U.S. Consumer Product Safety Commission
Personal Identity Verification and Credential Issuance Process

Effective Date: October 27, 2005

Summary:

This CPSC Policy provides guidelines and clarifies procedures for initiating, preparing, issuing, maintaining, and managing the Personal Identity Verification (PIV) system for CPSC **Federal** employees and **contractors** required by Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.

Implementation of the PIV system at the CPSC will be accomplished in two phases; PIV-1 which includes personal identity proofing, registration, and issuance of credentials that are physically compliant with applicable Standards, and PIV-II which includes interoperability of credentials among Federal departments and agencies. Sections of this Policy that are annotated as being PIV-II requirements are not required to be completed until implementation of PIV-II has been completed.

References:

1) COMMON, X.509 *Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 2.0, November 1, 2004.

2) Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

3) Federal Information Processing Standards Publication, FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, February 25, 2005.

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

5) OMB Form I-9, OMB No. 1615-0047, *Employment Eligibility Verification*, May 31, 2005.

6) The Privacy Act, *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

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

8) SP800-53, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, September 2004.

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

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

11) SP800-76, NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, February 2005.

12) SP800-78 NIST Special Publication 800-78, *Recommendation for Cryptographic Algorithms and Key Sizes*, February 2005.

Introduction:

Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, directed implementation of a mandatory, Government-wide Standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. HSPD-12 defines that "secure and reliable forms of identification" means identification that is based on sound criteria for verifying an individual employee's identity; is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; uses electronic methods of rapid authentication; and is issued only by providers whose reliability has been established by an official accreditation process.

The overall goal of HSPD-12 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.

Federal Information Processing Standards Publication, FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated February 25, 2005, establishes the detailed requirements necessary for implementing HSPD-12. The requirements in FIPS PUB 201 are applicable to identification issued by all Federal departments and agencies for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems, except for "national security systems" as defined by 44 U.S.C. 3542(b)(2).

FIPS PUB 201 consists of two parts, PIV-I and PIV-II. PIV-I describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration and issuance. PIV-II provides detailed technical specifications to support the control and

security objectives of PIV-I as well as the interoperability among Federal departments and agencies.

The physical credential characteristics, storage media, and data elements that make up PIV credentials are specified in FIPS PUB 201. FIPS PUB 201 specifies implementation and use of identity credentials on integrated circuit cards for use in a Federal personal identity verification system and that PIV credentials must be personalized with identity information for the individual to whom the PIV credential is issued in order to perform identity verification by humans and automated systems.

Per the Federal Information Security Act of 2002, waivers to Federal Information Processing Standards are not allowed.

This Policy applies to:

- All Federal employees.
- Individuals employed by, detailed to or assigned to the agency.
- Contractors requiring routine access to federally controlled facilities and/or federally controlled information.
- 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: Occasional visitors to Federal facilities to whom you would issue temporary identification.

Roles and Responsibilities:

Applicant – The individual to whom a CPSC PIV Credential needs to be issued. Upon being issued CPSC PIV Credential the Applicant becomes a **CPSC PIV Credential Holder**.

CPSC HSPD-12 Point of Contact – The individual who acts as the CPSC point of contact with the Assistant to the President for Homeland Security and the Director of OMB for implementing and administering HSPD-12.

CPSC Official Responsible for Logical Security and Access (Office of Information and Technology Services [EXIT]) is responsible for determining the graduated assurance levels for access to CPSC logical resources, and is responsible for obtaining, and making available for use, the hardware and software associated with compliant Federal PIV credentials necessary for accessing CPSC physical resources.

CPSC Official Responsible for Physical Security and Access (EXIT) is responsible for determining the graduated assurance levels for access to CPSC physical resources, and is responsible for obtaining, and making available for use, the hardware and software associated with compliant Federal PIV credentials necessary for accessing CPSC physical resources.

CPSC Official Responsible for PIV Information and Credential Security is responsible for ensuring the required physical and logical characteristics of the CPSC PIV Credential comply with FIPS PUB 201 requirements, and that optional physical and logical characteristics are and included as necessary to enhance flexibility of the credential. This person is responsible for obtaining, and makes available for use, the hardware and software necessary for obtaining (generating or capturing) and placing digital data on compliant Federal PIV credentials. This person is responsible for overseeing security-related matters in the CPSC PIV information system and the CPSC PIV Credential security process, and is responsible for ensuring that the technologies used to implement and sustain the CPSC PIV system are compliant with FIPS PUB 201, SP800-37, SP800-53, SP800-63, SP800-73, SP800-76, and SP800-78. This individual also ensures that the technologies allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the CPSC PIV system.

CPSC PIV Credential System Registry Administrator (Office of Human Resources [EXRM]) is the CPSC individual who maintains administrator access rights to the CPSC PIV system registry, and who is authorized to invalidate CPSC PIV Credentials when a CPSC PIV Credential holder separates, or if a CPSC PIV Credential becomes damaged, lost, or stolen, or some other reason requires invalidation of a previously active CPSC PIV Credential. The CPSC PIV Credential System Registry Administrator shall also maintain a registry for all CPSC PIV Credentials issued, and will establish and maintain a method for monitoring CPSC PIV Credential expiration dates that will provide notification to CPSC PIV Credential Holders **at** least six weeks prior to expiration of their CPSC PIV Credential.

CPSC Senior Official Responsible for Privacy (General Counsel [GC]) – The CPSC individual who oversees privacy-related matters in the CPSC PIV system, and is responsible for implementing the privacy requirements associated with FIPS PUB 201, OMB322, and The Privacy Act. The person serving in this role may not assume any other operational role in the CPSC PIV process.

CPSC PIV Authentication Certification Authority (CA) – The CA that signs and issues the CPSC PIV Authentication Certificate. The CPSC PIV Authentication CA is a CA accredited to issue certificates under the Common Policy as specified in Section 5.4.1 of FIPS PUB 201. This person may be a non-CPSC employee who has been designated to perform this function. (This role only applies for PIV-II.)

CPSC PIV Digital Signatory – The individual who digitally signs the PIV biometrics and Card Holders Unique Identifier (CHUID). This person may be a non-CPSC

employee who has been designated to perform this function. (This role only applies for PIV-II.)

CPSC PIV Issuer (Facilities Support Branch, EXIT [TSFS]) – The individual who personalizes the credential and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The CPSC PIV Issuer is also responsible for maintaining records and controls for CPSC PIV Credential stock to ensure that stock is only used to issue valid credentials. This person may be a non-CPSC employee who has been designated to perform this function.

CPSC PIV Registrar (EXRM) – The individual responsible for identity proofing of the Applicant and ensuring the successful completion of the background check. The CPSC PIV Registrar provides the final approval to the CPSC PIV Issuer for the issuance of a CPSC PIV Credential to the Applicant.

CPSC PIV Sponsor (CPSC Manager/Supervisor) – The CPSC individual who substantiates the need for a CPSC PIV Credential to be issued to the Applicant, and provides sponsorship to the Applicant. The CPSC PIV Sponsor requests the issuance of a CPSC PIV Credential to the Applicant. The CPSC PIV Sponsor is also the individual responsible for remaining aware of Applicant status and the associated continuing need for holding a CPSC PIV Credential. The CPSC PIV Sponsor will inform the Agency CPSC PIV Credential System Registry Administrator when a CPSC PIV Credential holder retires, terminates, or for another reason no longer requires a CPSC PIV Credential.

NOTE: The roles of CPSC PIV Applicant, CPSC PIV Sponsor, CPSC PIV Registrar, and CPSC PIV Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The CPSC PIV Issuer and CPSC PIV Digital Signatory roles may be assumed by one individual or entity.

CPSC Specific Assignment of Roles and Associated Responsibilities

Role	Primary CPSC Individual	Alternate CPSC Individual
CPSC HSPD-12 Point of Contact		
CPSC Official Responsible for Physical Security	EXIT	
CPSC Official Responsible for Logical Security	EXIT	
CPSC Official Responsible for CPSC PIV Information and Credential Security		
CPSC PIV Authentication Certification Authority (May be a non-CPSC employee)		
CPSC PIV Credential System Registry Administrator	EXRM	
CPSC PIV Digital Signatory (May be a non-CPSC employee)		
CPSC PIV Issuer (May be a non-CPSC employee)	TSFS	
CPSC PIV Registrar	EXRM	
CPSC PIV Sponsor	Applicant's Supervisor or COTR	
CPSC Senior Official Responsible for Privacy	GC	

Processes:

CPSC PIV Credential Issuance and Management Subsystem

The role based model for initiating and completing the CPSC PIV Credential issuance process is described in this section, and is implemented by the CPSC Personal Identity Verification Credential Request Form (CPSC Sponsor Form). Another agency or support service contractor may perform some action steps on the CPSC Personal Identity Verification Credential Request Form, but responsibility for maintaining the integrity and security of the CPSC PIV system remains with the CPSC employee assigned responsibility for that aspect of the system. The source document for the CPSC PIV Credential issuance process is FIPS PUB 201, Appendix A.

1. Identity Proofing and Registration of New and Current Employees and Contractors
   This section of the Policy defines a process that uses identity source document inspection and a background check to establish assurance of identity. The process provides the minimal functional and security requirements for achieving a uniform level of assurance for issuing CPSC PIV identity credentials. The identity proofing and registration requirements shall include the following:

   a. The **CPSC PIV Sponsor** shall complete a CPSC PIV Sponsor Form for a particular **Applicant**, and submit the CPSC PIV Sponsor Form to the **CPSC PIV Registrar (EXRM)** and the **CPSC PIV Issuer (TSFS)**. The CPSC PIV Sponsor Form shall include the following:

      - Name, organization, and contact information of the **CPSC PIV Sponsor (Supervisor/COTR)**
      - Name, date of birth, position, and contact information of the **Applicant**
      - Name and contact information of the designated **CPSC PIV Registrar (EXRM)**
      - Name and contact information of the designated **CPSC PIV Issuer (TSFS)**
      - Signature of the **CPSC PIV Sponsor (Supervisor/COTR)**

   b. The **CPSC PIV Registrar (EXRM)** shall confirm the validity of the CPSC PIV Credential Request Form prior to acceptance.

   c. The **Applicant** shall access e-Qip to complete the Standard Form (SF) 85, OPM Questionnaire for Non-Sensitive Positions, or an equivalent, to provide the required background information. The **CPSC PIV Registrar (EXRM)** will initiate the background investigation with the Office of Personnel Management

(OPM) via e-Qip. A Background check is not required for current **CPSC PIV Credential Holders** if the **CPSC Registrar (EXRM)** can verify the completion of the background check with OPM.

d. The **Applicant** shall appear in person and provide two forms of identity source documents in original form to the **CPSC PIV Registrar (EXRM)**. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. List of Acceptable Documents From OMB Form I-9 that establishes identity:

- U.S. Passport (un-expired or expired)
- Certificate of U.S. Citizenship (Form N-560 or N-561)
- Certificate of Naturalization (Form N-550 or N-570)
- Un-expired foreign passport, with I-551 stamp or attached Form I-94 indicating un-expired employment authorization
- Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-551)
- Un-expired Temporary Resident Card (Form I-688)
- Un-expired Employment Authorization Card (Form I-688A)
- Un-expired Reentry Permit (Form I-327)
- Un-expired Refugee Travel Document (Form I-571)
- Un-expired Employment Authorization Document issued by DHS that contains a photograph (Form I-688B)
- Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address
- ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address
- School ID card with a photograph
- Voter's registration card
- U.S. Military card or draft record

- Military dependent's ID card
- U.S. Coast Guard Merchant Mariner Card
- Native American tribal document
- Driver's license issued by a Canadian government authority
- For persons under age 18 who are unable to present a document listed above:
- School record or report card
- Clinic, doctor or hospital record

At least one document shall be a valid State or Federal government-issued picture identification (ID). The **CPSC PIV Registrar (EXRM)** shall visually inspect the identification documents and authenticate them as being genuine and unaltered. In addition, the **CPSC PIV Registrar (EXRM)** 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 **CPSC PIV Registrar (EXRM)** shall use other available tools to authenticate the source and integrity of the identity source documents. The **CPSC PIV Registrar (EXRM)** 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 **CPSC PIV Registrar (EXRM)** 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**.

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

f. The **CPSC PIV Registrar (EXRM)** (or other CPSC employee designated to perform that task) shall capture a facial image of the **Applicant** that conforms to specifications in SP800-76, and retain a file copy of the image.

g. The **CPSC PIV Registrar (EXRM)** (or other CPSC employee designated to perform that task) shall fingerprint the **Applicant**, obtaining all the **Applicant's** fingerprints in an electronic format as defined in Section 4.4 of FIPS PUB 201, and retain a copy. (PIV-II only)

h. The **CPSC PIV Registrar (EXRM)** (or other CPSC employee designated to perform that task) shall initiate a National Agency Check with Inquiries (NACI) on the **Applicant** as required by Executive Order 10450 [EO10450]. Any unfavorable results of the investigation shall be adjudicated to determine the suitability of the **Applicant** for obtaining a CPSC PIV Credential.

i. When all of the above requirements are completed, the **CPSC PIV Registrar (EXRM)** shall notify the **CPSC PIV Sponsor (Supervisor/COTR)** and the designated **CPSC PIV Issuer (TSFS)** that the **Applicant** has been approved for the issuance of a CPSC PIV Credential. Conversely, if any of the required steps are unsuccessful, the **CPSC PIV Registrar (EXRM)** shall send appropriate notifications to the same authorities.

j. The **CPSC PIV Registrar (EXRM**) shall make available the following information to the **CPSC PIV Issuer (TSFS)** through a secure process:

- **Applicant's** digital facial image
- Confirmation of the satisfactory results of the **Applicant's** background investigation.
- Other data associated with the **Applicant** (e.g., employee affiliation).
- The period that the CPSC PIV Credential will remain valid. For permanent employees the credential expiration date will be established at six months from date of issue if the credential is issued based on a National Agency Check (NAC) only, and five years if the credential is issued based on a National Agency Check with Inquiries (NACI). For temporary employees, the credential expiration date will be established at six months from date of issue if the credential is issued based on a NAC, or the date the temporary employment is expected to end if the credential is issued based on a NACI.

In PIV-II, the **CPSC PIV Registrar (EXRM)** shall make available the following information to the **CPSC PIV Digital Signatory** through a secure process:

- Electronic biometric data for CPSC PIV Credential personalization

- Other data associated with the **Applicant** that is required for the generation of signed objects for CPSC PIV Credential personalization.

k. The **CPSC PIV Registrar (EXRM)** shall be responsible for maintaining the following:

- Completed and signed CPSC PIV Sponsor Form.
- 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 FIPS PUB 201, Section 2.3.

2. CPSC PIV Credential Issuance (TSFS)

The CPSC PIV Credential issuance process shall meet the functional and security requirements defined below. The CPSC may enhance the issuance process to meet local constraints and requirements; however, the resulting process shall meet the minimum requirements listed below:

a. The **CPSC PIV Issuer (TSFS)** shall confirm the validity of the CPSC PIV Credential Request Form received from the **CPSC PIV Sponsor (Supervisor/COTR)**, and the approval notification received from the **CPSC PIV Registrar (EXRM)**. The **CPSC PIV Issuer (TSFS)** shall also confirm that the approval notification is consistent with the results of the background investigation.

b. The **CPSC PIV Issuer (TSFS)** shall control the creation and personalization of a new CPSC PIV Credential using the information provided by the **CPSC PIV Registrar (EXRM)**. In PIV-II, the **CPSC PIV Issuer (TSFS)** shall initiate the creation of a CHUID (Card Holders Unique Identifier) for the new CPSC PIV Credential. This CHUID shall be made available to the **CPSC PIV Digital Signatory** through a secure mechanism.

c. In PIV-II, the **CPSC PIV Digital Signatory** shall create digitally signed credential elements (biometric and CHUID) needed for the CPSC PIV Credential personalization process, using the data supplied by the **CPSC PIV Registrar**

(EXRM) 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 **CPSC PIV Issuer (TSFS).**

d. The **Applicant** shall appear in person to the **CPSC PIV Issuer (TSFS)** (or an authorized delegate) to collect the CPSC PIV Credential. Before the newly created CPSC PIV Credential is given to the **Applicant**, the **CPSC PIV Issuer (TSFS)** 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 **CPSC PIV Issuer (TSFS)** (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new CPSC PIV Credential being personalized. Additionally, the **CPSC PIV Issuer (TSFS)** (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the CPSC PIV Credential.

   - In PIV-II, the **CPSC PIV Issuer (TSFS)** (or their authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the CPSC PIV Credential.

e. The **CPSC PIV Issuer (TSFS)** shall personalize the CPSC PIV Credential. The personalized CPSC PIV Credential shall meet all of the technical and interoperability specifications in Section 4 for compliance with PIV-II requirements.

f. In PIV-II, the recipient's name, issuer identity, CPSC PIV Credential number, and possibly PKI certificate identification information shall be enrolled and registered with back-end data stores that support the CPSC PIV system. Depending on the infrastructure design, the back-end data stores may be centralized or decentralized.

g. The **CPSC PIV Issuer (TSFS)** (or an authorized delegate) shall obtain a signature from the **Applicant** (now **CPSC PIV Credential Holder**) attesting to the **Applicant's** acceptance of the CPSC PIV Credential and the related responsibilities.

h. When all of the above requirements are completed, the **CPSC PIV Issuer (TSFS)** shall notify the **CPSC PIV Sponsor (Supervisor/COTR)** and the designated **CPSC PIV Registrar (EXRM)** signifying that the personalization and issuance process has been completed. Conversely, if any of the required steps are unsuccessful, the **CPSC PIV Registrar (TSFS)** shall send appropriate notifications to the appropriate authorities.

i The **CPSC PIV Issuer (TSFS)** shall be responsible for maintaining the following:

- Completed and formally authorized **CPSC PIV Credential Request Form (Sponsor Form)**
- The approval notice from the **CPSC PIV Registrar (EXRM)**
- The name of the CPSC PIV Credential holder (**Applicant**)
- The credential identifier. In PIV-II, this identifier is the CPSC PIV Credential serial number
- The expiration date of the CPSC PIV Credential
- The signed acceptance form from the **CPSC 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 FIPS PUB 201, Section 2.3.

3. CPSC PIV Credential Maintenance

The CPSC PIV Credential shall be maintained using processes that comply with the specifications FIPS PUB 201. It is important to keep track of active cards as well as lost, stolen and expired cards. The **CPSC PIV Credential System Registry Administrator (EXRM)** shall maintain a registry for all CPSC PIV Credentials issued, and will establish and maintain a method for monitoring CPSC PIV Credential expiration dates that will provide notification to **CPSC PIV Credential Holders** at least six weeks prior to expiration of their CPSC PIV Credential to allow the **CPSC PIV Credential Holder** sufficient time to complete the CPSC PIV Credential renewal process.

The data and credentials held in the CPSC PIV Credential may need to be invalidated prior to the expiration date of the card. The **CPSC PIV Credential Holder** may retire or terminate employment, or a CPSC PIV Credential may become damaged, lost, or stolen, requiring invalidation of a previously active CPSC PIV Credential

In the event a **CPSC PIV Credential Holder** retires or terminates employment, the **PIV Sponsor** (Supervisor/COTR) for the **CPSC PIV Credential Holder** will notify the **CPSC PIV Credential System Registry Administrator (EXRM)** with the exact date of the **CPSC PIV Credential Holder's** departure, and the **CPSC PIV Credential System Registry Administrator (EXRM)** will invalidate the CPSC PIV Credential within 24 hours of **CPSC PIV Credential Holder's** departure or sooner based on the level of risk.

The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating an **CPSC PIV Credential Holder**. In this regard, procedures for PIV Card maintenance must be integrated into CPSC procedures to ensure effective card management.

4. CPSC PIV Credential Renewal
   Renewal is the process by which a CPSC PIV Credential is replaced without the need to repeat the full registration procedure.

   a. The **PIV Issuer (TSFS)** shall verify that the **CPSC PIV Credential Holder** remains in good standing and personnel records are current before renewing the CPSC PIV Credential.

   b. When renewing the CPSC PIV Credential for a current **CPSC PIV Credential Holder**, the NACI check shall be followed in accordance with the OPM guidance. The CPSC PIV Credential shall be valid for no more than five years.

III. Access Control Subsystem

The **CPSC Official Responsible for Logical Security and Access (EXIT)** determines the graduated assurance levels for access to CPSC logical resources, and the **CPSC Official Responsible for Physical Security and Access (EXIT)** determines the graduated assurance levels for access to CPSC physical resources.

With the exception of visual PIV authentication required for physical access to CPSC facilities, the graduated assurance levels for PIV authentication required to access CPSC physical and logical Resources contained in the following table only apply to PIV-II.

Forms Requirements

CPSC PIV Initial Credential Request Form (Sponsor Form)

CPSC PIV Renewal of Credential Form

CPSC PIV Cancellation of Credential Form