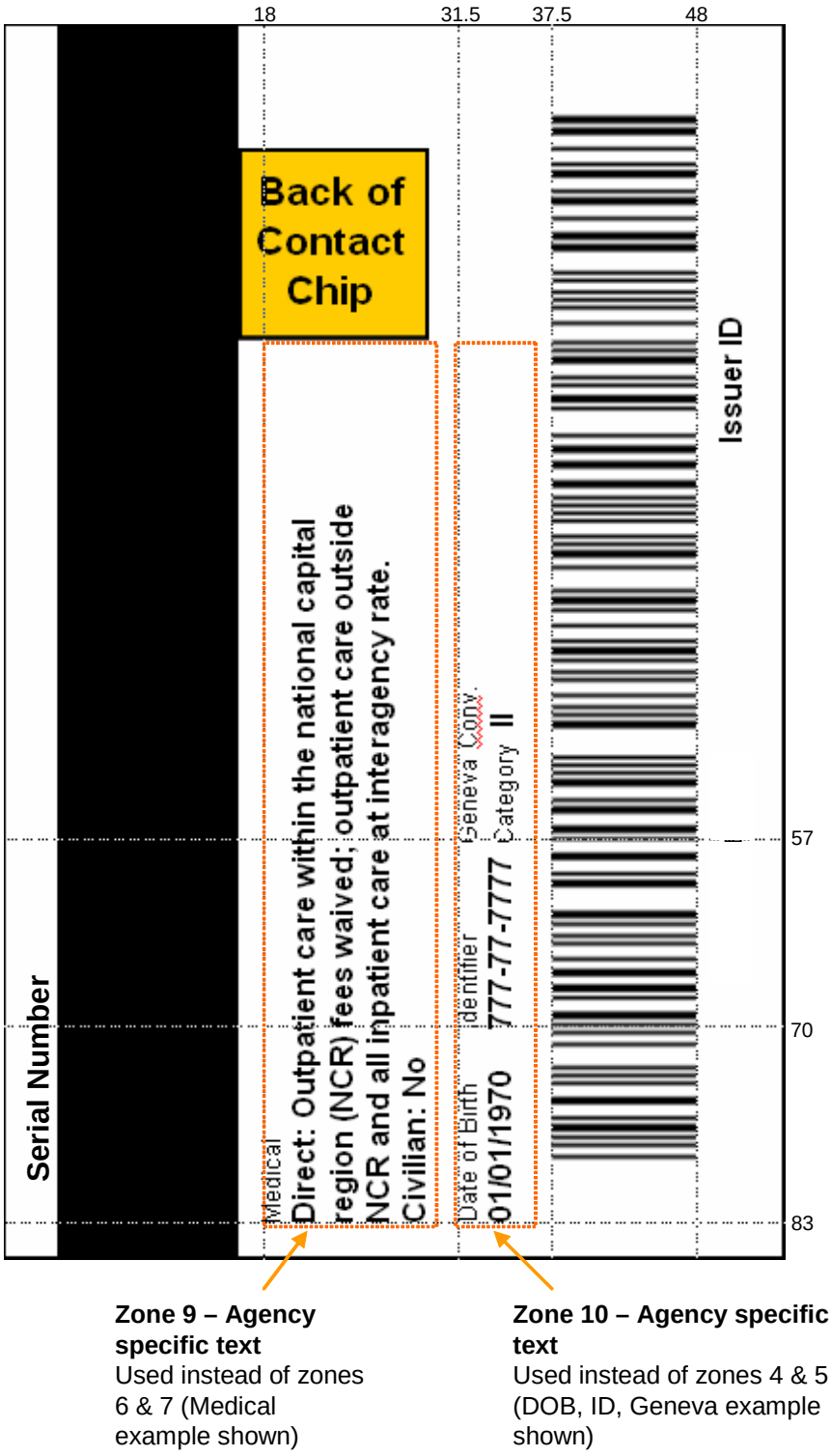


Figure 4-8. Card Back—Optional Data Placement—Example 2

EXHIBIT C

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

M-05-24

August 5, 2005

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors

On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive). The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard 201 (the Standard). This memorandum provides implementing instructions for the Directive and the Standard.

Inconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the Federal government. Successful implementation of the Directive and the Standard will increase the security of your Federal facilities and information systems. As noted in the attached guidance, this standard identification applies to your employees and contractors who work at your facilities or have access to your information systems. Following implementation, Federal departments and agencies will be able to recognize and accept this common identification standard.

It is important to note the use of standard identification does not replace your existing law or OMB policy responsibilities; including the laws and policies governing personnel security, acquisition, and information technology security law.

If you have questions about this guidance, contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget. Phone (202) 395-3562, fax (202) 395-5167, or e-mail: eauth@omb.eop.gov.

Attachments

A) HSPD-12 Implementation Guidance for Federal Departments and Agencies
B) HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors

Attachment A

HSPD-12 IMPLEMENTATION GUIDANCE FOR FEDERAL DEPARTMENTS AND AGENCIES

1. To whom does the Directive apply?

As defined below, Department and Agency heads must conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to Federally controlled facilities and/or information systems.

A. Departments and Agencies

- "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).

Does **not** apply to:

- "Government corporations" as defined by title 5 U.S.C. § 103(1) are encouraged, but not required to implement this Directive.

B. Employee

- Federal employees, as defined in title 5 U.S.C § 2105 "Employee," within a department or agency.
- Individuals employed by, detailed to or assigned to a department or an agency.
- Within the Department of Defense (DoD) and the Department of State (DoS), members of the Armed Forces, Foreign Service, and DoD and DoS civilian employees (including both appropriated fund and non-appropriated fund employees).
- Applicability to other agency specific categories of individuals (e.g., short-term (i.e. less than 6 months) guest researchers; volunteers; or intermittent, temporary or seasonal employees) is an agency risk-based decision.

Does **not** apply to:

- Within DoD and DoS, family members and other eligible beneficiaries.
- Occasional visitors to Federal facilities to whom you would issue temporary identification.

C. Contractor

- Individual under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to whom you would issue Federal agency identity credentials, consistent with your existing security policies.

Does **not** apply to:

- Individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.

D. Federally Controlled Facilities

- Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency covered by this Directive.
- Federally controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the Directive applies to the 10th floor only.
- Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
- Facilities under a management and operating contract. Such as for the operation, maintenance, or support of a Government-owned or-controlled research, development, special production, or testing establishment.

E. Federally Controlled Information Systems

- Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3502(8)).
- Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (44 U.S.C. § 3544(a)(1)(A)).
- Applicability for access to Federal systems from a non-Federally controlled facility (e.g. a researcher up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on the risk determination required by existing National Institute of Standards and Technology (NIST) guidance.[1]

Does **not** apply to:

- Identification associated with national security systems as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3542(2)(A)).[2]

[1] Federal Information Processing Standard (FIPS 199): Standards for Security Categorization for Federal Information and Information Systems, 2/04, http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[2] See NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System, 8/03, http://www.csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf.

2. What is the schedule for implementing the Directive?

A. The Department of Commerce's National Institute of Standards and Technology (NIST) shall meet the following milestones:

Date	Department of Commerce Action
2/25/05	HSPD-12 Standard Published –Federal Information Processing Standard 201 (FIPS 201)[3]
6/25/05	Technical reference implementation released
8/5/05	Conformance testing information released

B. All covered departments and agencies shall complete the following actions:

Date	Agency Action
6/27/05	Implementation plans submitted to OMB
8/26/05	Provide list of other potential uses of Standard (see question 7)
10/27/05	Comply with FIPS 201, Part 1 (see question 3)
10/27/06	Begin compliance with FIPS 201, Part 2 (see question 4)
10/27/07	Verify and/or complete background investigations for all current employees and contractors (see question 3)
10/27/08	Complete background investigations for all Federal department or agency employees employed over 15 years (see question 3)

C. The General Services Administration (GSA) shall complete the following actions:

Date	General Services Administration Action
7/31/05	Establish authentication acquisition services (see question 5)
10/27/05	Sponsor Federal Acquisition Regulation (FAR) amendment implementing the Standard.

3. How should I implement Part 1 of the Standard?

The Standard, required by HSPD-12, contains two parts to guide department and agency implementation. The requirements of part 2 build upon the requirements of part 1. They are:

- **Part 1: Common Identification, Security and Privacy Requirements –** minimum requirements for a Federal personal identification system that meets the control and security objectives of the Directive, including the personal identity proofing, registration, and issuance process for employees and contractors.

[3] FIPS 201: Personal Identity Verification for Federal Employees and Contractors, 2/25/05, http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf. All technical documents are available at http://www.csrc.nist.gov/piv-project/.

- **Part 2: Government-wide Uniformity and Interoperability –** Detailed specifications to support technical interoperability among departments and agencies, including card elements, system interfaces, and security controls required to securely store and retrieve data from the card.

For all new employees, contractors and other applicable individuals your department or agency must by October 27, 2005:

A. **Adopt and accredit a registration process** consistent with the identity proofing, registration and accreditation requirements in section 2.2 of the Standard and forthcoming technical guidance issued by NIST, regardless of whether your agency will be ready to issue standard compliant identity credentials by October 27, 2005. This registration process will apply to all new identity credentials issued (i.e. no new identity credentials can be issued until these conditions are met).[4]

B. **Initiate the National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to credential issuance**. Before issuing the credential, agencies should receive notification of results of the National Agency Checks.[5] If you do not receive the results in 5 days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check).[6]

   Identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable (i.e. information is stored in the data on the card) from identity credentials issued to individuals who have a completed investigation. The Department of Commerce will provide the electronic format for this information.

   Agencies shall not re-adjudicate individuals transferring from another department or agency provided: 1) possession of a valid Federal identity credential can be verified by the individual's former department or agency, and 2) the individual has undergone the required NACI or other suitability or national security investigation at individual's former agency.

   Since Foreign National employees and contractors may not have lived in the United States long enough for a NACI to be meaningful, agencies should conduct an equivalent investigation, consistent with your existing policy. OMB will establish an interagency working group to explore whether guidance is necessary with respect to background investigations for foreign national employees and contractors.

---

[4] NIST Special Publication 800-79: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, 7/05, http://www.csrc.nist.gov/piv-project/publications/sp800-79.pdf.

[5] The National Agency Checks are the Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check. The National Agency Check with Written Inquiries includes all of the National Agency Checks plus searches of records covering specific areas of an individual's background during the past five years.

[6] Section 2.2 of the Standard has been revised to clarify for the initial credential issuance, only the fingerprint check must be completed.

C. **Include language implementing the Standard in applicable new contracts.** All new contracts (including exercised options) requiring contractors (as defined in 1.C. above) to have long term access to federally controlled facilities or access to federally controlled information systems shall include a requirement to comply with the Directive and Standard for affected contractor personnel. Agencies must comply with the forthcoming Federal Acquisition Regulation sections on these requirements.

For current employees, contractors and other applicable individuals, your department or agency must by October 27, 2005:

D. **For current employees,** develop a plan and begin the required background investigations for all current employees who do not have an initiated or successfully adjudicated investigation (i.e., "completed National Agency Check with Written Inquires or other Office of Personnel Management [OPM] or National Security community investigation") on record. By October 27, 2007 verify and/or complete background investigations for all current employees.

At card renewal (every 5 years), the NACI requirements should be followed in accordance with OPM guidance. Currently OPM does not have a requirement to reinvestigate employees, not otherwise subject to an investigation (e.g. for a security clearance).

For individuals who have been Federal department or agency employees over 15 years, a new investigation may be delayed, commensurate with risk, but must be completed no later than October 27, 2008.

E. **For current contractors and other applicable individuals,** develop a plan and begin the required background investigations for all current contractors who do not have a successfully adjudicated investigation on record. Phase in this requirement to coincide with the contract renewal cycle, but no later than October 27, 2007.

4. How should I implement Part 2 of the Standard?

By October 27, 2006, all departments and agencies must begin deploying products and operational systems meeting these requirements:

A. **Issue and require the use of identity credentials for all new employees and contractors,** compliant with Parts 1 and Part 2 of the Standard. For current employees and contractors, phase in issuance and use of identity credentials meeting the Standard to end no later than October 27, 2007.

B. **Implement the technical requirements of the Standard** in the areas of personal authentication, access controls and card management, consistent with the Standard (i.e. sections 3, 4, and 5) and NIST Special Publication 800-73.[7]

C. **Risk Based Facility Access –** Use the appropriate card authentication mechanism described in section 6 of the Standard, with minimal reliance on visual authentication to the maximum extent practicable (section 6.2.1). Officials who control access shall determine the appropriate mechanism based on risk determinations.

D. **Use of Digital Certificates –** Compliance with the Standard requires the activation of at least one digital certificate on the identity credential for access control. This digital certificate (and any optional digital certificates on the identity credential) must originate from:

1) An agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher by December 31, 2005; or

2) An approved Shared Service Provider.[8]

Agencies must require the use of the identity credential for system access. Prioritize this requirement based on risk, using your authentication risk assessments required by previous OMB guidance and the categorization required by FIPS 199.[9] Document the results and make available to your Chief Information Officer, security office and Inspector General's Office upon request.

You are already required to have rules of behavior in place (including the consequences for violation) before employees and contractors are granted access to systems.[10] All employees and contractors must have access to this documentation.

5. What acquisition services are available?

A. **Requirement to use federally approved products and services –** To ensure government-wide interoperability, all departments and agencies must acquire products and services that are approved to be compliant with the Standard and included on the approved products list. A forthcoming Federal Acquisition Regulation will require the use of only approved products and services.

---

[7] NIST Special Publication 800-73: Integrated Circuit Card for Personal Identity Verification, 4/8/05, http://www.csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf.

[8] OMB Memorandum M-05-05: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services, 12/20/04, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf.

[9] OMB Memorandum M-04-04: E-Authentication Guidance for Federal Agencies, 12/16/03, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf and FIPS 199: Standards for Security Categorization for Federal Information and Information Systems, 2/04, http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[10] See OMB Circular A-130 at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

B. **Use of GSA Acquisition Services –** GSA has been designated as the "executive agent for Government-wide acquisitions of information technology" under section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. § 11302(e)) for the products and services required by the Directive. GSA will report to OMB annually on the activities undertaken as an executive agent.

   GSA will make approved products and services available through blanket purchase agreements (BPA) under Federal Supply Schedule 70 for Information Technology, a schedule under the Multiple Award Schedules (MAS) Program. When developing BPAs, GSA will ensure all approved suppliers provide products and services that meet all applicable federal standards and requirements.

   Departments and agencies are encouraged to use the acquisition services provided by GSA. Any agency making procurements outside of GSA vehicles for approved products must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components.

C. **Sponsorship –** For small departments and agencies and agencies who share facilities with another agency it may not be cost effective to procure your own products or services. GSA will identify agency sponsors who will provide a range of services to agencies. The extent and cost of services to be provided will be determined by agreement between the sponsor and the customer agency.

6. How must I consider privacy in implementing the Directive?

You are already required under the Privacy Act of 1974 (5 U.S.C. § 552a), the E-Government Act of 2002 (44 U.S.C. ch. 36), existing OMB policy and section 2.4 of the Standard to satisfy privacy and security requirements. Implementing the Directive does not alter these requirements. In addition, **prior to identification issuance you must:**

A. Ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a).

B. Assign an individual to be responsible for overseeing the privacy-related matters associated with implementing this Directive.

C. Submit to OMB, and make publicly available, a comprehensive privacy impact assessment (PIA) of your HSPD-12 program, including analysis of the information technology systems used to implement the Directive. The PIA must comply with section 208 of the E-Government Act of 2002 (44 U.S.C. ch. 36) and OMB Memorandum M-03-22 of September 26, 2003, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002." You must periodically review and update the privacy impact assessment. Email your completed PIA to pia@omb.eop.gov.

D. Update the pertinent employee and contractor identification systems of records notices (SORNs) to reflect any changes in the disclosure of information to other Federal agencies (i.e. routine uses), consistent with Privacy Act of 1974 (5 U.S.C. § 552a) and OMB Circular A-130, Appendix 1.[11] These SORNs should be periodically re-reviewed to ensure accuracy.

E. Collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. ch. 35), where applicable. Departments and agencies are encouraged to use Standard Form 85, Office of Personnel Management Questionnaire for Non-Sensitive Positions (OMB No. 3206-0005) or the Standard Form 85P, Office of Personnel Management Questionnaire for Positions of Public Trust (OMB No. 3206-0005) when collecting information. If you plan to collect information from individuals covered by the PRA using a new form you must obtain OMB approval of the collection under the PRA process.

F. Develop, implement and post in multiple locations (e.g., agency intranet site, human resource offices, regional offices, provide at contractor orientation, etc.) your department's or agency's identification privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification credentials are revoked, and sanctions for employees violating agency privacy policies.

G. Adhere to control objectives in section 2.1 of the Standard. Your department or agency may have a wide variety of uses of the credential not intended or anticipated by the Directive. These uses must be appropriately described and justified in your SORN(s) and PIA.

Note: OMB has established a small working group to develop model language for common portions of the SORN, PIAs and Privacy Act Statements for department and agency use when implementing the Directive. These products will be completed no later than October 27, 2005.

7. Is there anything else I must consider or know?

A. **Paragraph 5 of the Directive** asks departments or agencies to "identify those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are **important for security** and for which use of the Standard in circumstances not covered by this Directive should be considered" by August 26, 2005. This determination should be consistent with the privacy requirements specified in question 6 of this guidance and should include any uses of the Standard not meeting the control objectives listed in the Standard. If you have identified other facilities, information systems or applications, submit them to the Assistant to the President for Homeland Security, with an electronic copy to the Office of Management and Budget at eauth@omb.eop.gov.

[11] See http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

B. **Annual Reporting –** The applicability section of the Standard requires annual reporting on the numbers of agency issued credentials, to include the respective numbers of agency-issued 1) general credentials and 2) special-risk credentials (issued under the Special-Risk Security Provision on page v of the Standard). Future OMB guidance will address this requirement.

C. **Biometrics Implementation –** This OMB guidance is being issued before finalization of NIST Special Publication 800-76: Biometric Data Specifications for Personal Identity Verification. Agencies may defer the capture of biometrics for the identity credential until the NIST guidance is final.

D. **Employees Serving Undercover –** Agencies with employees who serve undercover shall implement this Directive in a manner consistent with maintenance of the cover, and to the extent consistent with applicable law and policy.

E. **Relationship to Personnel Security Clearances –**The directive reaffirms the existing requirement, first enumerated in Executive Order 10450 of April 27, 1953 to conduct background investigations on all Federal employees. This investigation is used to determine suitability. Thus, the investigation required by the directive is not the same as the investigations required for personnel security clearances or for public trust determinations. The issuance of a security clearance is a discrete privilege and should be done in accordance with applicable standards. Personnel security investigations for the purpose of issuing security clearances or for the purpose of making public trust determinations can be sufficient for the required background investigations required by the directive.

F. **Applying guidance to temporary employees and contractors –** The requirements for temporary employees and contractors should be viewed as the minimum requirements, dependent on risk and other factors. Agencies who employ temporary personnel (e.g. contract employment under special arrangements with schools, businesses, state and local governments, etc.) should apply this guidance as follows:

- **Employed greater than 6 months –** Apply all sections of this guidance, including the background investigation requirements in the Standard (e.g. "completed National Agency Check with Written Inquires [NACI] or other Office of Personnel Management or National Security community investigation").

- **Employed 6 months or less**
  a) Apply adequate controls to systems and facilities (i.e. ensuring temporary staff has limited/controlled access to facilities and information systems).
  b) Provide temporary employees and contractors with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems.
  c) Document any security violations involving these employees, and report them to the appropriate authority within 24 hours.

d) Identity credentials issued to these individuals must be visually and electronically distinguishable from identity credentials issued to individuals to whom the Standard does apply. Agencies should be careful not to develop policies which overlap or contradict the Standard's processes for identity proofing and issuance.

- **Occasional visitors**
  a) Apply adequate controls to systems and facilities (i.e. ensuring visitors have limited/controlled access to facilities and information systems).
  b) Develop agency-specific visitor policies (as appropriate).

Attachment B

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-12

August 27, 2004

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b) (2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

# # #

EXHIBIT D

NASA Procedural Requirements

NPR 1600.1
Effective Date: November 03, 2004
Expiration Date: November 03, 2009

COMPLIANCE IS MANDATORY

NASA Security Program Procedural Requirements w/Change 1 (11/08/2005)

Responsible Office: Office of Security & Program Protection

NASA Interim Directive: Security Identification System Requirements, NM 1600-46

Preface

P.1. Purpose

a. This NASA Procedural Requirements (NPR) establishes Agency-wide security program implementation requirements set forth in NASA Security Policy Directive (NPD) 1600.2, as amended.
b. This NPR prescribes NASA Security Program procedural requirements to assist NASA Centers and component facilities in executing the NASA security program to protect people, property, and information. It establishes security program standards and specifications necessary to achieve Agency-wide security program consistency and uniformity, while allowing for reasonable flexibility in implementing risk management principles, where appropriate. It also provides for the assignment of management security responsibilities.

P.2. Applicability

This NPR is applicable to NASA Headquarters and all NASA Centers including Component Facilities, the Jet Propulsion Laboratory (JPL) and other NASA Contractors, grant recipients, and other partners to the extent specified in their contracts or agreements.

P.3. Authority

42 U.S.C. 2455, 2456, 2456a, and 2473(c) - - Sections 304 and 203(c), respectively, of the National Aeronautics and Space Act of 1958.

P.4. References

a. 5 U.S.C. 552, (b)(1)-(9), Exemptions, Freedom of Information Act (FOIA).
b. 5 U.S.C. 7312, Employment and clearance, individuals removed for reasons of national security.
c. 5 U.S.C. 7511, Definitions; Application.
d. 5 U.S.C. 7512, Actions covered.
e. 5 U.S.C. 7532, Suspension and Removal.
f. 18 U.S.C. 799 Violation of Regulations of National Aeronautics and Space Administration.
g. 40 U.S.C. 1441, et seq., Computer Security Act of 1987, as amended.
h. 42 U.S.C. 13041, Child Care Worker Employee Background Checks.
i. 50 U.S.C. 435, Access to Classified Information - Procedures.
j. EO 10450, Security Requirements for Government Employees, as amended.
k. EO 12356, National Security Information, as amended.
l. EO 12829, National Industrial Security Program, as amended.
m. EO 12958, Classified National Security Information, as amended.
n. EO 12968, Access to Classified Information, as amended.
o. 5 CFR Part 731, Suitability
p. 5 CFR Part 732, National Security Positions
q. 14 CFR, Parts 1203, 1204, and 1214.
r. 22 CFR Parts 120-130, International Traffic in Arms Regulations (ITAR).
s. 32 CFR 2001, Classified National Security Information.
t. Security Policy Board (SPB) Issuance 1-97, Investigative Standards, 3/24/97.
u. SPB Issuance 2-97, Adjudicative Guidelines, 3/24/97.
v. SPB Issuance 3-97, Investigative Standards for Temporary Eligibility for Access.
w. National Security Directive (NSD) 63, Single Scope Reliability Investigation.
x. OMB Circular A-130, Security of Federal Automated Information Resources, (Appendix III).

y. Director, Central Intelligence, Directive (DCID 6/9), Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFS), November 18, 2002.
z. National Security Decision Directive (NSDD) 84, Safeguarding National Security Information (Nondisclosure Agreement), 3/11/83.
aa. NSDD-145, National Policy on Telecommunications and Automated Information Systems Security, 9/17/84.
bb. FIPS 201, Federal Information Processing Standards, "Personnel Identity Verification (PIV) of Federal Employees and Contractors."
cc. NSDD 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, 9/21/85
dd. NSDD-298, National Operational Security Program, 1/22/88.
ee. DoD-56, MOU, Defense Investigative Service and NASA, Kennedy Space Center, 5/07/87, as regards the Industrial Security Program.
ff. DoD-86, MOU, Defense Investigative Service and NASA, 12/17/90, as regards access to Defense Clearance and Investigative Index (DCII) and Larsen System.
gg. DOT/ Federal Arrest Authority, AC 108-3, Screening of Persons Carrying U.S. Classified Material.
hh. Presidential Decision Directive (PDD) 39, Counterterrorism Policy.
ii. PDD 62, Combating Terrorism.
jj. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.
kk. PDD 67, Enduring Constitutional Government and Continuity of Government.
ll. HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors
mm. Department of Justice (DOJ) Report, Vulnerability Assessment of Federal Facilities, June 1995.
nn. General Accounting Office Report (GAO-03-8), Security Responsibilities for Federally Owned and Leased Facilities, October 2002.
oo. NPD 1371.5, Coordination and Authorization of Access by Foreign Nationals and Foreign Representatives to NASA.
pp. NPD 1440.6, NASA Records Management.
qq. NPD 1660.1, NASA Counterintelligence (CI) Policy.
rr. NPD 1600.2, NASA Security Policy.
ss. NPD 2190.1, NASA Export Control Program.
tt. NPD 2810.1C, NASA Information Security Policy.
uu. NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities.
vv. NPR 1441.1, NASA Records Retention Schedules.
ww. NPR 1600.6, Communications Security Procedural Requirements.
xx. NPR 2190.1, NASA Export Control Program.
yy. NPR 2810.1, Security of Information Technology.
zz. NPD 9800.1, NASA Office of Inspector General Programs.

P.5. Cancellation

NPR 1620.1A, Security Procedural Requirements--w/Change 2

NPD 1620.2, NASA Badging System

/S/
David A. Saleeba
Assistant Administrator for Security and Program Protection

Chapter 1: Introduction

1.1 Security Responsibilities

1.1.1. The NASA Administrator is responsible for implementing a comprehensive and effective security program for the protection of people, property, and information associated with the NASA mission. The Administrator shall appoint an Assistant Administrator for Security and Program Protection (AA/OSPP).

1.1.2. Security is the direct, immediate, and inherent responsibility of all NASA personnel, contractors, and others granted access to NASA Centers, facilities, information and technology. General security responsibilities are set forth in this chapter. Specific procedural requirements are cited in each subsequent chapter of this NPR.

1.1.3. The AA/OSPP shall:

1.1.3.1. Oversee Agencywide implementation, integration of, and compliance with the NASA Security Program by providing executive management policy direction and ensuring, through Agencywide advocacy, adequate resources are identified and committed to accomplish the security mission in support of the overall NASA mission, NASA Strategic Plan, and National level security requirements.

1.1.3.2. In collaboration with the Chief Information Officer (CIO), develop and implement Agency Information Technology Security policy via NPD 2810 and NPR 2810, and serve as the Agency Certification and Accreditation (C&A) authority for NASA IT.

1.1.3.3. Serve as the Agency Risk Acceptance Authority (RAA) for all NASA Security Program risk management determinations that require a waiver of Agency security requirements. This does not include IT Security RAA, which falls under the CIO.

1.1.3.4. Develop and implement a program to ensure certification and accreditation of Information Technology (IT) resources identified for processing classified national security information (CNSI) and data.

1.1.3.5. Serve as the focal point for Agency Special Access Program (SAP) and Sensitive Compartmented Information (SCI) security activity.

1.1.3.6. Serve as the Agency point of contact with the intelligence community for intelligence matters and ensure development and issuance of policy and requirements related to NASA's counterintelligence program.

1.1.3.7. Ensure law enforcement and investigative activity performed in conjunction with OSPP security responsibilities at NASA installations is developed and implemented consistent with authorities granted under the Space Act, and in concert with the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.3.8. Appoint a qualified senior security professional as Director, Security Management Division (DSMD).

1.1.3.9. Serve as the Agency Critical Infrastructure Assurance Officer (CIAO) responsible for approving all Center proposals for additions and deletions to the Mission Essential Infrastructure (MEI) Inventory List when such proposals are concurred on by the respective Mission Directorate Associate Administrator.

a. Comply with the requirements of Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.
b. Effectively collaborate with the CIO to ensure critical cyber assets are identified and included in the Mission Essential Infrastructure (MEI) inventory, as appropriate.

1.1.3.10. Establish and implement organizational standards that ensures NASA security programs are appropriately configured, properly staffed with qualified security professionals, and adequately funded to enable each NASA Center

to properly and efficiently manage day-to-day security operations while allowing for transition to increased threat environments and emergency scenarios, including appropriate continuity of operations capabilities.

1.1.3.11. Develop and issue, under separate NPR, asset specific physical security vulnerability risk assessment requirements and physical and procedural security standards to ensure consistency and uniformity in application of security measures appropriate for the vulnerabilities identified.

1.1.3.12. Establish and disseminate staffing, equipment, training, and performance standards for security services contractor organizations to ensure security services obtained are professional, comprehensive, uniform, and consistent with NASA requirements.

1.1.3.13. Develop and disseminate Agency antiterrorism program standards and procedures necessary to ensure appropriate response to threats and acts of terrorism on NASA installations and component facilities.

1.1.3.14. Implement and manage procedures for certifying and obtaining accreditation of IT resources that process CNSI and data.

1.1.3.15. In coordination with the NASA Office of General Counsel, ensure development and dissemination of appropriate policy and procedures regarding use and deployment of covert surveillance equipment (CCTV, etc.).

1.1.3.16. Develop and issue interim policy and procedural requirements as necessary to address specific issues.

1.1.4. The NASA CIO is responsible for the NASA-wide Information Technology Security (ITS) program, and shall:

1.1.4.1. Provide advice and assistance to the Administrator and other Senior Management Officials to ensure that Agency ITS goals, priorities, and requirements are effectively and efficiently addressed to protect the Agency's investment in Information Technology (IT).

1.1.4.2. Develop and implement NASA IT Security policy via the issuance of IT Security Procedural Requirements, architectures, standards, and best practices. This includes common security classification schema, which contribute to open, standard, scaleable, interoperable, yet secure IT environments and assess, with the assistance of the Competency Center for ITS, the state of the Agency's ITS posture, and the effectiveness of its IT Security policies.

1.1.4.3. Except as noted in subsection 1.1.5 below, appoint Agency representatives to Federal groups concerned with ITS.

1.1.4.4. Appoint a Competency Center for IT Security (CCITS) responsible for developing ITS architectures, standards, and best practices for the Agency on behalf of the NASA CIO.

1.1.5. Director, Security Management Division (DSMD) shall:

1.1.5.1. Provide overall focus and direction for the NASA security program.

1.1.5.2. Serve as the Agency oversight official for implementation and management of the Agency Federal Arrest Authority Program and Use of Force policy in compliance with 42 U.S.C. 2456a, and 14 CFR part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

1.1.5.3. Develop and implement Agencywide policy and procedural requirements to ensure investigation activity is coordinated and/or referred to the local Office of Inspector General, local, State, and Federal law enforcement agencies, as appropriate.

1.1.5.4. Establish and maintain a Central Adjudication Activity at the Headquarters level charged with adjudicating all Agency requests for security clearances for access to CNSI.

1.1.5.5. Deny or revoke security clearances in accordance with the provisions of EO 12968 in strict accordance with due process.

1.1.5.6. Develop and promulgate, subject to coordination with and concurrence by the Office of the General Counsel (OGC), all NASA security policy and procedures.

1.1.5.7. Through periodic site visits, evaluate compliance with this NPR and overall effectiveness of the NASA security program, including effectiveness of NASA IT Security policy and procedures.

1.1.5.8. Manage the Mission Essential Infrastructure Protection Program (MEIPP).

1.1.5.9. Serve as the Senior Agency Official for implementing procedures for managing and safeguarding CNSI.

1.1.5.10. Ensure that the NASA security program operates in compliance with National security policy, homeland security program directives, and other National level regulations.

1.1.5.11. Coordinate, as appropriate, with the Office of the Chief Medical Officer on all matters related to the Mission Critical Space Systems Personnel Reliability Program screening process requiring evaluations and medical determinations from NASA or outside medical authorities.

1.1.5.12. Ensure appropriate physical security and antiterrorism construction standards are developed and published in cooperation with NASA Facilities Engineering Division personnel.

1.1.5.13. Serve as the focal point for NASA representation on all security and national security policy development forums and committees.

1.1.6. Center Directors shall:

1.1.6.1. Provide current and effective security of personnel, property, facilities, operations, and activities at NASA Centers.

1.1.6.2. Ensure the development and management, through the Center Chief of Security (CCS), of written Center specific security program policy and procedural requirements that implement, to the fullest extent possible, the requirements of this NPR.

1.1.6.3. Appoint, with coordination and concurrence of the AA/OSPP, a qualified and experienced CCS with sufficient authority and resources to accomplish National, Agency, and Center security goals and objectives. Minimum qualifications include:

a. Relevant experience in the law enforcement, military intelligence, or security professions.
b. Leadership and managerial experience at a proven level commensurate with the expectations of the CCS position.
c. Ability to obtain and maintain a Top Secret security clearance.

1.1.6.4. In accordance with this NPR, establish, fund, and maintain a comprehensive security program through the CCS. This includes:

a. Personnel, facilities, and equipment necessary to implement and sustain an effective security program.
b. Appropriate training and professional certification of security personnel, as established by the AA/OSPP.

1.1.6.5. When recommended by the CCS and Center CIAO, propose, as appropriate, Critical Infrastructure (CI) and Key Resource (KR) assets for inclusion in the Mission Essential Infrastructure (MEI) Inventory, to the Mission Directorate Associate Administrator.

1.1.6.6. Act as the Risk Acceptance Authority (RAA) for Center security program risk management determinations that do not require waiver of national security requirements.

1.1.6.7. Grant or suspend eligibility for security clearances up to and including Top Secret, with proper coordination with the NASA Central Adjudication Activity. This authority shall be delegated, in writing, to the CCS.

1.1.6.8. Appoint, in writing, a Certifying Authority (CA) responsible for certifying to the Agency Designated Approval Authority (DAA), Center IT resources identified to process classified information.

1.1.7. The CCS shall:

1.1.7.1. Act as the principal advisor and authority to the Center Director in all matters relating to the NASA security program, as established and defined in NPD 1600.2C.

1.1.7.2. With coordination and concurrence of the AA/OSPP, ensure that the Center Security Office is appropriately staffed with qualified and experienced security personnel.

1.1.7.3. To ensure continuity of operations capability, establish the necessary processes and procedures to cross-train staff into other disciplines of the Center's security program, as practical.

1.1.7.4. Develop, implement, and maintain written Center-specific security program policy and security procedural requirements that implement the requirements of this NPR.

1.1.7.5. Direct, plan, control, and evaluate the overall Center security program, regardless of the specific security discipline and processes involved.

1.1.7.6. Through periodic assessments, determine the adequacy of physical security, loss prevention, and antiterrorism programs and recommend improvements to the Center Director.

1.1.7.7. Using all available sources of intelligence information (i.e., NASA CI Program, Local Law Enforcement, NASA Office of Inspector General (OIG), other Federal agencies), continuously evaluate Center and program-level criticality and vulnerabilities, local threats, and prepare appropriate countermeasures tailored to the resources requiring protection, specifically identifying Center Critical Infrastructure and Key Resources, in coordination with the Center CIO and CIAO, for inclusion in the MEI Protection Program.

1.1.7.8. Establish priorities for the effective deployment of Center security resources and processes during routine and emergency situations.

1.1.7.9. Direct and control Center investigative efforts related to NASA security program operations. Ensure appropriate notifications and referrals to local and supporting Federal law enforcement agencies and the NASA OIG are conducted in accordance with this NPR and established formal agreements. [NOTE: Investigations conducted under NPR 1660, NASA Counterintelligence Program Procedural Requirements, are excluded from the requirements of this NPR.]

1.1.7.10. Exercise Original Classification Authority (OCA).

1.1.7.11. Upon written approval by the AA/OSPP, perform duties as the Center Declassification Authority for all Center declassification and classification downgrading activity, as required. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management. With written approval from the AA/OSPP, the CCS may delegate this authority to qualified subject matter experts cleared to the appropriate level and properly trained in classification management.

1.1.7.12. Initiate the appropriate personnel security investigation and grant interim security clearances up to and including Top Secret, based on information contained in the investigative request, and grant final clearance upon notification from the NASA CAF that an individual has been adjudicated and determined eligible for the clearance requested or suspend security clearances on behalf of the Center Director and the AA/OSPP.

1.1.7.13. Designate a Center Personnel Security Officer who shall:

a. Properly adjudicate all requests for interim clearances per chapter 2.
b. Properly determine contractor employee security reliability per chapter 4.
c. Successfully complete a minimum of two specified personnel security adjudication courses prior to conducting adjudications and maintain current qualifications.
d. Ensure that designated Senior Adjudicators successfully complete three specified personnel security adjudication courses, one of which must be an advanced adjudicator's course, and maintain current qualifications.

1.1.7.14. Ensure Federal Arrest Authority is properly administered at their respective Center and act as the Center Certifying Official for the authority to carry and use concealed or unconcealed firearms by security forces, both NASA civil service personnel and contractor.

1.1.7.15. Notify the OIG of all suspected criminal activity, when appropriate.

1.1.7.16. Integrate and maintain oversight of all Center security activity, including those of tenant organizations to the extent practical.

1.1.7.17. Ensure appropriate training and professional certifications for security staff and armed security force personnel, commensurate with their assigned tasks, weapons, and equipment, as established by the AA/OSPP.

1.1.7.18. Act as the Center Director's primary staff advisor during any security-related crisis or serious incident and as primary point of contact with all external Law Enforcement agencies.

1.1.7.19. Establish and maintain annual security awareness and training programs for Center employees.

1.1.7.20. Participate as a principal member of Center teams dealing with resolution of workplace violence and protection issues.

1.1.7.21. Serve as a member of property survey boards.

1.1.7.22. Maintain a Center map of the precise jurisdictional boundaries of Center geographical areas, as determined by the Chief Counsel.

1.1.7.23. Develop and maintain personnel identification programs in accordance with established requirements.

1.1.7.24. Provide operational support to the NASA counterintelligence (CI) program, as appropriate.

1.1.7.25. Participate in all facility design reviews and on Center Master Planning Committees to ensure facility physical security and antiterrorism design criteria are appropriately incorporated into individual facility designs and Center Master Plans.

1.1.7.26. Maintain Center security program statistics and provide quarterly reports to the DSMD under the standards set forth in Appendix L.

1.1.7.27. Establish and maintain all organization informational and operational files pursuant to NPD 1440.6G, NASA Records Management and NPR 1441.1D, NASA Records Retention Schedules.

1.1.7.28. Designate, with coordination and concurrence of the AA/OSPP, a qualified and experienced Center Information Assurance Officer (IAO) who shall:

a. Have relevant experience in IT security and information assurance. Note: Having at least one of the following certifications is highly desired:
(1). Information Systems Audit and Control Association (ISACA) as a Certified Information Security Manager (CISM) or Certified Information Systems Auditor (CISA)
(2). International Information Systems Security Certification Consortium (ISC)2 Certified Information System Security Professional (CISSP)

b. Leadership and communication experience at a proven level commensurate with the expectations of the CIAO position.

c. Ability to obtain and maintain a Top Secret security clearance.

d. Fulfill the specific roles and responsibities for a CIAO described in NPR 2810.1.

e. Support Center Security Offices in certification, auditing, and inspection of unclassified IT systems

f. Support Center Security Offices in investigations of IT security incidents as appropriate. [Note: Center IAOs will not possess federal arrest authority credentials and will not be designated as investigators.]

g. Not have concurrent duties as part of the Center IT security staff.

1.1.8. Program, Line Managers, and Supervisors shall:

1.1.8.1. Support the CCS in the implementation of comprehensive security programs and mission-oriented protective services for the Center, along with individual programs and projects.

1.1.8.2. Effectively manage the level of "cleared" personnel and immediately advise the CCS of any changes in the requirements for access to classified national security information or eligibility for security clearance.

1.1.8.3. Employ CCS recommended security and loss-prevention measures within their programs or organizations.

1.1.8.4. In coordination with the CCS, employ Systems Security Engineering processes at program inception and throughout the individual program life cycle as necessary to ensure appropriate protection and accountability of program resources.

1.1.9. The Center CIO shall:

1.1.9.1. Ensure implementation of IT Security policies and develop and implement local IT Security Procedural Requirements, as deemed appropriate.

1.1.9.2. Coordinate with and support the CCS in the protection of classified and unclassified but sensitive information residing on automated systems.

1.1.9.3. Report IT security incidents to the CCS to ensure appropriate action and necessary referral is effected.

1.1.9.4. Provide technical assistance during investigations as requested by the CCS.

1.1.10. Individual employees shall:

1.1.10.1. Report suspicious activity, criminal activity, violations of national security, and other Center security responsibilities to the Security Office.

1.1.10.2. Be aware of and comply with individual responsibilities and roles in maintaining the Agency and Center security program.

1.1.10.3. Protect Government property, CNSI, and sensitive information in accordance with the requirements of this NPR.

1.1.10.4. Cooperate with Center and Agency Security Officials during inquiries and investigations.

1.1.11. The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel with regard to implementation of this NPR, as appropriate.

1.2 Best Practices

1.2.1. This NPR seeks to establish uniform security program standards across NASA. One way in which to accomplish "standardization" is to develop, implement, qualify, and share "Best Practices." "Best Practices" serves as a model for other NASA security organizations to learn and, where possible, benefit through adoption for use in improving or enhancing their security program. "Best Practices" occur inside and outside the NASA family, in Government or private industry.

1.2.2. The DSMD and CCS shall develop and share "Best Practices" programs and processes, where appropriate.

1.3 Waivers and Exceptions

1.3.1. Centers may occasionally experience difficulty in meeting specific requirements established in the series of NASA Security Program NPRs. The process for submitting requests for waivers or exceptions to specific elements of the NASA Security Program is as follows:

1.3.1.1. The asset, program, or project manager and CCS shall justify the waiver request through security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; inability of the CCS to perform its missions and goals, etc. (a) Justification must also include an explanation of any compensatory security measures implemented in lieu of specific requirements. (b) The waiver request shall be submitted to the Center Director.

1.3.1.2. The Center Director shall either recommend approval or return the waiver request to the CCS for further study or closure. The Center Director shall forward concurrence to the Center's Mission Directorate Associate Administrator.

1.3.1.3. The Mission Directorate Associate Administrator shall forward waiver requests to the Assistant Administrator for Security and Program Protection (AA/OSPP) at Headquarters or return proposals to the Center Director for further study or closure.

1.3.1.4. The AA/OSPP shall return the waiver request to the appropriate Center Director with an approved waiver, for further study, or denial and closure.

1.4 Violations of Security Requirements

1.4.1. Center Directors, Headquarters Operations Director, the AA/OSPP, the DSMD, or the CCS, shall order the removal or debarment of any person who violates NASA Security requirements or whose continued presence on NASA property constitutes a security or safety risk to persons or property. Any determinations to reconsider granting access subsequent to the removal action must receive the concurrence, in writing, of the AA/OSPP.

1.4.2. Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA Security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. 799, that provides for fines or imprisonment for not more than 1 year, or both.

1.5 Terms, Abbreviations, and Acronyms

Terms, Abbreviations, and Acronyms used throughout the family of NASA Security program NPRs are defined in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms."

Chapter 2: NASA PERSONNEL SECURITY PROGRAM: REQUIREMENTS , INVESTIGATIONS , AND ADJUDICATION PROCESS FOR POSITIONS (NATIONAL SECURITY POSITIONS) REQUIRING ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI)

2.1 General

2.1.1. Title 5 Code of Federal Regulations (CFR), Part 732, National Security Positions, requires each agency to follow established procedures to identify national security positions. Positions identified by this process within the National Aeronautics and Space Administration (NASA) require regular use of or access to classified information. This chapter addresses the sensitivity designation program associated only with national security, the criteria for determining national security sensitivity levels, and screening (i.e., the type of investigation) required under Executive Order (E.O.) 10450, Security Requirements for Government Employment, and E.O. 12968, Access to Classified Information.

2.1.2. This chapter does not address other aspects of the position risk designation program which include Personnel Suitability described in Title 5 CFR, OPM Part 731, Suitability; HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors , and Federal Information Processing Standards (FIPS) 201, "Personnel Identity Verification (PIV) of Federal Employees and Contractors," Automated Information System Security defined in the Office of Management and Budget (OMB) Circular A-130; and numerous laws.

a. These programs, outlined in chapters 3 and 4 respectively, require a determination of a position's risk level (i.e., Low Risk, Moderate Risk, or High Risk) using criteria that are separate and distinct from the national security criteria. Designation of position risk level must occur prior to establishment of sensitivity level. See Appendix M.

b. Information regarding Personnel Suitability may be obtained from the Office of Human Resources.

c. NPR 2810.10, NASA Automated Information Systems Security, establishes the policy, assigns responsibilities, and prescribes standards and procedures for the management of the Information Technology (IT) security program for NASA

2.1.3. Position sensitivity designation is based on an assessment of the degree of damage that an individual, by virtue of the occupancy of a national security position, could cause to the national security.

2.1.4. Investigations are conducted to provide a basis for ensuring that the granting of a security clearance to an individual is clearly consistent with the interests of national security.

2.1.5. Personnel security reports and records shall be handled in accordance with the Privacy Act of 1974.

2.1.6. The Office of Personnel Management (OPM) conducts a range of investigations that satisfy the various requirements for the three position-sensitivity levels described in this chapter, as they relate to accessing CNSI.

2.1.7. NASA Contracts requiring the generation of and/or access to CNSI will be processed and individuals investigated in accordance with the requirements established in chapter 6 of this NPR, and the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

2.2 Scope

2.2.1. This chapter prescribes the procedures whereby employees are selected, processed, investigated, and adjudicated for national security positions, consistent with U.S. Security Policy Board (SPB) Procedures contained in SPB Issuance 1-97, SPB Issuance 2-97, and SPB Issuance 3-97.

2.2.2. This chapter does not apply to contractor personnel providing services under a NASA classified contract that requires access to CNSI. Refer to chapter 6, "Industrial Security," for requirements on NASA classified contract processes and procedures.

2.3 Responsibilities

2.3.1. The DSMD shall establish a Central Adjudication Facility (CAF) at the Headquarters level responsible for adjudicating all investigative results for security clearances for access to CNSI. The CAF shall process and manage all requests for security clearance, adjudicate all investigative results, grant clearance eligibility, and deny, revoke, or suspend security clearances in accordance with the provisions of EO 12968 due process considerations.

2.3.2. Center Directors shall ensure the CCS manages the Center personnel security program in accordance with this NPR.

2.3.3. The CCS shall:

2.3.3.1. Process security clearances for employees under their jurisdiction, subject to the eligibility standards set forth in this chapter.

2.3.3.2. Ensure only the on-line e-QIP version of the SF 86 is used when it becomes available.

2.3.3.3. Grant a NASA employee a security clearance or suspend an employee's clearance for cause.

2.3.3.4. Delegate these responsibilities to a senior personnel security specialist who is a civil service employee, who has attended a recognized Personnel Security Suitability and Security Adjudication course, and who has maintained currency in that field.

2.3.3.5. In cooperation with Center Human Resources Organizations, management, and supervisory personnel, implement these procedures for appropriate designation of National Security position sensitivity, per section 2.7, for all existing and newly established positions whose duties clearly reflect the requirement for a security clearance and access to CNSI, in accordance with the requirements set forth in this chapter. This collaborative approach is essential if NASA is to effectively comply with established national security position sensitivity designation requirements outlined in 5 CFR 732.101 - 732.401 and the requirements of EO 12968.

2.3.4. Center Human Resources Organizations shall:

2.3.4.1. Ensure that position descriptions are developed by the appropriate management and supervisory personnel, and that they accurately reflect National Security position sensitivity and establishes clear requirements for access to CNSI, as required under 5 CFR 732.101 - 732.401 and EO 12968.

2.3.4.2. Ensure no recruitment, hiring, or change of position action takes place until the appropriate position sensitivity level and risk designation has been established.

2.3.4.3. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this chapter.

2.3.5. Program, line managers, and supervisors shall ensure full compliance with the requirements established in this chapter.

2.4 Personnel Security Program Oversight

As part of its responsibility for the functional management of the NASA Security Program, the DSMD shall include personnel security program matters in periodic audits of Center security programs.

2.5 Basic Principles of Personnel Security Clearance Management

2.5.1. EO 12958, Classified National Security Information, clearly emphasizes the requirement to establish procedures to prevent unnecessary access to classified information, including procedures that require that a demonstrable need for