The following information was posted with the attached DRAFT document:

Jun 2, 2014

SP 800-79-2

DRAFT Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)

NIST announces that Draft Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, is now available for public comment. This document has been updated to align with the release of FIPS 201-2, published in September 2013. The major changes for this revision of SP 800-79 include additions and updates to issuer controls in response to new or changed requirements in FIPS 201-2. These are:

- Inclusion of issuer controls for Derived PIV Credentials Issuers (DPCI),
- Addition of issuer controls for issuing PIV Cards under the grace period and for issuing PIV Cards to individuals under pseudonymous identity,
- Addition of issuer controls for the PIV Card's visual topography,
- Updated issuer controls to detail controls for post-issuance updates of PIV Cards,
- Updated references to the more recent credentialing guidance issued by OPM,
- Addition of issuer controls with respect to the optional chain-of-trust records maintained by a PIV Card issuer, and.
- Modified process to include an independent review prior to authorization of issuer.

Draft NIST Special Publication 800-79-2

Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)

Ramaswamy Chandramouli
Hildegard Ferraiolo
Nabil Ghadiali
Jason Mohler
Scott Shorter

http://dx.doi.org/10.6028/NIST.SP.XXX

INFORMATION SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-79-2

Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)

Ramaswamy Chandramouli
Hildegard Ferraiolo
Computer Security Division
Information Technology Laboratory

Nabil Ghadiali
National Gallery of Art

Jason Mohler
Scott Shorter
Electrosoft Services, Inc

http://dx.doi.org/10.6028/NIST.SP.XXX

June 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 et seq., Public Law 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III, Security of Federal Automated Information Resources.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-79-2
Natl. Inst. Stand. Technol. Spec. Publ. 800-79-2, 120 pages (June 2014)
http://dx.doi.org/10.6028/NIST.SP.XXX
CODEN: NSPUE2

Public comment period: *June 2, 2014* through *June 30, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

The purpose of this SP is to provide appropriate and useful guidelines for assessing the reliability of issuers of PIV Cards and Derived PIV Credentials. These issuers store personal information and issue credentials based on OMB policies and on the standards published in response to HSPD-12 and therefore are the primary target of the assessment and authorization under this guideline. The reliability of an issuer is of utmost importance when one organization (e.g., a Federal agency) is required to trust the identity credentials of individuals that were created and issued by another Federal agency. This trust will only exist if organizations relying on the credentials issued by a given organization have the necessary level of assurance that the reliability of the issuing organization has been established through a formal authorization process.

Keywords

Assessment; Authorization; Controls; Derived PIV Credentials; Issuer; personal identity verification; PIV card

Acknowledgments

The authors wish to thank their colleagues who contributed to this document's development and reviewed its many versions. The authors also gratefully acknowledge and appreciate the many comments and contributions made by government organizations, private organizations, and individuals in providing direction and assistance in the development of this document.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, established a policy for creation, issuance, and use of personal identification credentials in the Federal government. The Directive requires the development and use of a standard for secure and reliable forms of identification for Federal employees and contractors. The Personal Identity Verification (PIV) specifications of the resulting standard (Federal Information Processing Standard (FIPS) 201) is the foundation for securely identifying every individual seeking access to valuable and sensitive Federal resources, including buildings, information systems, and computer networks. The implementation of PIV specifications, in turn, involves operations such as the collection, access protection, and dissemination of personal information, which itself requires privacy protection.

NIST developed and published the Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification (PIV) of Federal Employees and Contractors*, as well as several NIST Special Publications (SPs) to provide additional specifications and supporting information in response to HSPD-12. These documents provide the required foundation for standardizing the processes related to the adoption and use of government-wide personal identification credentials as a means to verify the identity of the credential holders.

In light of the requirements for both improved security and protection of personal privacy, HSPD-12 established four control objectives, one of which includes the call for forms of identification that is "*issued by providers whose reliability has been established by an official accreditation process*." In response, Appendix A.1 of FIPS 201 specifies that NIST "…develop a new accreditation methodology that is objective, efficient, and will result in consistent and repeatable accreditation decisions…". This led to development of the first version of this NIST Special Publication (SP) in 2005.—in prior revision entitled *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*[1].

The update to this SP is to reflect the 2nd revision of FIPS 201 (i.e., FIPS 201-2) published in 2013. It provides appropriate and useful guidelines for assessing the reliability of issuers of PIV Cards and introduces guidelines for issuers of the newly introduced Derived PIV Credential for mobile devices[2]. The reliability of an issuer is of utmost importance when an organization (e.g., a Federal agency) is required to trust the identity credentials of individuals that were created and issued by another organization. This trust only exists if the relying organization has the necessary level of assurance of the issuing organization that the credential is established via a formal authorization process and thus reliable.

[1] The prior revision of this document entitled was *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. As NIST 800-37-1 has deprecated the use of the term accreditation in favor of the term authorization, this revision is entitled Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).

2 A mobile device, for the purpose of this document is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

This SP provides an assessment and authorization methodology for verifying that issuers are adhering to standards and implementation directives developed under HSPD-12. The salient features of the methodology are:

(i) Controls derived from specific requirements in FIPS 201-2 and relevant documents for PIV Card issuer (PCI) and Derived PIV Credential issuer (DPCI);
(ii) Procedures for verifying and monitoring adherence to the requirements through an assessment of the implementation of the controls (control assessment); and
(iii) Guidance for evaluating the result of an assessment in order to arrive at the accreditation decision.

Authorizing an issuer based on the assessment and authorization methodology in this document establishes the reliability of the issuer.

Authorization is the basis for establishing trust in an issuer and requires that the assessment be thorough and comprehensive. Careful planning, preparation, and commitment of time, energy, and resources are required. These guidelines are designed to assist agencies in creating the needed roles, assigning responsibilities, developing an acceptable operations plan, drawing the issuer's authorization boundary, evaluating the findings of all control assessments, and making a proper authorization decision. Realizing that organizations may vary significantly in how they choose to structure their operations, these guidelines have been developed to support organizational flexibility, and are designed to minimize the effort needed to assess, authorize, and monitor the reliability of the issuer.

In addition to flexibility and efficiency, the authorization methodology defined in these guidelines generates assessment findings and resulting authorization decisions that are consistent and repeatable. These characteristics provide assurance to an organization's management that when an issuer has been authorized based on these guidelines they can be trusted as a provider of secure and reliable identification credentials as required by HSPD-12.

This document shall be used by both small and large organizations and can be applied whether issuance processes are:

- Centrally located;
- Geographically dispersed; or
- Outsourced in varying degrees to another organization(s) or service provider(s).

1. Introduction

In order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy, Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractor*s was issued on August 27, 2004. This Directive established a Federal policy to create and use government-wide secure and reliable forms of identification for Federal employees and contractors. It further defined *secure and reliable forms of identification* as ones that—

- Is issued based on sound criteria for verifying an individual's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

NIST developed and published Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification (PIV) of Federal Employees and Contractors,* and several Special Publications providing additional specifications in response to HSPD-12. These documents provide the foundation for Government personal identification, verification, and access control systems.

Appendix A.1 of FIPS 201-2 states the following:

"… [HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process..."

To determine consistency in operations of issuers of PIV Cards, NIST developed a set of attributes as the basis of reliability assessment and published the first version of this document in July 2005. Subsequent lessons learned in various agencies' implementation, experience in credential management and PIV Card issuance together with the evolution of PIV Card issuing organizations motivated NIST to develop an updated methodology that is objective, efficient, and resulted in a consistent and repeatable authorization decisions. These developments led NIST to publish the first revision to SP 800-79 (i.e., SP 800-79-1) in June 2008. In 2013, FIPS 201 was superseded by FIPS 201 revision 2 (FIPS 201-2). FIPS 201-2 incorporates additional lessons learned from PIV Card issuers and allows for mobile device-integrated PIV credentials. This revision reflects the update to FIPS 201-2 and its new associated publication, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* which details the issuance and use of Derived PIV Credentials[3] that are integrated in mobile devices.

[3] The Derived PIV Credential is an additional common identity credential under HSPD-12 and FIPS 201-2 that is issued by a Federal department or agency and used with mobile devices. Derived PIV Credentials are based on the general concept of derived credential in SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials. When applied to PIV, identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential. Instead, the user proves possession of a valid PIV Card to receive a Derived PIV Credential. To achieve interoperability with the PIV infrastructure and its applications, a Derived PIV Credential is a subset of PIV Credential and restricted to PKI Credentials.

Unless there is a need to differentiate between PCIs and DPCIs, this document uses the common term issuer to refer to both types of issuers. Similarly, Derived PIV Credential and the PIV Card's credentials are collectively referred to as credentials, unless a distinction is made. An issuer is considered to be owned and managed by an *organization* which may be a Federal department, agency, or a private entity authorized by a Federal department or agency. Ensuring the reliability of an issuer is of critical importance in light of the security and privacy implications of credentials used for meeting the objective of secure and reliable forms of identification to millions of employees and contractors. HSPD-12 and its standards and guidelines were developed to address a range of security concerns, including those posed by terrorists in a post-9/11 world. Providing a comprehensive set of standards for controlling access to the physical and logical resources through the use of standard credentials, provides the assurance that certain pre-defined levels of security can be achieved. However, it requires organizations to implement and use the standards in a consistent and reliable manner. An organization must have confidence in the credentials it issues to its own employees and contractors. Possibly more importantly, since HSPD-12 requires a common inter-agency-interoperable standard, all organizations need to have confidence in the identity credentials issued by other organizations. This confidence can only be established if the issuer's functions in those other organizations are assessed and authorized. Thus, authorization of the issuer plays a key role in meeting the objectives of HSPD-12.

NIST has considerable experience in the development of assessment and authorization methodologies, most significantly with the widely accepted approach to authorization in SP 800-37-1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and its family of related documents. While SP 800-37-1 is focused on the authorization of the security of information systems, rather than the authorization of the reliability of an issuer, it does offer a practical foundation for the authorization programs envisioned by HSPD-12. This document utilizes the various aspects of SP 800-37-1 and applies them to authorizing the reliability of an issuer. Authorization of an issuer requires prior assessment of the security of all information systems used by that issuer in accordance with SP 800-37-1.

One difference between the authorization of the security of information systems and the authorization of the reliability of an issuer is that an organization has considerable flexibility in how they prepare for an SP 800-37-1 authorization (particularly in implementing security controls), but have little room for variation for an SP 800-79-2 authorization. Much of the flexibility in SP 800-37-1 comes from the necessity of acceptable variations in security controls, since individual information systems within varied environments may have significantly different security requirements. Conversely, the desire for standardization in HSPD-12 has led to the development of a stable set of requirements. There may be some flexibility in how a requirement is met, but a majority of requirements must be satisfied in a uniform manner in order to deem an issuer as reliable. Allowing too much latitude in how a requirement is met undermines its reliability.

Although organizations may feel constrained by the uniformity required by FIPS 201-2, standardization greatly contributes to achieving the objectives of HSPD-12 across issuer implementations. For all organizations to accept PIV Cards or Derived PIV Credentials of other organizations, one set of rules (i.e., FIPS 201-2) must be followed by all PIV system participants. This Special Publication provides a way of determining if the participants are following these

rules. Assessment methods that are consistent, reliable, and repeatable provide a basis for determining the *reliability* and *capability* of issuers of PIV Cards and Derived PIV Credentials, which herein is defined as *consistent adherence to the PIV standards.* In particular, if an issuer meets the requirements of FIPS 201-2 and relevant documents as verified through applicable assessment procedures and maintain consistency of their operations with respect to meeting these criteria, they can be considered reliable as is required by HSPD-12.

The objectives of the guidelines in this document are to—

- Outline the requirements for PIV Card Issuers and for the Derived PIV Credentials Issuers, the rationale for the requirements and the assessment procedures required to determine the satisfaction of those requirements through a combination of policies, procedures, and operations.
- Describe an authorization methodology that provides a framework for organizing the requirements and assessment procedures stated above and at the same time provides coverage for all the control objectives stated in HSPD-12.
- Emphasize the role of risk associated with an authorization decision, based on assessment outcomes that take into account the organization's mission.

1.1 Applicability, Intended Audience, and Usage

This document is applicable to, and shall be used by all Federal organizations. It may also be used by any other organization (e.g., state and local government, educational, non-profit) desiring close alignment with FIPS 201-2 and associated PIV credentials.

All Federal organizations are required to adopt HSPD-12 and implement FIPS 201-2. They must use SP 800-79-2 to assess the adequacy of their implementations as well as the reliability of either the directly-controlled or sub-contracted services involved in creating and issuing the mandatory PIV Cards and the optional Derived PIV Credentials (if implemented).

SP 800-79-2 is consistent and compatible with the control objectives in HSPD-12, FIPS 201-2, and SP 800-37-1. SP 800-79-2 includes a number of roles, requirements, definitions, specifications, and procedures needed to assess the reliability of an issuing organization. In situations where an issuer fails to meet the assessment criteria in SP 800-79-2, they must immediately halt operations.

Once an issuer is authorized to operate using the guidelines from 800-79-2, trust can be maintained in the credentials issued. Hence, organizations that accept PIV Cards or Derived PIV Credentials from issuers that are not authorized (either to SP 800-79-2 or at all), are doing so at their own risk, since the reliability of their operations cannot be assured.

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

1.2 Changes for this Revision

The major changes for this revision include additions and updates to issuer controls in response to new or changed requirements in FIPS 201-2. These are:

- Inclusion of issuer controls for Derived PIV Credentials Issuers (DPCI),
- Addition of issuer controls for issuing PIV Cards under the grace period and for issuing PIV Cards to individuals under pseudonymous identity,
- Addition of issuer controls for the PIV Card's visual topography,
- Updated issuer controls to detail controls for post-issuance updates for PIV Cards,
- Updated references to more recent credentialing guidance issued by OPM,
- Addition of issuer controls with respect to the chain-of-trust records maintained by a PIV Card issuer.
- Modified process to include an independent review prior to authorization of issuer..

1.3 Timelines for using the revised Guidelines

This publication is effective immediately and it supersedes the previous version.

FISP 201-2 mandates the implementation of some PIV Card features that were previously optional to implement. The Standard also requires that all new or replacement PIV Cards include these previously optional features beginning September 2014. These new FIPS 201-2 requirements results in the following re-authorization scenarios:

- Organizations that already issue PIV Cards with the new mandatory features do not have to be re-authorized since the current Authorization to Operate (ATO) addresses issuance of FIPS 201-2 PIV Cards[4];

- Organizations that do not currently issue PIV Cards with the new mandatory features shall be required to undergo re-authorization to operate using the guidelines of SP 800-79-2 immediately upon publication.

Derived PIV Credentials are optional PIV credentials introduced in FIPS 201-2. The timeline for their use on mobile devices depends on the final release of SP 800-157. Similarly, authorization of Derived PIV Credential Issuers is depended on the final release date of SP 800-157, the Authorization to Operate (ATO), and the availability of validated Derived PIV Credential tokens. No Derived PIV Credentials shall be issued unless the issuer has met the requirements of and is operating under the guidelines of SP 800-79-2[5].

4 Re-Authorization using the revised guidelines (SP 800-79-2) is required within three (3) years of current Authorization to Operate (ATO).

[5] Because of the re-authorization scenario (ii), the final release of this document may occur before the final release of SP 800-157. Any changes in the final SP 800-157 that are not reflected in SP 800-79-2 will be addressed in a revision of SP 800-79.

1.4 Key Related NIST Publications

The following NIST publications were utilized as the basis for the requirements listed in this document.

- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- SP 800-37-1 Rev. 1**,** *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* or as amended
- SP 800-73-4, *Interfaces for Personal Identity Verification (3 Parts),* or as amended
  Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation
  Pt. 2- PIV Card Application Card Command Interface
  Pt. 3- PIV Client Application Programming Interface
- SP 800-76-2, *Biometric Data Specification for Personal Identity Verification,* or as amended
- SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV),* or as amended
- SP 800-85 A-3, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73-4 Compliance),* or as amended
- SP 800-85 B-2, *PIV Data Model Conformance Test Guidelines,* or as amended
- *SP 800-157 Guidelines for Derived Personal Identity Verification (PIV)Credentials,* or as amended

1.5 Organization of this Special Publication

The remainder of this publication is organized as follows:

- **Chapter 2** provides background information needed to understand issuer assessment and authorization methodology, as well as the inputs and outputs involved in the assessment of the issuance processes. These include: (i) definition of the target entities (issuer, issuer facilities, issuer boundaries); (ii) the relationship between authorization under SP 800-37-1 and authorization under SP 800-79-2; (iii) preparatory tasks for the assessment of an issuer organization including assignment of roles and responsibilities; (iv) two alternative authorization decisions; (v) acceptance of risk in the authorization decision; and (vi) the contents of the authorization package.
- **Chapter 3** describes the building blocks of the issuer assessment and authorization methodology, including Authorization Topics, Authorization Focus Areas, and the control requirements (issuer controls) within each area.
- **Chapter 4** provides a detailed description of the assessment methods for the issuer controls whose outcomes form the basis for the authorization decision.
- **Chapter 5** describes the 4 phases of the authorization process and the tasks involved in each phase.

- **Appendices** include— (A) references; (B) glossary and acronyms; (C) issuer readiness review checklist; (D) issuer operations plan templates; (E) assessment report template; (F) sample authorization transmittal and decision letters; (G) issuer controls and assessment procedures; and (H) summary of tasks and sub-tasks.

2. PREPARATION FOR ASSESSMENT AND AUTHORIZATION

This chapter presents the fundamentals of an authorization of a PIV Card Issuer (PCI) and a Derived PIV Credential Issuer (DPCI). It includes: (i) definitions of an issuer and issuing facility; (ii) outsourcing issuer services or functions; (iii) the differences between an assessment and authorization; (iv) authorization boundaries of an issuer; (v) roles and responsibilities; (vi) the relationship between authorization under Special Publication (SP) 800-37-1 and SP 800-79-2; (vii) preparing for the assessment; (viii) types of authorization decisions; (xi) use of risk in the authorization decision; and (x) the contents of the authorization package.

2.1 Issuer

At the highest level, an issuer includes all functions required to produce, issue, and maintain PIV Cards or Derived PIV Credentials for an organization. A PCI or DPCI is considered operational if all relevant roles and responsibilities have been defined and appointed; suitable policies and compliant procedures have been implemented for all relevant PIV processes[6], including sponsorship, identity proofing/registration, adjudication, card production, activation/issuance, and maintenance; and information system components that are utilized for performing the above-mentioned functions (processes) have been assessed and shown to meet all technical and operational requirements prescribed in FIPS 201-2 and related documents.

In order to comply with Homeland Security Presidential Directive 12 (HSPD-12), an organization must first establish an issuer, to issue PIV Cards or Derived PIV Credentials, which conforms to and satisfies the requirements of FIPS 201-2 and related documents. The issuer must then be authorized (i.e., using the guidelines specified this document). An organization has certain flexibility in implementing its issuance functions. It may outsource some of the required processes or establish multiple units for fulfilling these processes. Regardless of its structure, the organization is responsible for the management and oversight and maintains full responsibility for its functions as an issuer as required in HSPD-12.

The organization must completely describe its PIV Card and/or Derived PIV Credential issuance functions in an operations plan. This comprehensive document incorporates all the information about the issuer that is needed for any independent party to review and assess the capability and reliability of its operations. An operations plan includes a description of the structure of the issuer, its facilities, any external service providers, the roles and responsibilities, policies and procedures which govern its operations, and a description of how requirements of FIPS 201-2 are being met. A template for an operations plan is provided in Appendix D.

2.2 Issuing Facilities

An *issuing facility* is a physical site or location–including all equipment, staff, and documentation–that is responsible for carrying out one or more of the following PIV functions: (i) identity proofing/registration; (ii) card/ token[7] production; (iii) activation/issuance; and (iv)

[6] Note: Some of the processes may not apply to Derived PIV Credentials Issuers.

[7] When the term token is used within this document it is used to refer to the various Derived PIV Credential tokens detailed in NIST SP 800-157.

maintenance. An issuing facility operates under the auspices of a PIV Card or Derived PIV Credential Issuer, and implements the policies and executes procedures prescribed by the issuer for those functions sanctioned for the facility (e.g. an identity proofing/ registration facility).

Based on certain characteristics (e.g. size, geographic locations, the organization(s) that it supports), an issuer may have its services and functions provided centrally, distributed across multiple locations, or may even be able to perform the entire issuance process remotely[8]. For example, in the case of PIV Card issuance, a geographically dispersed organization may decide to have identity proofing/registration and activation/issuance functions performed in different facilities in different parts of the country so that applicants can minimize travel. In this example, the different issuing facilities fall under the purview (policy, management) of a single issuer which encompasses all the functions necessary to issue PIV Cards.

Within that issuer, the geographically dispersed issuing facilities have specific responsibilities and are under the direct management control of the issuer.

2.3 Outsourcing of Issuing Functions

An organization may outsource its issuing functions to one or more organizations. As the complexity and cost of new technology increase, the organization may decide that the most efficient and cost-effective solution for implementing HSPD-12 is to seek the services of an external service provider. An external service provider may be a Government agency, a private entity, or some other organization that offers services or functions necessary to issue PIV Cards or Derived PIV Credentials.

Figure 1 provides an illustration of the functions that can be outsourced. Only the organization can decide which of its employees and contractors are required to apply for a PIV Card and a Derived PIV Credential (Sponsorship – a responsible official of the organization providing the biographic and organizational affiliation of the applicant) and under what conditions the application will be approved (Adjudication – the kind of background information that will form the basis for authorization to issue the PIV Card). Therefore, these two functions cannot be outsourced.

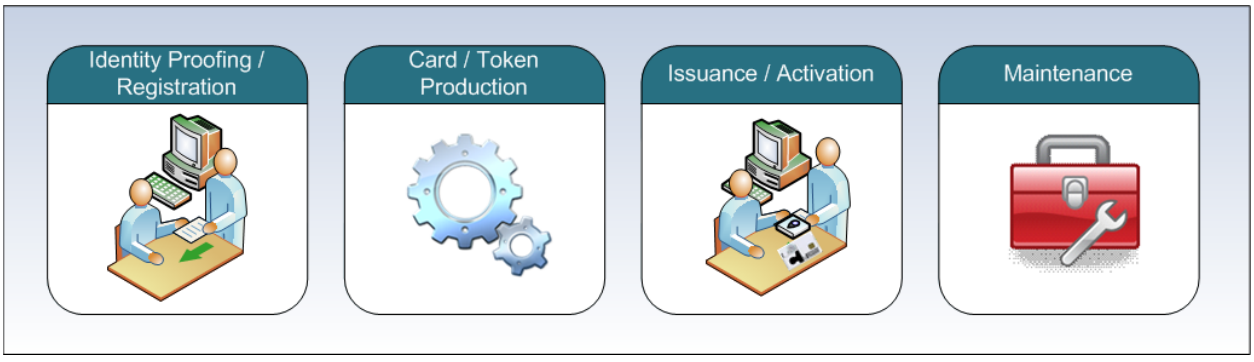

Figure 1 - Outsourcing of Issuer Functions[9]

[8] In the case of Derived PIV Credentials issued at Level of Assurance (LOA) 3.

[9] The term token is used in this document to refer to the various Derived PIV Credential tokens detailed in NIST SP 800-157.

A PCI or DPCI which out-sources services to an external provider must make sure that all privacy-related requirements are satisfied and as such is responsible for ensuring that privacy requirements are being met both internally and by every external service provider.

If an issuer is considering using PIV services set up by another organization, the operations plan and associated documents, the authorization decision and evidence of implementation of FIPS 201-2 requirements of that issuer (PCI or DPCI service provider) must be reviewed. Similarly, if an issuer is using the services of an external service provider selectively for one or more of its processes, the provider's capability to meet FIPS 201-2 requirements for those processes must be reviewed as well. In both cases, the information gathered as part of this review activity must be included in the issuer's assessment leading to authorization. Outsourced functions must be assessed prior to authorization of an issuer.

2.4 Assessment and Authorization

HSPD-12 mandates that identification credentials be "*issued only by providers whose reliability has been established by an official accreditation process*." This document contains guidelines for satisfying the requirements for an official authorization and provides a methodology that can be utilized to formally authorize an issuer. This methodology consists of two major sets of activities–assessment and authorization. While assessment and authorization are very closely related, they are two very distinct activities.

Assessment occurs before authorization and is the process of gathering evidence regarding an issuer's satisfaction of the requirements of FIPS 201-2, both at the organization and facility level. Assessment activities include interviews with the issuer and the issuing facility's personnel, a review of documentation, observation of processes, and execution of tests to determine overall reliability of the issuer. The result of the assessment is a report that serves as the basis for an authorization decision. The report is also the basis for developing corrective actions for removing or mitigating discovered deficiencies.

Distinct from assessment, authorization is the decision to permit the operation of the issuer once it has been established that the requirements of FIPS 201-2 have been met and the risks regarding security and privacy are acceptable. The individual making the authorization decision must be knowledgeable of HSPD-12 and aware of the potential risks to the organization's operations, assets, and personnel (e.g., applicants, issuing facility staff).

The assessment and the authorization are both carried out by the organization that "owns" (i.e., manages, controls, or privately owns) the issuance of PIV Cards and/or Derived PIV Credentials. In order to make an informed, risk-based authorization decision, the assessment process should seek to answer the following questions:

- Has the issuer implemented the requirements of FIPS 201-2 in the manner consistent with the standard?
- Do personnel understand the responsibilities of their roles and/or positions, and reliably perform all required activities as described in the issuer's documentation?

- Are services and functions at the issuer and its facilities (e.g., identity proofing/registration, card /token production, activation/issuance) carried out in a consistent, reliable, and repeatable manner?
- Have deficiencies identified during the assessment been documented, current and potential impact on security and privacy been highlighted, and the recommendations and timelines for correction or mediation been included in the assessment report?

2.5 Authorization Boundary of the Issuer

The first step in authorizing an issuer is to identify the appropriate authorization boundary. The authorization boundary defines the specific operations that are to be the target of the assessment and authorization. A PCI comprises the complete set of functions required for the issuance and maintenance of PIV Cards while a DPCI comprises of the complete set of functions required for the issuance and maintenance of Derived PIV Credentials. In determining the authorization boundary, the organization must consider if the functions are being performed identically in all issuing facilities, are using identical information technology components, and are under the same direct management control. For instance, an organization may have two sub-organizations, each of which has distinct processes and management structures. The organization may decide to establish two separate issuers, each with its own authorization boundary. In this example, two separate assessments would be undertaken. Each assessment would result in an independent authorization decision.

In drawing an authorization boundary, an organization may want to include only a subset of its issuing facilities. For example, if a PCI has several facilities, some of which are ready for operation and some that are still in the development stage, the organization may choose to define the authorization boundary to include the PCI and only those facilities that are ready to be assessed. If the authorization is successful, the PCI and a subset of its issuing facilities will be authorized to operate and begin issuing PIV Cards. The remaining issuing facilities can continue with implementation and be included in the authorization boundary at a later date.

In the case of outsourcing issuance services that are not under direct management control of the organization nor physically located within its facilities, the organization must include the functions provided by external service providers within the authorization boundary to make certain that they are included within the scope of authorization. This assures that no matter how and where the functions are performed, the organization maintains complete accountability for the reliability of its PIV program.

Care should be used in defining the authorization boundary for the issuer. A boundary that is unnecessarily expansive (i.e., including many dissimilar processes and business functions or geographically dispersed facilities) makes the assessment and authorization process extremely complex. Establishing a boundary and its subsequent authorization are organization-level activities that should include participation of all key personnel. An organization should strive to define the authorization boundary of their issuer such that it strikes a balance between the costs and benefits of assessment and authorization.

While the above considerations should be useful to an organization in determining the boundary for purposes of authorization, they should not limit the organization’s flexibility in establishing a

practical boundary that promotes an effective HSPD-12 compliant implementation. The scope of an authorization is an issuer - that is a PCI or DPCI (whose boundaries are formed by included issuing facilities) and not individual issuing facilities.

2.6 Issuer Roles and Responsibilities

PIV Card and Derived PIV Credential issuance roles and their processes are to be selected based on the organization's structure, its mission, and operating environment. The organization must make sure that a separation of roles has been established and the processes are in compliance with FIPS 201-2.

This document identifies roles and responsibilities of key personnel involved in the assessment and authorization of an issuer[10]. Recognizing that organizations have widely varying missions and structures, there may be some differences in naming conventions for authorization-related roles and in how the associated responsibilities are allocated among personnel (e.g. one individual may perform multiple roles in certain circumstances).

2.6.1 Senior Authorizing Official (SAO)

The Senior Authorizing Official (see Figure 2) of an organization is responsible for all operations. The SAO has budgetary control, provides oversight, develops policy, and has authority over all functions and services provided by the issuer.

2.6.2 Designated Authorizing Official (DAO)

The Designated Authorizing Official has the authority within an organization to review all assessments of an issuer and its facilities, and to provide an authorization decision as required by HSPD-12. Through authorization, the DAO accepts responsibility for the operation of the issuer at an acceptable level of risk to the organization. The SAO may also fulfill the role of the DAO. The DAO shall not assume the role of the OIMO.

2.6.3 Organization Identity Management Official (OIMO)

The Organization Identity Management Official is responsible for implementing policies of the organization, assuring that all PIV processes of the issuer are being performed reliably, and providing guidance and assistance to the issuing facilities. The OIMO implements and manages the operations plan; ensures that all roles are filled with capable, trustworthy, knowledgeable, and trained staff; makes certain that all services, equipment, and processes meet FIPS 201-2 requirements; monitors and coordinates activities with Issuing Facility Manager(s); and supports the authorization process.

2.6.4 Issuing Facility Manager

An Issuing Facility Manager manages the day-to-day operations of an issuing facility. The Issuing Facility Manager is responsible for implementing all operating procedures for those functions that have been designated for that facility by the issuer. The Manager must ensure that

[10] Organizations may define other significant roles (e.g., PIV System liaisons, operations managers) to support the authorization process.

all PIV processes adhere to the requirements of FIPS 201-2, and that all PIV services performed at the issuing facility are carried out in a consistent and reliable manner in accordance with the organization's policies and procedures and the OIMO's direction. In some cases (e.g. small organizations), the OIMO may fulfill the role of the Issuing Facility Manager.

2.6.5 Assessor

The Assessor is responsible for performing a comprehensive and 3rd party assessment of an issuer. The Assessor (usually supported by an assessment team) verifies that PIV processes in-place at the issuer comply with control objectives of FIPS 201-2. The results of the assessment are presented to the OIMO who reviews the assessment findings and prepares recommended corrective actions to reduce or eliminate any discrepancies or shortcomings. The Assessor is also responsible for providing recommendations for reducing or eliminating deficiencies and security weaknesses, describing the potential impact of those deficiencies if not corrected. An Assessor shall not be assigned the DAO's role and vice versa.

To preserve the impartial and unbiased nature of the assessment, the Assessor must be a 3rd party that is independent of the office(s) and personnel directly responsible for the day-to-day operation of the issuer. The Assessor shall also be independent of those individuals responsible for correcting deficiencies and discrepancies identified during the assessment phase. The independence of the Assessor is an important factor in maintaining the credibility of the assessment results and ensuring that the DAO receives objective information in order to make an informed authorization decision.

2.6.6 Applicant Representative (AR)

The Applicant Representative is an optional role and may be established and used at the discretion of the organization. The AR represents the interests of current or prospective employees and contractors who are applicants for PIV Cards or Derived PIV Credentials. ARs are responsible for assisting an applicant who is denied a PIV Card or Derived PIV Credential because of missing or incorrect information, and for ensuring that all applicants obtain useful information and assistance when needed. This role may be assigned to someone in the organization's personnel or human resources.

2.6.7 Privacy Official (PO)

The responsibilities of the Privacy Official are defined in FIPS 201-2. The person filling this role shall not assume any other operational role within the issuer organization. The PO issues policy guidelines with respect to collection and handling of personally identifiable information from applicants so as to ensure that the issuer is in compliance with all relevant directives of the privacy laws. The PO's role may be filled by an organization's existing official for privacy (e.g., a Chief Privacy Officer)[11].

[11] Privacy official refers to the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO).

2.6.8 Role Assignment Policies

Although issuer roles are independent and should be filled by different people if feasible, there may be a need (e.g., because of availability or economy) to have one person fill more than one role. Except for the roles of Assessor and Privacy Official, one person may perform more than one role if needed. If an organization has established multiple issuers, one person may be assigned the same role in several or all of them. For instance, an Issuing Facility Manager may be responsible for a number of issuing facilities. Of the roles described, the SAO, DAO, OIMO, AR, Assessor and PO must be employees of the organization that owns the PCI or DPCI (e.g., Federal employees).

2.6.9Assessment and Authorization Roles

Figure 2 illustrates a possible role structure when an issuer has multiple issuing facilities. The SAO has the primary authority and responsibility for the issuing organization. Reporting to the SAO are the OIMO and the DAO. An Issuing Facility Manager is responsible for managing operations at each issuing facility and reports to the OIMO. The dotted lines leading to the PO and the Assessor indicate their independence from the day to day operations of the issuer.

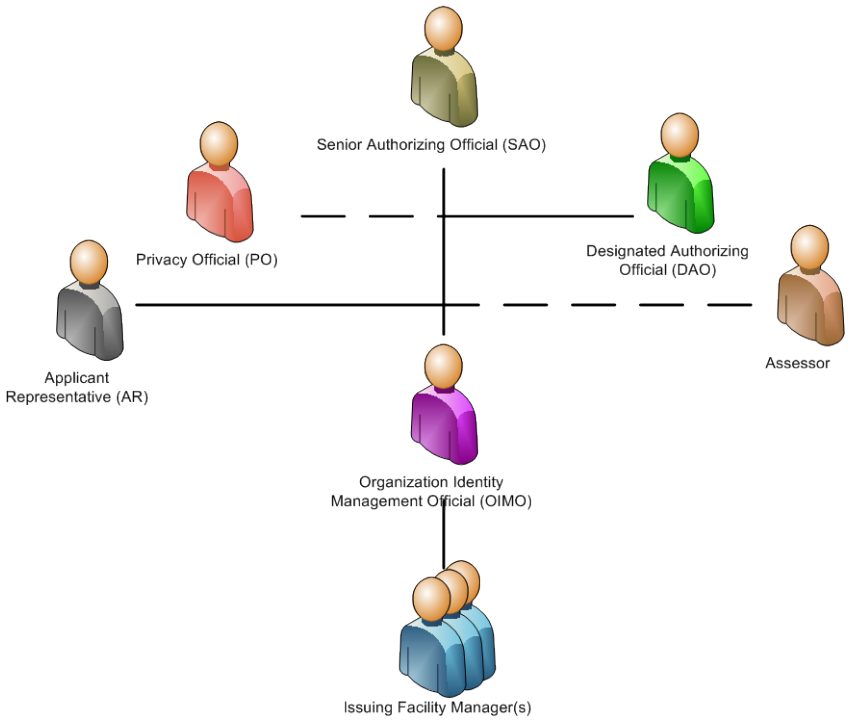

Figure 2 - Issuer Assessment and Authorization Roles

2.7 The Relationship between SP 800-79-2 and SP 800-37-1

While authorization is the major topic of both special publications, the goals of authorization are different in SP 800-37-1 and SP 800-79-2. Authorization under SP 800-37-1, as mandated by Appendix III of the Office of Management and Budget (OMB) Circular A-130, focuses on "authorizing processing" of information systems based on an assessment of security at the information system level. Authorization as discussed in this document and as mandated by HSPD-12 is concerned with the assessment of the "reliability" of an issuer to perform its

functions in accordance with FIPS 201-2. An authorization decision granted under SP 800-37-1 signifies that an organization official accepts responsibility for the security (in terms of confidentiality, integrity, and availability of information) of the information system. Authorization of an issuer's reliability under SP 800-79-2 indicates that the organization official accepts the responsibility that the issuer can operate within the control objectives outlined in HSPD-12 for "secure and reliable forms of identification" within an acceptable level of risk. However in both cases, the organization official (Authorizing Official (AO) in the case of SP 800-37-1, and DAO in the case of SP 800-79-2) is fully accountable for any adverse impacts to the organization if a breach in security, privacy, or policy occurs.

SP 800-79-2 focuses on the authorization of an organization's capability and reliability, but depends on adequate security for all the supporting information systems that have been authorized under SP 800-37-1. Therefore, before the organization official authorizes the issuer and its facilities, all relevant PCI or DPCI information systems used must be authorized.

In many cases, authorization under SP 800-37-1 will be granted by an organization official different than the official responsible for authorizing the issuer. The former is an organization official tasked with making a decision on whether to authorize operation of an information system based on its security posture. The latter must be someone designated specifically for authorizing the operation of an issuer after it has been assessed and determined to be compliant with FIPS 201-2 control objectives.

2.8 Preparing for the Assessment of an Issuer

To facilitate an assessment of an issuer in a timely, efficient, and thorough manner, it is essential that the staff of the issuer and members of the Assessment team understand their specific roles and responsibilities, and participate as needed. The issuer, its facility personnel, and the team responsible for performing the assessment must cooperate and collaborate to ensure the success of the assessment. Specific responsibilities of the assessment team are listed below. For further information, including considerations that an organization may want to take into account when outsourcing assessments refer to Draft NIST Interagency Report (IR) 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems.*

2.8.1 Issuer Duties

Before the assessment can begin, an Assessor must be designated. The Assessor[12] conducts the assessment and oversees the assessment team. The assessment team may be made up of employees from the organization or personnel provided by a public or private sector entity contracted to provide services. Members of the assessment team should have various capabilities that are required to perform the activities specified in this document. Assessment team members should work together to prepare for, conduct, and document the findings of the assessment within the authorization boundary. Each team must be made up of individuals that collectively have the knowledge, skills, training and abilities to conduct, evaluate, and document assessments, including those performed on the information systems being used by the issuer.

[12] The Assessor must be an employee of the organization that owns the PCI or DPCI.

Once an assessment team is in place, the OIMO and other relevant personnel should begin the preparation for the assessment. Thorough preparations by both the issuer organization and the assessment team are important aspects of conducting an effective assessment. The issuer sets the stage for the assessment by identifying all appropriate personnel and making them available during the assessment. A fundamental requirement for authorization is interviews by the assessment team of all issuer personnel. Personnel and officials must be notified of the pending assessment, must understand their roles in the process, and must be made available in accordance with the planned assessment schedule.

The OIMO must ensure that all relevant documentation has been completed and organized before the assessment begins. This documentation includes policies and procedures, organizational structure, information system architecture, product and vendor details, and specifics regarding the implementation of all the requirements from FIPS 201-2 and related publications. If the issuer has outsourced functions to an external service provider, all necessary documentation must be obtained from the provider regarding the outsourced operations. Before providing any documentation to the assessment team, the OIMO must review it to make certain it is complete, current and approved.

Another significant activity during the assessment is the observation by the assessment team of actual processes performed by the issuer. In order for the assessment team to confirm that processes are implemented in accordance with the operations plan, the issuer organization will need to ensure that assessment team members have access to facilities, and are able to observe PIV processes in real time. This could include scheduling activities to observe identity proofing, adjudication, card/token production, activation/issuance, and maintenance processes.

In order to aid the issuer's planning and preparation for the assessment, Appendix C includes an issuer readiness review checklist. This checklist contains items needed during the assessment process. Satisfying the list of items before the assessment commences will facilitate efficient utilization of the assessment team's time, and will contribute towards the overall effectiveness of the assessment activity.

2.8.2 Assessment Team Duties

The independence of the assessment team is an important factor in assessing the credibility of the assessment results. In order to ensure that the results of the assessment are impartial and unbiased, the members of the assessment team must not be involved in the development, day-to-day maintenance, and operations of the issuer, or in the removal, correction, or remediation of deficiencies.

The assessment team may obtain information during an assessment that the organization does not want to disclose publicly. The assessment team has an obligation to safely and securely store and protect the confidentiality of all security assessment related records and information, including limiting access to the individuals that need to know the information. When using, storing, and transmitting information related to the assessment, the assessment team shall follow the guidelines established by the organization in addition to all relevant laws, regulations, and standards regarding the need, protection, and privacy of information.

2.9 Authorization Decisions

An authorization decision is a judgment made by the DAO regarding authorizing operation of an issuer and its facilities. The DAO reviews the results of the assessment, considers the impact to the organization of any identified deficiencies, and then decides whether to authorize the operation of the issuer and its facilities. In doing so, the DAO agrees to accept the security and privacy risks of organization in issuing and maintaining PIV Cards or Derived PIV Credentials.

During the authorization decision process, the DAO must evaluate the assessment findings for the issuer and for each issuing facility within the authorization boundary. If the issuer has outsourced some of its services or functions, the DAO must review all relevant assessments and authorizations that have been granted to the external service provider and include them as a part of the overall evaluation of risk to the organization.

An authorization decision by a DAO must always be granted for a specific PCI or DPCI before commencement of operations, and for each issuer there can be only one authorization decision. In issuing this decision, the DAO must indicate the authorization boundary to which the authorization applies. A DAO grants an authorization to an issuer, and then specifies which facilities (along with any exceptions or restrictions) are permitted to operate under that authorization. This allows the issuer and any authorized issuing facilities to begin operations while any remaining facilities focus on addressing deficiencies identified during the assessment. At a later date, these latter facilities can be reassessed. After reviewing the new findings, the DAO can reissue the authorization for the issuer and expand the authorization boundary to which the authorization applies by including the newly assessed facilities.

The major input to the authorization decision is the assessment report. To ensure the assessment report is properly interpreted and the justification for the authorization decision properly communicated, the DAO should meet with the Assessor, the OIMO, and the Issuing Facility Manager(s) prior to issuing an authorization decision to discuss the assessment findings and the terms and conditions of the authorization.

There are three authorization alternatives that can be rendered by the DAO:

- Authorization to operate;
- Interim authorization to operate; or
- Denial of authorization to operate.

2.9.1 Authorization to Operate (ATO)

If, after reviewing the results of the assessment phase, the DAO deems that the operations of the issuer and its facilities conform to control objectives of FIPS 201-2 to an acceptable degree, and will continue to do so reliably during the authorization validity period, an *authorization to operate* (ATO) may be issued[13]. The issuer and its issuing facilities are authorized to perform services in compliance with all relevant policies, in conformance to all relevant standards, and in

[13] Note The PCI/DPCI ATO can be affected by the underlying system authorization status (see Section 2.9.4).

accordance with the documented operations plan. The DAO shall indicate exactly which issuing facilities are included in the ATO authorization decision. An ATO can only be granted to an issuer if there are no limitations or restrictions imposed on any of its issuing facilities that are included in the authorization boundary. The ATO is transmitted to the OIMO.

After receiving an ATO under SP 800-79-2, re-authorization shall be performed within three (3) years, or when there is a significant change in personnel or operating procedures (includes both improvement and degradation of operations) or when additional issuing facilities are being added to the issuer organization. There may also be cases where one or more issuing facilities cease operation. If this situation results in a PIV service identified in the operations plan becoming unavailable, then the DAO must issue a Denial of Authorization to Operate (DATO - See Section 2.9.3). On the other hand, if the issuer can continue to provide all services in the operations plan, then the authorization decision letter has to be modified to exclude those issuing facilities that have ceased operations (thus revising the authorization boundary). The required re-authorization activities are at the discretion of the DAO and based on the extent and type of change.

2.9.2 Interim Authorization to Operate (IATO)

If, after reviewing the results of the assessment phase, the DAO deems the discrepancies to be significant, but there is an overarching necessity to allow the issuer to operate, an *interim authorization to operate (IATO)* may be issued[14]. An interim authorization to operate is rendered to an issuer when the identified deficiencies are significant, but can be addressed in a timely manner. These deficiencies must be documented so that they can be addressed during the planning of corrective actions. An interim authorization is an authorization to operate under specific terms and conditions. The DAO shall indicate exactly which facilities are included in the IATO authorization decision during this interim period, along with any limitations or restrictions imposed. The maximum duration of an IATO is three (3) months. A maximum of two (2) consecutive IATOs may be granted. Failure to correct deficiencies after the expiration of the second IATO must result in an issuance of a denial of authorization to operate (DATO) for the issuer. The authorization boundary may be revised to exclude issuing facilities that exhibit significant deficiencies in performing their functions. The IATO is transmitted to the OIMO.

An issuer is *not considered* authorized during the period of an IATO. When the deficiencies have been corrected, the IATO should be replaced with an ATO. Significant changes in the status of an issuer (e.g. addition of new issuing facilities) that occur during the IATO period shall be reported immediately to the DAO.

2.9.3 Denial of Authorization to Operate (DATO)

If, after reviewing the results of the assessment phase, the DAO deems operation of the issuer to be unacceptable, a denial of authorization to operate (DATO) shall be transmitted to the OIMO. Failure to receive authorization to operate indicates that there are major deficiencies in reliably meeting the requirements of FIPS 201-2 and its related documents. The issuer is not authorized and must not be allowed to operate. If issuance services are currently in operation, all functions must be halted including all operations at the any issuing facility. If an issuer was previously

[14] Note The PCI/DPCI IATO can be affected by the underlying system authorization status (see Section 2.9.3).

authorized and had issued PIV Cards or Derived PIV Credentials under an ATO, the OIMO along with the Issuing Facility Manager(s) should consider whether a revocation of PIV Cards and their Derived PIV Credentials are necessary. The DAO and the Assessor should work with the OIMO and Issuing Facility Manager(s) to ensure that proactive measures are taken to correct the deficiencies.

2.9.4Authorization Impact of Information Systems under NIST SP 800-37

An issuer must not be authorized to operate if one or more of its critical information systems is deemed insecure and therefore is issued a DATO under SP 800-37-1. In the case where an IATO (under SP 800-37-1) has been issued for an information system, the DAO may issue no greater than an IATO for the issuer. Once the SP 800-37-1 IATO is replaced with an SP 800-37-1 ATO, the DAO can issue a SP 800-79-2 ATO. If the SP 800-37-1 ATO expires for one or more of information systems during the course of operation of an issuer, the OIMO shall assess the criticality of the system for operations and present the analysis to the DAO. The DAO then can exercise the following options:

- Specify a short time during which the information systems of the issuer must be re-authorized under SP 800-37-1 without changing the ATO status;
- Downgrade the current SP 800-79-2 ATO to an IATO; or
- If circumstances warrant, issue a SP 800-79-2 DATO and halt all issuer operations.

2.10 The Use of Risk in the Authorization Decision

Authorization is the official management decision by the DAO to permit operation of an issuer based on an assessment of its reliability and an acceptance of the risk inherent in that decision. By granting an authorization to operate, the DAO accepts responsibility for the reliability of the issuer and is fully accountable for any adverse impact to the organization or any other organization from the use of issued PIV Card or Derived PIV Credentials.

The assessment of an issuer provides the DAO with the basis for not only determining its reliability, but also for determining whether to accept the risk to the organization in granting an ATO. As the requirements in FIPS 201-2 and related documents form the basis of the authorization and are ultimately derived from the policy objectives of HSPD-12, those not reliably met by the issuer and its issuing facilities represent the potential for adverse impact.

Implementation of an HSPD-12 program exposes an organization to specific risks at the mission level of the organization. The PIV Card is used to establish assurance of an identity, and as such, it must be trusted as a basis for granting access to the logical and physical resources of the organization. Similarly, the Derived PIV Credential is also used to establish the assurance of an identity, and must be trusted as a basis for granting access from mobile devices to the remote IT resources of the organization. Any problem with an issued PIV Card or Derived PIV Credential that undermines this assurance could expose an organization to harm. Furthermore, the collection, processing, and dissemination of personal information is required to issue these

credentials and thereby increases the threat of this information being used for malicious purposes[15] if not secured. It is the DAO's responsibility to weigh the risks of these and other security and privacy impacts when making the authorization decision. Furthermore, as HSPD-12 is a government-wide mandate based on a standard of interoperability allowing organizations to accept other organizations' credentials, authorization decisions within a single organization directly impact other organizations. For example, an interoperable credential issued by an authorized organization becomes the source of trust for another organization to grant access to physical and logical resources, based on verification of that identity. The DAO's signature on the authorization letter thus signifies his/her acceptance of responsibility (i.e., accountability) for the operations of the issuer, not only to the issuing organization, but also to other organizations that are in the federated circle of trust.

2.11 Authorization Submission Package and Supporting Documentation

The *authorization submission package* documents the results of the assessment phase and provides the DAO with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the issuer. Unless specifically designated otherwise by the DAO, the OIMO is responsible for the assembly, compilation, and presentation of the authorization submission package. The authorization submission package contains the following documents:

- The operations plan (including all Issuing Facilities Standard Operating Procedures (SOPs) and attachments)
- SP 800-37-1 authorization letters
- The assessment report
- The Corrective Actions Plan (if required) (CAP)

The operations plan contains the policies, procedures, and processes for all the major PIV functional areas. The operations plan provides a complete picture of the structure, management, and operations of an issuer to the Assessor and DAO. Appendix D provides templates of what to include in the operations plan for PIV Card Issuers and for Derived PIV Credential Issuers. One of the most significant pieces of information contained within the operations plan is the list of issuer controls, how they were implemented, and who is responsible for their management. This description of the issuer controls makes it a simple process for the Assessor to quickly ascertain how they were implemented and by whom.

If certain functions described in the operations plan are outsourced, the operation plan can reference or "point to" the external service provider's operation plan and related documentation, such as support agreements and any contracts. In this manner, the Assessor has access to the information regarding the external service provider's operations without requiring the issuer to duplicate any documentation. Upon receiving and reviewing the authorization package and in consultation with the Assessor, the DAO decides whether to authorize operations of the issuer.

[15] Note: PII collection is minimized for Derived PIV Credentials because of the derivation process.

The authorization decision letter transmits the authorization decision from the DAO to the OIMO. The authorization decision letter contains the following information:

- Authorization decision;
- Supporting rationale for the decision; and
- Terms and conditions for the authorization, including which issuing facilities (Authorization Boundary) are included.

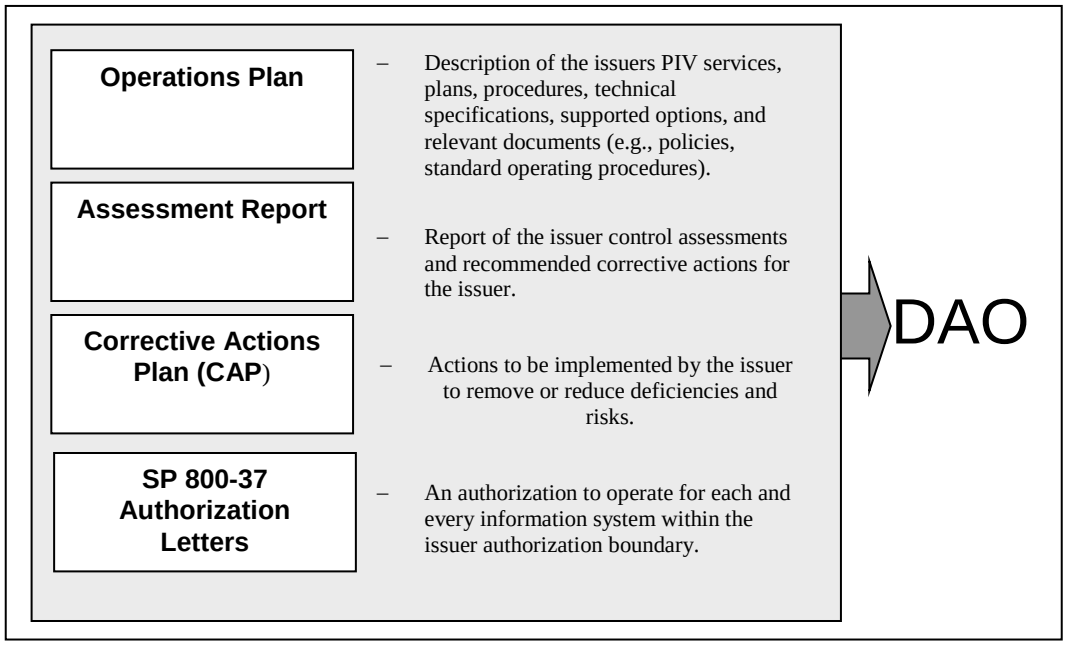

Figure 3 - Authorization Submission Package

The authorization decision letter (see Appendix F for examples) informs the OIMO that the issuer is— (i) authorized to operate; (ii) authorized to operate on an interim basis; or (iii) not authorized to operate. The supporting rationale includes the justification for the DAO's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the issuer, including which issuing facilities are included in the decision. The authorization decision letter is attached to the authorization submission package and becomes the authorization decision package.

The DAO sends the authorization decision package to the OIMO and retains a copy of it. The OIMO carefully reviews the terms and conditions of authorization before initiating the necessary steps for issuer operations. Both parties mark the authorization decision package appropriately for storage under the organization's record retention policy.

3. TAXONOMY OF ISSUER CONTROLS

3.1 Introducing Issuer Controls

Assessment of a PIV Card or Derived PIV Credential Issuer is a broader endeavor than assessment of the security of an information system under SP 800-37-1. The requirements specified in Federal Information Processing Standard (FIPS) 201-2 cover all major aspects of an issuer, including organizational preparedness; security management and data protection; infrastructure; and issuance processes. Each broad area is defined herein as an Issuer Authorization Topic (IAT). In addition to providing structure to the assessment, IATs are also used to summarize the assessment results for reporting. In addition, they are used to structure the report to senior organization management that provides an analysis of the strengths and weaknesses within an issuer organization.

The Issuer Authorization Topics (IAT):

- **Organizational Preparedness** relates to the capability, knowledge, and understanding of senior management regarding the formation and operation of the issuer. Roles and responsibilities must be clearly identified, and policies and procedures must be defined, documented, implemented, and enforced.

- **Security Management & Data Protection** involves implementing and operating appropriate security management procedures, operational controls, and technical protection measures to ensure that privacy requirements are satisfied, the rights of individuals are assured, and personal data is protected.

- **Infrastructure Elements** represents the activities required to procure, deploy, and maintain the information system components used for issuance of PIV Cards or Derived PIV Credentials tokens. These information system components (e.g., PKI, biometrics, card or token personalization, etc.) must meet the technical specifications defined in FIPS 201-2 and related documents and need to be authorized under Special Publication (SP) 800-37-1 for FISMA compliance.

- **Processes** are classes of functions that collectively span the entire lifecycle activities[16], such as sponsorship, identity proofing/registration, adjudication, card /token production, activation/issuance, and maintenance of the PIV Card and the Derived PIV Credential.

Each IAT is sub-divided into one or more Authorization Focus Areas. A focus area is a set of closely-related requirements that need to be met by an issuer. Under each focus area is a procedure or technical product (termed an "Issuer Control") that is used to satisfy a particular requirement listed under a focus area. However, the manner in which the requirements are satisfied and how the specifications are implemented and managed may vary from organization to organization.

[16] Note: Some of the processes may not apply to Derived PIV Credential issuers.

For instance, each issuer (but not DPCI) is required to identity-proof their applicants (i.e., use due diligence in validating the claimed identity of the applicant). This process can be implemented in one of several ways, depending upon the structure, size, and geographical distribution of the organization's facilities. The process could be conducted at a central location or distributed throughout the country within regional centers. It could be operated directly by the organization or by an outside service provider. However, irrespective of the implementation approach, this identity proofing/registration activity must be reliably and accurately performed.

The evidence that ensures the presence of issuer controls that are derived from FIPS 201-2 requirements and its related documents as well as OMB Memoranda, and verified through appropriate assessments, establishes the capability of the issuer. However, authorization is generally based not merely on the demonstration of capability, but also on the presence of certain organizational characteristics that will provide a high degree of confidence to the Assessor that the demonstrated capabilities will be carried out in a dependable and sustainable manner. This dependability measure, or reliability (as it is generally called), has to be established by adequately assessing that an issuer has the desired organizational characteristics, including adequate issuing facilities, appropriate equipment, trained personnel, adequate resources, trustworthy management, and properly vetted operations staff. Hence, the assessment and authorization methodology includes a set of issuer controls, verification of which establishes the reliability of the issuer. This set of controls is grouped under the IAT's Authorization Focus Area called- "Facility and Personnel Readiness". These reliability-relevant issuer controls are formulated, based on "commonly accepted security readiness measures" that have evolved in response to lessons learned in security incidents that have taken place due to threats, such as insider attacks, and risks, such as physical security lapses. In addition to the controls provided herein, an organization may develop additional mission-specific controls that will contribute towards the overall reliability of the issuer to meet the organization's mission needs.

Table 1 provides a listing of the four Issuer Authorization Topics (IATs) and associated Authorization Focus Areas under each topic:

Organizational Preparedness
Preparation and Maintenance of Documentation (DO)
Assignment of Roles and Responsibilities (RR)
Facility and Personnel Readiness (FP)
Security Management & Data Protection
Protection of Stored and Transmitted Data (ST)
Enforcement of Applicable Privacy Requirements (PR)
Infrastructure Elements
Deployed Products & Information Systems (DP)
Implementation of Credential Infrastructures (CI)
Processes
Sponsorship Process (SP)
Identity Proofing/Registration Process (EI)
Adjudication Process (AP)
Card/Token Production Process (CP)
Activation/Issuance Process (AI)
Maintenance Process (MP)

Table 1 - IATs and Associated Authorization Focus Areas

Appendices G.1 and G.2 contains required issuer controls grouped by IAT and associated Authorization Focus Area for a PCI and a DPCI respectively. Each issuer control represents how one or more requirements from FIPS 201-2 and its related documents can be satisfied. Issuer controls are sequentially numbered using the two-character identifier assigned to the Authorization Focus Area under which they are listed. Identifiers for issuer controls applicable to both PCIs and DPCIs are aligned for ease of reference. In addition, controls for DPCIs are marked with (DC) for quick identification. For example, DO-1 applies to a PCI and DO(DC)-1 applies to a DPCI. Both these issuer controls are targeted at assessing the same requirement.

Table 2 shows the relationships between IATs, Authorization Focus Areas, and issuer controls for a PIV Card Issuer.

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Preparation and Maintenance of Documentation (DO)	DO-1	The organization develops and implements an operations plan according to the template in Appendix D.1. The operations plan references other documents as needed.	SP 800-79-2, Section 2.11 – Authorization Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for identity proofing and registration that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency.	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements

Table 2 - IAT, Authorization Focus Area, and Issuer Control Relationships for PCIs

Unlike for a PIV Card Issuer, not all issuer controls are applicable to a Derived PIV Credential Issuer. Certain issuer controls are applicable to only Level of Assurance 3 (LOA-3) or to only LOA-4 PIV Derived Credentials and therefore must be implemented by the issuer only if they are issuing that level of a Derived PIV Credential. This is represented via the "*applicability*" column within Appendix G.2 for DPCIs as seen in Table 3. Controls with an applicability column marked with DPCI (e.g., without LOA-4 or 3 postfix) applies to both LOA-3 and LOA-4 Derived PIV Credential.

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Maintenance Process	MP(DC)-17	If the PIV Derived Authentication private key was created and stored on a hardware cryptographic token that does not permit the user to export the private key, then termination of the Derived PIV Credential is performed by collecting and either zeroizing the private key or destroying the token. Otherwise, termination is performed by revoking the PIV Derived Authentication certificate.	DPCI – LOA 4 Only	SP 800-157, Section 2.3 – Termination
	MP(DC)-18	The linkage between the Derived PIV Credential and the subscriber's PIV Card is updated when the subscriber obtains a new PIV Card (e.g., the subscriber obtains a replacement PIV Card after compromise of their original PIV Card).	DPCI	SP 800-157, Section 2.4 – Linkage with PIV Card

Table 3 - IAT, Authorization Focus Area, Issuer Control and Applicability Relationships for DPCIs

Irrespective of whether the information systems utilized by the issuer and its issuing facilities are categorized at low, moderate, or high impact levels according to FIPS 199, the same set of issuer controls apply, regardless of an individual system's impact level. Furthermore, nothing precludes an issuer from implementing additional controls to ensure a higher level of confidence in mitigating risks associated with issuing PIV Cards or Derived PIV Credentials.

3.2 Implementing Issuer Controls

Each issuer control must be properly implemented, managed, and monitored in order for the issuer to be authorized. Depending on how an organization decides to implement their HSPD-12 program, the authority to implement some of the controls may not directly come under the management of the issuer organization (due to outsourcing of certain PIV processes or using the issuing facilities of other organizations). However, it is still the responsibility of the management of the issuer organization to ensure that these issuer controls are being deployed, enforced, and maintained by its service provider.

3.2.1 Issuer Controls implemented at the Organization or Facility Level

The nature of each issuer control dictates where it is implemented. Controls that are common to or impact multiple PIV processes are implemented at the organization level. The development of the operations plan is an example of an issuer control implemented at the organizational level. Generally, controls specific to a process are implemented at the issuing facility where that process or function is carried out. For example, the control that states that a "1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record must be performed before releasing the PIV Card to the applicant" is implemented at an activation/issuance facility.

For Derived PIV Credentials issued at LOA-3, an issuer may implement all the requirements necessary to issue these credentials remotely. In such a case, the issuer may not need to have an issuing facility and issuing facility-specific controls may not be applicable. Regardless of the system and process architecture on how PIV Card and Derived PIV Credentials are issued, it is the responsibility of issuer organization to ensure that all applicable controls are implemented.

4. ISSUER CONTROLS ASSESSMENT & AUTHORIZATION DECISION PROCESS

An assessment is a set of activities performed by the Assessor to gain assurance that the issuer controls for a PIV Card Issuer (PCI) or a Derived PIV Credential Issuer (DPCI) have been implemented properly and meet their required function or purpose. Understanding the overall effectiveness of the issuer controls implemented by the issuer and its facilities is essential in determining the risk to the organization's overall mission, and forms the basis for the authorization decision by the Designated Authorizing Official (DAO).

An Assessor must– (i) compile evidence that the issuer controls are implemented correctly, operating as intended, and producing the desired results; and (ii) present this evidence in a manner such that the DAO can make a credible, risk-based decision about the operation of the issuer.

The focus of an assessment is the issuer controls, each of which is designed to satisfy one or more specific requirements from FIPS 201-2 and related documents. The objective for the Assessor is to use the assessment procedures associated with each issuer control (described in Appendix G) as a means to measure conformance to the requirements. The assessment procedures are designed to facilitate the gathering of evidence that issuer controls are implemented correctly, operating as intended, and producing the desired outcome.

In preparation for an assessment, the Assessor performs the following two preparatory steps:

- Determination of the authorization boundary to understand the target of the assessment. The authorization boundary dictates which issuing facilities and outsourced services are to be included in the assessment.

- Review of the operations plan to determine which issuer controls are implemented at the organizational level and which at the facility level. This analysis should provide the Assessor with an understanding of where different responsibilities lie within the issuer organization and how to address them during the assessment.

In cases where PIV functions have been outsourced, the issuer is responsible for ensuring that the external service provider has implemented the control. During the assessment, it is the service provider's responsibility to provide documentation to the Assessor regarding the implementation of that control. If results from a previous assessment of the service provider (provided the current assessment is part of re- authorization after substantial changes) can be referenced, the Assessor may elect to incorporate these results (not exceeding one year) or re-do part or all of the assessment. The extent of re-use of the results of the previous assessment is entirely at the discretion of the Assessor.

Issuer controls implemented at the organizational level generally need to be assessed only once, since these controls span across the entire issuer and its issuing facilities. In other words, these controls may not be re-assessed when the authorization boundary changes (e.g., due to addition of facilities). Examples of organizational level controls include the set of controls under the authorization focus areas Preparation and Maintenance of Documentation (DO) and Assignment of Roles and Responsibilities (RR).

There are certain controls that although they are put in place at the organizational level, they need to be reviewed at the issuing facility level. An example of such a control artifact is "contingency/disaster recovery plan for information systems". Though the development of the contingency/disaster recovery plan is an organizational level control, a review of this control artifact is needed whenever new information systems in the existing facilities or new facilities are added to ensure that these new systems are brought within the scope of the plan.

Unlike organization level issuer controls, facility level issuer controls need to be assessed individually at each facility. A facility is often designated based on the type of PIV process it performs (exceptions are the Sponsorship Process and Adjudication Process). Hence, for example, if there are multiple facilities for identify proofing/registration (e.g., multiple registration centers), assessment of the issuer controls under the focus area identity proofing/registration, should take place in each of the enrollment centers. However, if all facilities are operating using uniform operational procedures and underlying information systems, it is acceptable to perform assessments at facilities that are selected randomly or through some other established criteria (e.g., geographical region or service provider).

Prior assessments may be used as a starting point for the assessment of an issuer. While past assessments provide insight into the implementation and operation of an issuer, a number of factors affect the validity of past assessments. These include updates in policies and procedures, changes in systems/technology, and turnover in employees and contractors. Any significant changes in one or more of these factors should trigger a new assessment. The Assessor must validate whether the issuer is currently operating as expected using the given assessment procedures, including specially tailored or augmented procedures. It is only through a current valid assessment of issuer controls that the Assessor and Organization Identity Management Official (OIMO) will have confidence in the reliability of the issuer and its issuing facilities.

The use of automated security controls, if reliably implemented and maintained in information systems, results in a high assurance of the protection of information and other organizational assets. Human involvement results in more variability in how issuer controls are implemented and operated, as security and reliability depend on many factors, including an individual's training, knowledge, motivation, experience, and management. Relying on humans for data protection, rather than on reliable, automated security mechanisms, makes it critical that trust and reliability assessments of management, operators, and maintenance personnel are current and up-to-date. Many of the assessment procedures rely on interactions among the Assessor, issuer management, and facilities staff. Interviews with all involved personnel and observations of all PIV processes are required. On-site visits, real-time observations, and reviews of processes are essential, as the Assessor must not rely solely on documentation to determine if a given issuer control has been implemented.

4.1 Assessment Methods

In order to assess the capability and reliability of an issuer, one or more assessment procedures associated with each issuer control have to be completed. An assessment procedure is carried out using one or more of the following assessment methods. (The assessment methods associated with an assessment procedure are given in parenthesis in Appendices G.1 & G.2.)

- *Review* – An evaluation of documentation that describes plans, policies, and procedures in order to verify that they are adequate, understood by management and operations personnel, and that they are in accordance with applicable policies, regulations, standards, technical guidelines, and organizational guidance.
- *Interview* – a directed conversation with one or more issuer personnel in which both pre-established and follow-on questions are asked, responses documented, discussion encouraged, and conclusions reached.
- *Observe* – a real-time viewing of PIV processes in operation, including all information system components of the issuer involved in creation, issuance, maintenance, and termination of PIV Cards or Derived PIV Credentials.
- *Test* – an evaluation of a component against a set of relevant PIV specifications using applicable test methods and metrics (as given in the associated assessment procedure in Appendix G.1 and G.2).

These methods are intended to provide the Assessor with sufficient, precise, accurate, and relevant evidence regarding an IAT topic and its focus areas. One or more assessment methods may be required to determine if the issuer has satisfactorily met the objective outlined for that assessment procedure. Assessment results are used by the Assessor to determine the overall effectiveness of the issuer control.

Table 4 shows an example of the relationships among an IAT, an Authorization Focus Area, several issuer controls, and their assessment procedures. Controls with an applicability column marked with DPCI (e.g., without LOA-4 or 3 postfix) applies to both LOA-3 and LOA-4 Derived PIV Credentials.

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Preparation and Maintenance of Documentation	DO(DC):1	The organization develops and implements an issuer operations plan according to the template in Appendix D.2. The operations plan references other documents as needed. **Assessment** *Determine that:* *(i) the operations plan includes the relevant elements from the template in Appendix D.2 (review);* *(ii) the operations plan includes the list of issuer controls and the issuer control owner for each, how they were implemented and whether they are organization or facility specific (review);* *(iii) documentation that is not included in the operations plan is referenced accurately (review);*	DPCI	SP 800-79-2, Section 2.11 – Authorization Package and Supporting Documentation

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
		(iv) the operations plan has been reviewed and approved by the DAO within the organization (review, interview).		
	DO(DC):3	The organization has a written policy and procedures for initial issuance that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for issuance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal department or agency (review);* (iv) *the organization will periodically review and update the policy and procedures as required (review, interview).*	DPCI	SP 800-157, Section 2 Lifecycle Activities and Related Requirements SP 800-157, Section 2.1 – Initial Issuance

Table 4 – Sample Issuer Controls with Assessment Procedures (for DPCI)

Some organizations may need to customize some of the issuer controls to meet their specific characteristics and mission needs. In such cases, the associated assessment procedures may also have to be customized/augmented to ensure proper implementation of these controls.

4.2 The Issuer Assessment Report

The Assessment report contains the results of the assessment in a format that facilitates reviewing by the DAO. The DAO must evaluate the information in the Assessment Report in order to make a sound, credible decision regarding the residual risk of authorizing the operations of the issuer.

An Assessment Report template is provided in Appendix E. The report is organized by Authorization Focus Area. For each issuer control, it must be documented as to which entity is

responsible for the implementation of that control (the organization or an external service provider) and if the issuer control is at the organizational or facility level.

Activation/Issuance Process

Issuer Control Identifier— AI-7

Control Description— Before the PIV Card is provided to the applicant, the issuer performs a 1:1 biometric match of the applicant against biometrics available on the PIV Card or in the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. If the match is unsuccessful, or if no biometric data is available, the cardholder provides two identity source documents (as specified in Section 2.7), and an attending operator inspects these and compares the cardholder with the facial image printed on the PIV Card.

Control Owner/ Control Level — External Service Provider/Facility Level

ASSESSMENT DETAILS

Assessment Method(s):

Review: Operations Plan

Observe: Activation/Issuance Process

Assessment Result— **Partially Satisfied**

Assessment Findings— There is operational evidence that a 1:1 biometric match is carried out before the card is released to the applicant.

Assessment Deficiency and Potential Impact— The requirement to carry out this task is not documented clearly enough in the operations plan. Although personnel are knowledgeable about this requirement, and the task was observed to be performed correctly during card issuance, the lack of documentation could be a problem if there is turnover in staff. Alternate processes when fingerprints are unavailable are not in place.

Recommendation— Update the issuance process description within the operations plan to include a clear description of this task in the process and develop alternate processes for issuance when fingerprints are not available.

Figure 4 - Sample Issuer Control Assessment Result (for DPCI)

The assessment result for each issuer control shall be one of the following:

- Satisfied
- Partially Satisfied
- Not Satisfied
- Not Applicable

After carrying out an assessment procedure, the Assessor records his/her conclusion in one of two ways: MET, NOT MET. Using the list of conclusions pertaining to assessment procedures associated with an issuer control, the assessment result (which is one of the 4 outcomes listed above) is arrived at as follows:

- If the conclusion from all assessment procedures is MET, then the assessment result for the issuer control is "Satisfied"
- If some of the conclusions are NOT MET, then the assessment result for the issuer control is marked as either "Partially Satisfied" or "Not Satisfied", depending on whether or not any of the underlying tasks in the assessment procedures are critical (i.e., they represent the only way to meet the issuer control's objective). An example of an assessment that resulted in "Partially Satisfied" is given in Figure 4. In this instance, there is an awareness of a task requirement, and the task itself is being carried out, but the reference to the task is missing in the document.

In drawing a conclusion after carrying out an assessment procedure, the Assessor must consider the potential subjective and objective aspects of the assessment methods used (e.g., interviews, document reviews, observations, and tests) for that assessment procedure. Deficiencies that result in "Partially Satisfied" or "Not Satisfied" must be reported by the Assessor. The Assessor must also outline the potential adverse impacts if the issuer control is deployed with the identified deficiencies.

The assessment report template provides the means for recording the assessment result for each issuer control. The assessment results for all issuer controls are aggregated to generate the assessment result for an Issuer Authorization Focus area. The set of Issuer Authorization Focus Area results are aggregated to generate Issuer Authorization Topic results. Finally, the group of Issuer Authorization Topic results is used to generate the overall Issuer Assessment Report and an accompanying Executive Summary (intended for Senior Management).

5.0 ASSESSMENT & AUTHORIZATION LIFECYCLE

The authorization of a PIV Card Issuer (PCI) or a Derived PIV Credential Issuer (DPCI) consists of four phases: (i) Initiation; (ii) Assessment; (iii) Authorization; and (iv) Monitoring. Each phase consists of tasks and sub-tasks that are to be carried out by the responsible officials (e.g., the Designated Authorizing Official (DAO), Assessor, Organization Identity Management Official (OIMO), and Issuing Facility Manager(s)). Figure 5 provides a view of the authorization phases, including the tasks associated with each phase. A table of authorization phases, tasks, sub-tasks, and the official responsible for each is provided in Appendix H.

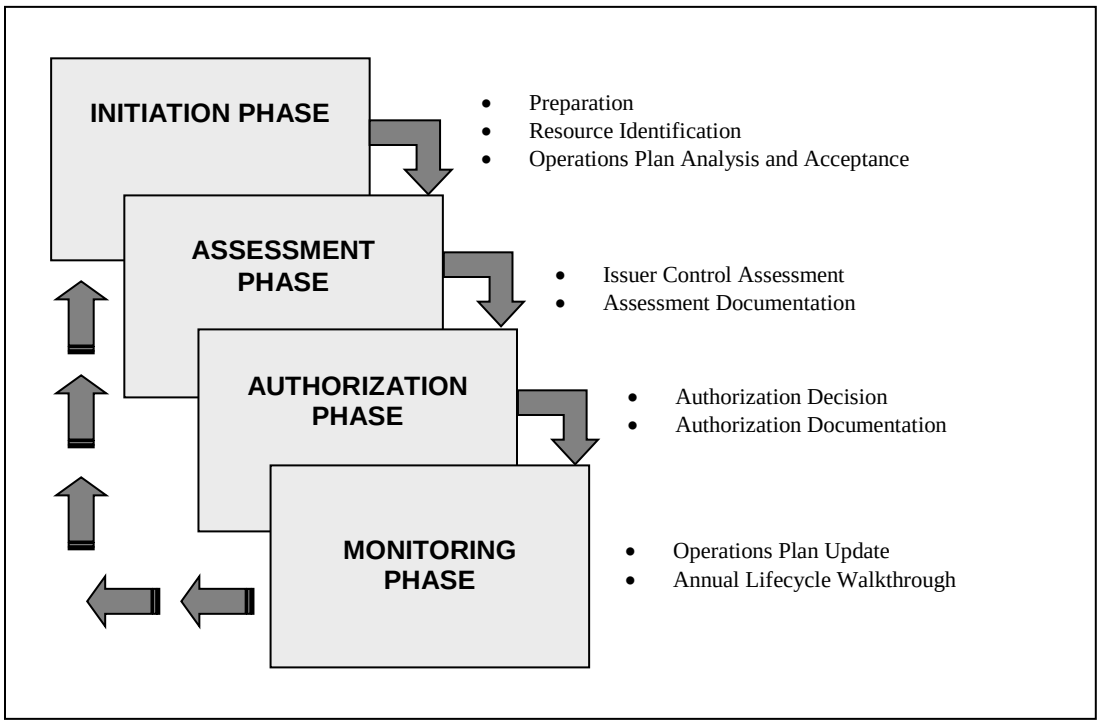

Figure 5 - Authorization Phases

5.1 Initiation Phase

The Initiation Phase consists of three tasks: (i) preparation; (ii) resource identification; and (iii) operations plan analysis and acceptance. The primary purpose of this phase is to ensure that the issuer is prepared for the assessment, including having all the resources and documentation in place. The other purpose of this phase is to include the DAO early in the process in order to assure success of the assessment and authorization.

Task 1: Preparation

The objectives of this task are to prepare for authorization by reviewing the operations plan and confirming that the plan is consistent with Federal Information Processing Standard (FIPS) 201-2 and the template provided herein.

Subtask 1.1: Confirm that the operations of the issuer have been fully described and documented in their operations plan.

Responsibility: OIMO

Guidance: The operation plan includes, at a minimum, the sections defined in the operations plan template in Appendices D.1 or D.2 depending on whether the issuer is issuing PIV Cards or Derived PIV Credentials. An issuer of both PIV Cards and Derived PIV Credentials may develop a single operations plan that addresses both without repeating common elements. It is the OIMO's responsibility to ensure that the organization's operations plan incorporates a complete and accurate description of the issuer's operations. If a process or function is provided by an external service provider, their operating procedures should be documented and incorporated by reference in the issuer's operations plan. In this case, the operations plan includes a pointer, guiding the reader to additional documentation and information.

Subtask 1.2: Confirm that processes performed are conducted in accordance with the policies and procedures specified in the issuer's operations plan and are documented in standard operating procedures.

Responsibility: OIMO, Issuing Facility Manager

Guidance: Even though an issuer may be following requirements from FIPS 201-2, their processes need to be consistent within their operations plan and documented in standard operating procedures.

Task 2: Resource Identification

The objectives of the resource identification task are to– (i) identify and document the resources required for assisting with the assessment; (ii) identify the scope of the assessment and authorization boundary; and (ii) prepare a plan of assessment activities indicating the proposed schedule and key milestones.

Subtask 2.1: Identify the Senior Authorizing Official (SAO), Designated Authorizing Official (DAO), Privacy Official (PO), Issuing Facility Managers, Assessor, and other key personnel at the facility level who are performing functions, such as identity proofing/registration, card production, and activation/issuance. Maintenance personnel also should be contacted to provide requested assessment information to the Assessor.

Responsibility: OIMO

Guidance: Notify these individuals of the upcoming assessment, and inform them of the need for their participation during the process.

Subtask 2.2: Determine the authorization boundary for the issuer.

Responsibility: OIMO; DAO

Guidance: The authorization boundary determines the target of the assessment. In preparation for the issuer assessment, the OIMO and DAO should identify which issuing facilities and external service providers are to be included. This

ensures that functions performed and processes managed by the external service provider are considered during the authorization process. An organization may want to include only those issuing facilities that are ready to operate; other facilities can be assessed at a later date.

Subtask 2.3: Determine the resources and the time needed for the assessment of the issuer, and prepare a plan for execution of the assessment.

Responsibility: OIMO; DAO

Guidance: The level of effort required for an assessment depends on numerous factors— (i) the size of the issuer; (ii) the location and number of its facilities; (iii) the level of outsourcing utilized by the issuer; and (iv) the number of cards and/or derived credentials being, or to be issued. By examining factors that could influence the complexity of the assessment, the organization can make informed judgments about the size of the assessment team, the resources needed to support the assessment, and the time-frame for completing it.

Task 3: Operations Plan Analysis and Acceptance

The objectives of the operations plan analysis and acceptance task are: (i) determine if the requirements of FIPS 201-2 have been implemented; (ii) evaluate the operations plan and revise as needed; and (iii) obtain acceptance of the plan by the DAO prior to conducting an assessment of the issuer controls.

Subtask 3.1: Review the list of required issuer controls documented in the organization's operation plan and then confirm that they have been implemented properly.

Responsibility: DAO; OIMO

Guidance: Since the issuer controls serve as the basis for the assessment, review the operations plan and supporting documentation to identify the controls that must be implemented before investing time in assessment activities such as interviews or testing. The operations plan must document each issuer control, whether it is organization or facility specific, the owner of the issuer control, and how the control is implemented.

Subtask 3.2: Analyze the operations plan to determine if there are deficiencies in satisfying all the policies, procedures, and other requirements in FIPS 201-2 that could result in a Denial of Authorization to Operate (DATO) being issued. After discussing the discovered deficiencies in the documentation and operations plan with the OIMO, the organization may still want to continue with the assessment, if it has determined that it can address all deficiencies within the time period of the current assessment. In this situation, the DAO can either authorize continuation of the assessment or terminate the assessment effort depending upon the evaluation of the issuer's ability to address the deficiencies.

Responsibility: DAO, OIMO

Guidance: The operations plan should adequately specify the policies, procedures, and processes of the issuer so that, subsequent to an initial review, deficiencies that could lead to an eventual DATO may be identified and remediated as soon as possible.

Subtask 3.3: Verify that the operations plan is acceptable.

Responsibility: DAO

Guidance: If the operations plan is deemed acceptable, the DAO should authorize the authorization processes to advance to the next phase. Acceptance of the operations plan signifies that the resources required to initiate and complete the authorization activities may be deployed.

5.2 Assessment Phase

The Assessment Phase consists of two tasks— (i) issuer control assessment; and (ii) assessment documentation. The purpose of this phase is to determine the extent to which the requirements of FIPS 201-2 are implemented correctly, operating as intended, and producing the desired outcomes. This phase also specifies actions to be taken to correct all identified deficiencies. An analysis of the impact of identified deficiencies that cannot be corrected or mitigated efficiently on the reliable operation of the issuer should be conducted and documented. Successful completion of this phase should provide the DAO with the information needed to make an appropriate authorization decision.

Task 4: Issuer Control Assessment

The objectives of this task are to— (i) initiate and conduct an assessment of the issuer controls; and (ii) document the results of the assessment. The Assessor shall first verify the acceptability of all documentation, including the operations plan and previous assessments, along with all relevant Federal laws, regulations, standards, and directives. Issuer control assessment should then commence. The Assessor should schedule interviews, schedule real-time observations of issuance processes, and initiate all needed testing of the PIV Card, Derived PIV Credential and relevant information system components. Once the Assessor has gathered the results of the assessment procedures, descriptions of all discovered deficiencies shall be prepared, along with recommendations for removing these deficiencies.

Subtask 4.1: Review the suggested and selected assessment methods for each issuer control in preparation for the assessment.

Responsibility: Assessor

Guidance: Based on the authorization boundary, the scope of the assessment should be established. The Assessor should review the selected assessment procedures (based on the scope of the assessment) in order to plan and coordinate activities for the assessment. For instance, if a particular issuer control requires the observation of a particular process, the Assessor will need to schedule this activity in a timely fashion after coordinating it with the issuing facility management. The Assessor, as directed by the DAO, may supplement the assessment methods and procedures recommended in these guidelines.

Assessment methods and procedures may be created or tailored for a particular issuer.

Subtask 4.2: Assemble all documentation and supporting materials necessary for the assessment of the issuer; if these documents include previous assessments, review the findings and determine if they are applicable to the current assessment.

Responsibility: OIMO; Assessor

Guidance: The OIMO assists the Assessor in gathering all relevant documents and supporting materials from the organization that will be required during the assessment of the issuer. Central to this effort is the operations plan. The issuer's operations shall be completely described in the operations plan. The operations plan may include by reference, or point to, the supporting materials. In this case, the OIMO will also need to gather this supporting material for the Assessor. Examples of other documentation include: (i) letters of appointment; (ii) privacy-related documentation; (iii) information forms utilized by the issuer; (iv) documentation from each outsourced service provider, including control implementation specifics, support and service level agreements, and contracts; (v) standard operating procedures for the issuing facilities within the authorization boundary is; and (vi) signed authorization letters under SP 800-37-1 for all information systems.

When previous assessments exist, including the one on which the current Authorization to Operate (ATO) is based, the Assessor is strongly encouraged to review these results. The Assessor may satisfy some of the issuer control assessment requirements by reviewing and referencing previous assessment report(s). Although previous assessments cannot be used as a substitute for the current assessment, they provide a snapshot view of the issuer and highlight problems that may have existed in the past.

Subtask 4.3: Assess the required issuer controls using the prescribed assessment procedures found in Appendix G.1 and G.2 based on the scope of the issuance functions.

Responsibility: Assessor

Guidance: The Assessor performs the assessment procedures selected for each issuer control to assess if they have been implemented correctly, are operating as intended, and producing the desired outcomes. The Assessor uses the assessment methods specified in Section 4.1. Documentation collected in the previous task is reviewed, and any deficiencies are identified. Interviews can be used as an opportunity to clarify issues encountered during a review of the issuer's documentation, as well as to determine the expertise of the personnel performing key PIV functions. Processes need to be observed to ensure that they are being followed as documented and tests executed to determine if the PIV components have been configured and are operating in a PIV-compliant manner.

As part of an assessment all applicable issuer controls need to be assessed. If PIV services have been outsourced to an external provider, the Assessor shall verify

that the issuer controls applying to those services have been assessed, and the reliability of the service provider has been found satisfactory. If an issuer and its facilities have already been assessed and are operating under a current ATO, and the purpose of the assessment is to add a facility(s) to the authorization letter, the Assessor may reuse the results of a previous assessment for the organization level issuer controls and then assess a random sample of the new issuing facilities.

Subtask 4.4: Prepare the assessment report.

Responsibility: Assessor

Guidance: The assessment report contains— (i) the results of the assessment; (ii) recommendations for correcting deficiencies; and (iii) the residual risk to the organization if those deficiencies are not corrected or mitigated. The assessment report is the Assessor's statement of the results of analyzing and evaluating the issuer's implementation of controls. The sample assessment report template in Appendix E should be used as a format for documenting the results after assessing the issuer controls.

Task 5: Assessment Documentation

This task consists of the Assessor submitting the assessment report to the OIMO and the latter adding the issuer's operations plan (revised if necessary) and the corrective actions plan (CAP) to generate an authorization submission package for the DAO. In situations where the assessment report contains deficiencies, the OIMO may choose to address some deficiencies based on the recommendations by the Assessor and revise the operations plan (if needed), even before submitting the package for authorization.

Subtask 5.1: Provide the OIMO with the assessment report.

Responsibility: Assessor

Guidance: The OIMO relies on the expertise, experience, and judgment of the Assessor to: (i) provide recommendations on how to correct deficiencies in the planned or performed operations; and (ii) to understand the potential impacts of those deficiencies. The OIMO may choose to act on selected recommendations of the Assessor before the authorization package is finalized. To optimize the utilization of resources organization-wide, any actions taken by the OIMO prior to the final authorization decision must be coordinated with the DAO. The Assessor reviews any changes made in response to the corrective actions and revises the assessment report, as appropriate.

Subtask 5.2: Revise the operations plan (if necessary) and implement its new provisions.

Responsibility: OIMO

Guidance: The revised operations plan must include all changes made in response to recommendations for corrective actions from the Assessor.

Subtask 5.3: Prepare the corrective actions plan (CAP).

Responsibility: OIMO

Guidance: The CAP, one of the three primary documents in the authorization submission package, describes actions that must be taken by the OIMO to correct deficiencies identified in the Assessment phase. The CAP identifies— (i) the tasks to be accomplished; (ii) the resources required to accomplish the tasks; (iii) scheduled completion dates for the tasks, and (iv) the person designated as responsible for completing each of the tasks.

Subtask 5.4: Assemble the authorization submission package and submit to the DAO.

Responsibility: OIMO

Guidance: The OIMO is responsible for the assembly and compilation of the authorization submission package with inputs from the OIMO. The authorization submission package shall contain: (i) the final assessment report; (ii) the CAP; (iii) the revised operations plan; and (iv) the SP 800-37-1 authorization letters for all information systems used by the issuer. The OIMO may wish to consult other key organization participants (e.g., the Assessor, PO) prior to submitting the authorization submission package to the DAO. The authorization submission package can be submitted in either paper or electronic form. The contents of the authorization submission package must be protected in accordance with organization policy.

5.3 Authorization Phase

The Authorization Phase consists of two tasks— (i) making an appropriate authorization decision; and (ii) completing the authorization documentation. Upon completion of this phase, the OIMO will have— (i) an authorization to operate the issuer's services as defined in its operations plan; (ii) an interim authorization to operate under specific terms and conditions; or (iii) a denial of authorization to operate.

Task 6: Authorization Decision

The authorization decision task determines if the assessment phase has been satisfactorily completed so that a recommendation concerning the operation of the issuer can be made with assurance. The DAO, working with the Assessor, reviews the contents of the assessment submission package, the identified and uncorrected or un-correctable deficiencies, the potential impacts on each organization using the issuer's services, and the CAP in determining the final risk to the organization(s) and the acceptability of that risk in light of the organization's mission.

Subtask 6.1: Review the authorization decision package to see if it is complete and that all applicable issuer controls have been fully assessed using the designated assessment procedures.

Responsibility: DAO

Guidance: Coverage for all issuer controls and proper adherence to assessment procedures and appropriate assessment methods helps to create confidence in assessment findings and is the main objective of the assessment review. Part of

the assessment review also includes understanding the impact of the identified deficiencies on the organization's operations, assets, and individuals.

Subtask 6.2: Determine if the risk to the organization's operations, assets, or potentially affected individuals is acceptable.

Responsibility: DAO

Guidance: After the completion of the assessment review, the DAO has a clear understanding of the impact of deficiencies. This helps the DAO to judge which deficiencies are of greatest concern to the organization and which can be tolerated without creating unreasonable organization-level risk. The CAP is also considered in determining the risk to the organization in terms of when and how the OIMO intends to address the known deficiencies. The DAO may consult the OIMO, Assessor, or other organization officials before completing the final risk evaluation. This risk evaluation in turn determines the degree of acceptability of issuer operations. The logic for using the latter as the basis for an authorization decision is described in Section 2.9.

Subtask 6.3: Provide the authorization package to an independent party for review and arrive at an authorization decision.

Responsibility: DAO

Guidance: Before providing the final authorization decision, the DAO seeks an independent review of the risks involved its issuer operations. The DAO shares the results of the assessment and the perceived risks with another issuer (e.g., another agency that issues PIV Cards or Derived PIV Credentials) to get their opinion and establish trustworthiness in the issued credentials.

Task 7: Authorization Documentation

The authorization documentation task includes— (i) completing and transmitting the authorization decision package to the appropriate individuals and organizations; and (ii) updating the issuer's operations plan.

Subtask 7.1: Provide copies of the authorization decision package, in either paper or electronic form, to the OIMO and any other organization officials having interests, roles, or responsibilities in the issuer's operations.

Responsibility: DAO

Guidance: The authorization decision package, including the authorization decision letter, should be transmitted to the OIMO. Upon receipt of the authorization decision package, the OIMO must review the authorization and its terms and conditions. The original authorization decision package must be kept on file by the OIMO. The DAO shall retain copies of the contents of the authorization decision package. The authorization decision package must be appropriately safeguarded and stored, whenever possible, in a centralized organization filing system to ensure accessibility. The authorization decision package shall be available to authorized auditors and oversight organizations upon

request. The authorization decision package must be retained in accordance with the organization's records retention policy. The issuer and specific facilities are authorized for a maximum of three (3) years from the date of the ATO. After the period ends, re- authorization must be performed.

Subtask 7.2: Update the operations plan.

Responsibility: OIMO

Guidance: The operations plan must be updated to reflect all changes made as the result of assessment and authorization. All conditions of issuer's operations that are set forth in the authorization decision must also be noted in the plan.

5.4 Monitoring Phase

The Monitoring Phase consists of two tasks— (i) operations plan maintenance; and (ii) annual lifecycle walkthrough. Based on the importance of reliably creating and issuing PIV Cards and Derived PIV Credentials, it is imperative that once the authorization is completed, the issuer is monitored to ensure that policies, procedures, and processes remain in effect as originally intended. There can be significant changes in an issuer's policies, management, operations personnel, and available technology during a three-year ATO. These changes must be monitored so that the organization minimizes exposing itself to security and privacy threats existing or arising after the authorization. For example, if there is a significant staff turnover, the organization must be sure that the new staff is performing the PIV functions using the same reliable processes that were previously approved.

In order to facilitate the monitoring of an issuer without undue burden in activities and paperwork, only two activities are required during this phase: maintenance of the operations plan and an annual lifecycle walkthrough of issuer operations. The latter entails reviewing all the services and functions of an issuer and its facilities for continued reliability. The annual walkthrough must cover a PIV Card's and/or Derived PIV Credential's lifecycle from sponsorship to maintenance. Observation of the full lifecycle ensures that all processes are still reliably operating as assessed during the authorization.

Task 8: Operations Plan Update

An operations plan is the primary description of what and how PIV Card and/or Derived PIV Credential issuing services are provided by the issuer. It is essential that this document be updated as changes occur in the issuer's operations. Management will be able to analyze the impact of changes as they occur and will be significantly better prepared when re- authorization is required.

Subtask 8.1: Document all relevant changes in the issuance processes within the operations plan.

Responsibility: OIMO

Guidance: In addition to the policies, procedures, and processes that must be documented if changes are made, the organization shall update the operations plan

if changes to the information system, the PIV Card, Derived PIV Credential, privacy policies, roles and responsibilities, or issuer controls are made.

Subtask 8.2: Analyze the proposed or actual changes to the issuer and determine the impact of such changes.

Responsibility: OIMO

Guidance: If the results of the impact analysis indicate that changes to the issuer could affect the reliability of the its operations, the changes and impact on the issuer must be reported to the DAO, corrective actions must be initiated, and the CAP must be updated. In instances where major changes have occurred, the issuer must be re- authorized.

Task 9: Annual Lifecycle Walkthrough

The annual lifecycle walkthrough is a monitoring activity to be performed initially by the issuer when its PIV Card and/or Derived PIV Credential issuing services begin, and annually thereafter. The OIMO (or designated appointee) is responsible for observing and reviewing the entire lifecycle of the PIV Card and/or the Derived PIV Credential. This walkthrough should provide an accurate snapshot of the issuer's operations and reliability at a point in time. By walking through the lifecycle, from sponsorship to issuance, including maintenance, the operations of an issuer can be examined as an integrated entity. During the walkthrough, the OIMO (or designated appointee) shall observe all processes involving the PIV Card or Derived PIV Credential, comparing them against the requirements defined in the issuer controls. This activity shall be performed every year after each authorization until re- authorization begins. All identified deficiencies in reliable operations shall be sent to the DAO for review and analysis. Any potential impact to the reliability of the issuer's operations and risk to the organization shall be documented and presented to the OIMO and the DAO.

Subtask 9.1: Observe all the processes involved in getting a PIV Card or a Derived PIV Credential, including those from sponsorship to maintenance. Observe each process and compare its controls against the applicable list of required issuer controls. If an issuer has several facilities, this process should be repeated using randomly selected issuing facilities.

Responsibility: OIMO (or designated appointee)

Guidance: As part of the walkthrough, the OIMO (or designated appointee) observes the processes followed for new employees and contractors (if different) as well any maintenance processes, such as termination, reissuance, or renewals. The OIMO (or designated appointee) observes each process and compares it against the documented steps for the issuer and the associated issuer controls. An annual walkthrough is required until re-authorization is initiated.

Subtask 9.2: The results of the lifecycle walkthrough are summarized in a report to the DAO. Deficiencies must be highlighted, along with corrective actions that must be implemented to correct any deficiencies.

Responsibility: OIMO, DAO

Guidance: The OIMO (or designated appointee) shall document the results of the walkthrough. The results shall be recorded in the assessment report template

included in Appendix E. All deficiencies should be highlighted, and a plan for correcting each deficiency shall be documented. The DAO shall decide if any deficiency is significant enough to require a change of the issuer's authorization-to-operate status.

APPENDIX A: REFERENCES

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974*, December 31, 1974 (effective September 27, 1975).
(Available at http://www.archives.gov/research_room/foia_reading_room/privacy_act/privacy_act.html.)

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002*, December 17, 2002.
(Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf.)

Executive Office of the President, Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953.
(Available at http://www.archives.gov/federal-register/codification/executive-order/10450.html.)

Executive Office of the President, Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
(Available at http://www.dhs.gov/homeland-security-presidential-directive-12.)

Executive Office of the President, Office of Management and Budget, Memorandum For Heads Of Departments And Agencies, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005.
(Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.)

United States Office Of Personnel Management, Memorandum For Heads Of Departments And Agencies. Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008.
(Available at http://www.opm.gov/investigations/background-investigations/reference/final-credentialing-standards.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001 or as amended.
(Available at http://csrc.nist.gov/groups/ST/FIPS140_3/documents/FIPS_140-3%20Final_Draft_2007.pdf)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004 or as amended.
(Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Security Controls for Federal Information Systems*, March 2006 or as amended.
(Available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 201-2, *Personal Identity Verification of Federal Employees and Contractors*, August 2013.
(Available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf),

National Institute of Standards and Technology, Special Publication 800-37-1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Revision 1, February 2010 or as amended.
(Available at http:/csrc.nist.gov/publications/nistpubs/ 800-37-1/SP 800-37-1-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53 Rev. 4 *Recommended Security Controls for Federal Information Systems*, April 2013 or as amended. (Available at http://dx.doi.org/10.6028/NIST.SP.800-53r4.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003 or as amended. (Available at http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf)

United States Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, October 2007 or as amended. (Available at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-73--4)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-76-2, *Biometric Data Specification for Personal Identity Verification*, May 2013 or as amended. (Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf)

United States Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2013 or as amended. (Available at http://csrc.nist.gov/publications/drafts/800-78-4/sp800_78-4_draft.pdf)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, April 2006 or as amended. (Available at http://csrc.nist.gov/publications/nistpubs/800-85A-2/sp800-85A-2-final.pdf))

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006 or as amended. (Available at http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Draft Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, February 2014 or as amended. (Available at http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Draft Interagency Report 7328, *Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems*, September 2007 or as amended. (Available at http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7328.)

United States Office of Management and Budget, *Circular No. A-130 Revised*, Appendix III, Security of Federal Automated Information Resources, February 2000. (Available at http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii .)

APPENDIX B: GLOSSARY AND ACRONYMS

Terms/Acronyms used in this document	Definition or explanation of terms; expansion of acronyms
Access Control	The process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, and border-crossing entrances).
Authorization (as applied to an issuer)	The official management decision of the Designated Authorizing Official to permit operation of an issuer after determining that the issuer's reliability has satisfactorily been established through appropriate assessment processes.
Authorization Package	The results of assessment and supporting documentation provided to the Designated Authorizing Official to be used in the authorization decision process.
Agency	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); or a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Applicant	An individual applying for a PIV Card.
Assessment (as applied to an issuer)	Assessment in this context means a formal process of assessing the implementation and reliable use of issuer controls using various methods of assessment (e.g., interviews, document reviews, observations) that support the assertion that an issuer is reliably meeting the requirements of FIPS 201-2.
Assessment Method	A focused activity or action employed by an Assessor for evaluating a particular issuer control.
Assessment Procedure	A set of activities or actions employed by an Assessor to determine the extent that an issuer control is implemented.
Assessor	The individual responsible for conducting assessment activities under the guidance and direction of a Designated Authorizing Official. The Assessor is a 3rd party.
ATO	Authorization to Operate; One of three possible decisions concerning an issuer made by a Designated Authorizing Official after all assessment activities have been performed stating that the issuer is authorized to perform specific PIV Card and/or Derived Credential issuance services.
CAP (Corrective Action Plan)	Corrective actions for an issuer for removing or reducing deficiencies or risks identified by the Assessor during the assessment of issuer operations. The plan identifies actions that need to be performed in order to obtain or sustain authorization.
Activation/Issuance	A process that includes the procurement of FIPS-approved blank PIV Cards or hardware/software tokens (for Derived PIV Credential), initializing them using appropriate software and data elements, personalization of these cards/tokens with the identity

Terms/Acronyms used in this document	Definition or explanation of terms; expansion of acronyms
	credentials of authorized subjects, and pick-up/delivery of the personalized cards/tokens to the authorized subjects, along with appropriate instructions for protection and use.
Component	An element such as a fingerprint capture station or card reader used by an issuer, for which FIPS 201-2 has defined specific requirements.
Credential	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a card or token possessed and controlled by a cardholder or subscriber.
DAO	Designated Authorizing Official; A senior organization official that has been given the authorization to authorize the reliability of an issuer.
DATO	Denial of Authorization to Operate; issued by a DAO to an issuer that is not authorized as being reliable for the issuance of PIV Cards or Derived PIV Credentials.
Derived PIV Credential	A credential issued based on proof of possession and control of the PIV Card, so as not to duplicate the identity proofing process as defined in SP 800-63-2. A Derived PIV Credential token is a hardware or software based token that contains the Derived PIV Credential.
DPCI	Derived PIV Credential (and associated token) Issuer; an issuer of Derived PIV Credentials as defined in SP 800-63-2 and SP 800-157.
FIPS	Federal Information Processing Standard
HSPD-12	Homeland Security Presidential Directive; HSPD-12 established the policy for which FIPS 201-2 was developed.
IATO	Interim Authorization to Operate; issued by a DAO to an issuer who is not satisfactorily performing PIV Card and/or Derived PIV Credential specified services (e.g., identity proofing/registration (if applicable)), card/token production, activation/issuance and maintenance).
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 Proofing	Verifying the claimed identity of an applicant by authenticating the identity source documents provided by the applicant.
ITL	Information Technology Laboratory
Maintenance	The process of managing PIV Cards or Derived PIV Credentials

Terms/Acronyms used in this document	Definition or explanation of terms; expansion of acronyms
	(and its token) once they are issued. It includes re-issuance, post issuance updates, and termination.
Mobile Device	A mobile device, for the purpose of this document is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.
NIST	National Institute of Standards and Technology
OIMO	Organization Identity Management Official; The individual responsible for overseeing the operations of an issuer in accordance with FIPS 201-2 and for performing the responsibilities specified in this guideline.
OMB	Office of Management and Budget
PCI	PIV Card Issuer
Information System	A computer-based system used by an issuer to perform the functions necessary for PIV Card or Derived PIV Credential issuance as per FIPS 201-2.
PII	Personally Identifiable Information; 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]
PIV	Personal Identity Verification as specified in FIPS 201-2.
PIV Card	The physical artifact (e.g., identity card, “smart” card) issued to an applicant by an issuer that contains stored identity markers or credentials (e.g., a photograph, cryptographic keys, digitized fingerprint representations) 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 Credential	Evidence attesting to one’s right to credit or authority; in FIPS 201-2, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
Risk	The level of potential impact on an organization operations (including mission, functions, image, or reputation), organization assets, or individuals of a threat or a given likelihood of that threat occurring.
Registration	Making a person’s identity known to the enrollment/Identity Management System information system by associating a unique

Terms/Acronyms used in this document	Definition or explanation of terms; expansion of acronyms
	identifier with that identity, and collecting and recording the person's relevant attributes into the information system. Registration is necessary in order to initiate other processes, such as adjudication, card/token personalization and issuance and, maintenance that are necessary to issue and to re-issue or maintain a PIV Card or a Derived PIV Credential token.
SAO	Senior Authorizing Official; A senior organization official that has budgetary control, provides oversight, develops policy, and has authority over all functions and services provided by the issuer.
SOP	Standard operating procedures
SOR	A system of records is a group of records under the control of a Federal agency which contains a personal identifier (such as a name, date of birth, finger print, Social Security Number, and Employee Number) and one other item of personal data (such as home address, performance rating, and blood type) from which information is retrieved using a personal identifier.
SORN	The Privacy Act requires each agency to publish a notice of its systems of records in the Federal Register. This is called a System of Record Notice (SORN).
SP	Special Publication
Subscriber	An individual applying for a Derived PIV Credential

1731

APPENDIX C: ISSUER READINESS REVIEW CHECKLIST

The readiness review checklist may be used by an issuer of PIV Cards or Derived PIV Credential tokens while preparing for assessment. The checklist may also be used to validate that the issuer has collected all relevant documentation, identified appropriate individuals and made them available to the assessment team.

Activity	Completed?	Comments
• Identify a 3rd party assessment team to assess the issuer.		
• Determine the authorization boundary.		
• Establish the scope and objectives of the assessment.		
• Determine the level of effort and resources necessary to carry out the assessment.		
• Establish the time-frame to complete the assessment and identify key milestone decision points.		
• Notify key personnel at the issuing facility and any external service providers (if applicable) of the impending assessment.		
• Validate that the operations plan is complete and includes all the required information.		
• Ensure that the necessary roles have been designated.		
• Validate that implementation and management responsibility for issuer controls have been accurately assigned.		
• Make sure that the information systems utilized by the issuer have been assessed and authorization to operate in accordance with SP 800-37-1.		
• Ensure that the following documentation has been developed and can be made available to the assessment team: (i) Operations plan (ii) Results from any past assessment and authorization decisions for the issuer (iii) Letters of appointment (if any) (iv) Service Level Agreements (SLA) and Memorandums of Understanding (MOU) between the organization and the service provider(s). (v) Listing of all HSPD-12 components		

Activity	Completed?	Comments
used within the PIV system (vi) Privacy-related documentation (vii) All forms utilized by the issuer (viii) Documentation from outsourced providers (ix) Standard operating procedures for the issuing facilities within the authorization boundary (x) Signed authorization letter under SP 800-37-1 for each information system within scope of the assessment.		
• Prior to authorization, a third party that is independent has reviewed the assessment.		
• The PIV system is operational and actual PIV processes can be observed by the assessment team.		
• The PIV system is in production and operational. PIV Cards and Derived PIV Credential tokens are ready to be personalized and can be used for testing by the assessment team.		
• Personalized PIV Cards and/or Derived PIV Credential tokens are submitted on an annual basis to GSA for testing and are issued from a production system.		

1738

APPENDIX D: OPERATIONS PLAN TEMPLATES

Appendices D.1 and D.2 are suggested outlines for a PIV Card Issuer (PCI) and a Derived PIV Credential Issuer (DPCI) respectively. It is highly recommended that an organization follow these templates to document its operations comprehensively and to the full extent as needed to support a successful authorization. An issuer of both PIV Cards and Derived PIV Credentials may develop a single operations plan that addresses all requirements without repeating common elements of the plan.

Appendix D.1: Operations Plan Template for PIV Card Issuers

I. Background

<Provide a brief background on HSPD-12, FIPS 201-2 and PIV, as well as how the organization has planned to meet the Directive. >

II. Purpose and Scope

<Describe the purpose and scope of the operations plan. >

III. Applicable Laws, Directives, Policies, Regulations & Standards

<Identify all Laws, Directives, Policies, Regulations and Standards that govern PIV Card issuance at the Organization.>

IV. PCI Roles and Responsibilities

<Identify the authorization-related roles and responsibilities of all key personnel within the PCI.>

V. Assignment of Roles

<Document how the various roles that have been identified in the section above are appointed. These can be either specific individuals or positions within the organization. Provide contact information for all the roles assigned.>

VI. PCI Description

<Provide a description of the organization's PCI. Details such as structure and geographic dispersion should be included.>

VII. Issuing Facility Details

<Identify all the issuing facilities that are included and are part of the authorization boundary. Provide details such as the location, PIV Card Process performed (e.g. registration) at the facility and the approximate number of PIV Cards personalized at each facility. >

VIII. PCI Management

<This section discusses various management aspects of the PCI. >

a. Coordination and Interaction

<Describe management interactions within the PCI, both at an organization level, and between the organization and the facility(s). >

b. Staffing

<Describe the procedures employed to make sure that adequate staff is available for performing PIV Card related functions. >

c. Training

<Describe the procedures employed to ensure that the staff is properly trained to perform their respective duties. >

d. Procurement

<Describe the mechanism typically used for procuring products/services related to the organization's HSPD-12 implementation. >

e. Outsourcing

<Describe the PIV Card functions being outsourced (if applicable). >

IX. PCI Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) identity proofing / registration, (iii)adjudication, (iv) card production, (v) activation and issuance and (vi) maintenance for PIV Cards. Also discuss the procedures for temporary badges, as well as for non-PIV badges employed by the organization. >

a. Sponsorship
b. Identity Proofing and Registration
c. Adjudication
d. Card Production
e. Activation/Issuance
f. Maintenance
    i. Re-issuance
    ii. Post-issuance updates
    iii. Termination
b. Temporary/Non-PIV Badges

X. PCI Issuance Information System (s) Description

<Provide a description of the technical aspects of the organization's PIV issuance system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, the PKI provider as well as the information system authorization status. >

a. Architecture
b. Interconnections and Information Sharing
c. Information System Inventory
d. Public Key Infrastructure
e. SP 800-37-1 C&A Information

XI. Card Personalization & Production

<Describe the organization's PIV Card graphical layout(s), as well the optional data containers being used. Provide details if there are any PIV Card expiration date requirements levied by the organization. Also describe the mechanisms in place for securing both pre-personalized and personalized PIV Card stock >

a. PIV Card Graphical Topology
b. PIV Card Electronic Data Elements
c. Expiration Date Requirements
d. Card Inventory Management

XII. Issuer Controls

<This section documents the issuer controls(from Appendix G.1) and provides the following information for each: (i) issuer control identifier and description, (ii) control owner, (iii) whether the control is organization-specific or facility- specific and (iv) a description of how the issuer control has been implemented by the organization. >

a. Issuer Control Identifier and Control Description
b. Issuer Control Owner
c. Organization/Facility Specific
d. How the issuer control is implemented

Appendix A - Memoranda of Appointment

<Attached copies of signed memoranda-of-appointment that record the various roles that have been assigned and the personnel fulfilling these roles that have accepted the position and its associated responsibilities. >

Appendix B - Privacy Requirements

<Attached copies of the privacy-related information as identified below. >

a. Privacy Policy
b. Privacy Impact Assessment
c. System of Record Notice
d. Privacy Act Statement/Notice
e. Rules of Conduct
f. Privacy Processes
    i. Requests to review personal information
    ii. Requests to amend personal information
    iii. Appeal procedures
    iv. Complaint procedures

Appendix C – Service Level Agreements, Memoranda of Understanding (MOU)

<Attached copies of any service level agreements and memoranda of understanding executed between the organization and any external service provider that has been contracted to provide certain PIV related functions.>

Appendix D.2: Operations Plan Template for Derived PIV Credential Issuers

I. Background

<Provide a brief background on HSPD-12, FIPS 201-2, PIV and SP 800-157, as well as how the organization has planned to meet the Directive. >

II. Purpose and Scope

<Describe the purpose and scope of the operations plan. >

III. Applicable Laws, Directives, Policies, Regulations & Standards

<Identify all Laws, Directives, Policies, Regulations and Standards that govern Derived PIV Credential token Issuance at the Organization.>

IV. DPCI Roles and Responsibilities

<Identify the authorization-related roles and responsibilities of all key personnel within the DPCI.>

V. Assignment of Roles

<Document how the various roles that have been identified in the section above are appointed. These can be either specific individuals or positions within the organization. Provide contact information for all the roles assigned.>

VI. DPCI Description

<Provide a description of the organization's DPCI. Details such as structure and geographic dispersion should be included.>

VII. Issuing Facility Details

<If applicable, identify all the Issuing facilities that are included and are part of the authorization boundary. Provide details such as the location, Derived PIV Credential functions performed at the facility and the types and approximate number of PIV Derived Credentials personalized at each facility. If issuance is conducted entirely remotely, indicate this within VI. >

VIII. DPCI Management

<This section discusses various management aspects of the DPCI. >

a. Coordination and Interaction

<Describe management interactions within the DPCI, both at an organization level, and between the organization and the facility(s). >

b. Staffing

<Describe the procedures employed to make sure that adequate staff is available for performing Derived PIV Credential related issuance functions. >

c. Training

<Describe the procedures employed to ensure that the staff is properly trained to perform their respective duties. >

d. Procurement

<Describe the mechanism typically used for procuring products/services related to the organization's HSPD-12 implementation. >

e. Outsourcing

<Describe the PIV Derived Credential functions being outsourced (if applicable). >

IX. DPCI Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) derivation and registration, (iii) token production and (iv) activation and issuance, and (v) maintenance for Derived PIV Credentials.

a. Sponsorship
b. Identity Proofing (i.e., Derivation) and Registration
c. Token Production
d. Activation/Issuance
e. Maintenance
    i. Re-issuance
    ii. Post-issuance updates
    iii. Termination

X. DPCI Issuance System (s) Description

<Provide a description of the technical aspects of the organization's PIV issuance system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, the PKI provider as well as the information system authorization status. >

a. Architecture
b. Interconnections and Information Sharing
c. Information System Inventory
d. Public Key Infrastructure
e. SP 800-37-1 C&A Information
f. Linkage between the PIV Card and the Derived PIV Credential

XI. Derived PIV Credential Details

<Provide details of the organization's implementation of the Derived PIV Credential token. Describe if its hardware or software based. If hardware-based, provide details of implementation (e.g. removable, SD Card, Universal Integrated Circuit Card, USB token or embedded)>

a. Derived PIV Credential token Data Elements
b. Inventory Management (for Hardware-based Tokens)

XII. Issuer Controls

<This section documents the issuer controls(from Appendix G.2) and provides the following information for each: (i) issuer control identifier and description, (ii) control owner, (iii) whether the control is organization-specific or facility- specific and (iv) a description of how the issuer control has been implemented by the organization. >

a) Issuer Control Identifier and Control Description
b) Issuer Control Owner
c) Organization/Facility Specific
d) How the issuer control is implemented

Appendix A - Memoranda of Appointment

<Attached copies of signed memoranda-of-appointment that record the various roles that have been assigned and the personnel fulfilling these roles that have accepted the position and its associated responsibilities. >

Appendix B - Privacy Requirements

<Attached copies of the privacy-related information as identified below. >

a. Privacy Policy
b. Privacy Impact Assessment
c. System of Record Notice
d. Privacy Act Statement/Notice
e. Rules of Conduct
f. Privacy Processes

i. Requests to review personal information
ii. Requests to amend personal information
iii. Appeal procedures
iv. Complaint procedures

Appendix C – Service Level Agreements, Memoranda of Understanding (MOU)

<Attached copies of any service level agreements and memoranda of understanding executed between the organization and any external service provider that has been contracted to provide certain PIV related functions.>

APPENDIX E: ASSESSMENT REPORT TEMPLATE

Below is a template to use when generating the assessment report. This is to be completed for each issuer control. An example using a specific issuer control follows.

Issuer Authorization Topic (IAT):

Authorization Focus Area

Issuer Control Identifier—

Control Description—

Issuer Control Owner / Control Level — (External Service Provider, Organization specific, Facility specific)

ASSESSMENT DETAILS

Assessment Method(s):

Review: (Artifact(s))

Observe: (Name of Process)

Assessment Result— (Satisfied, Partially Satisfied, Not Satisfied, Not Applicable)

Assessment Findings—

Assessment Deficiency and Potential Impact—

Recommendation—

Activation/Issuance Process

Issuer Control Identifier— AI-7

Control Description— Before the PIV Card is provided to the applicant, the issuer performs a 1:1 biometric match of the applicant against biometrics available on the PIV Card or in the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. If the match is unsuccessful, or if no biometric data is available, the cardholder provides two identity source documents (as specified in FIPS 201-2, Section 2.7), and an attending operator inspects these and compares the cardholder with the facial image printed on the PIV Card.

Issuer Control Owner— External Service Provider, Facility Specific

ASSESSMENT DETAILS

Assessment Method(s):

Review: Operations Plan

Observe: Activation/Issuance Process

Assessment Result— Partially Satisfied

Assessment Findings— There is operational evidence that a 1:1 biometric match is carried out before the card is released to the applicant.

Assessment Deficiency and Potential Impact— The requirement to carry out this task is not documented clearly enough in the operations plan. Although personnel are knowledgeable about this requirement, and the task was observed to be performed correctly during card issuance, the lack of documentation could be a problem if there is turnover in staff. Alternate processes when fingerprints are unavailable are not in place.

Recommendation— Update the issuance process description within the operations plan to include a clear description of this task in the process and develop alternate processes for issuance when fingerprints are not available.

Summary Report Template

IAT (% Satisfied, % Partially Satisfied, % Not Satisfied)

For each Authorization Focus Area

(% Issuer controls Satisfied, % Partially Satisfied, % Not Satisfied)

(% Review Assessments Satisfied, % Interview Assessments Satisfied, % Observe Assessments Satisfied, % Test Assessments Satisfied)

APPENDIX F: SAMPLE TRANSMITTAL AND DECISION LETTERS

Sample Assessment/Authorization Package Transmittal Letter

From: Organization Identity Management Official Date:

To: Designated Authorizing Official (DAO)

Subject: Authorization Submission Package for [PCI / DPCI]

An assessment of the [PCI/DPCI NAME] located at [PCI/DPCI Location and Issuing Facility Locations] has been conducted in accordance with NIST Special Publication (SP) 800-79-2, *Guidelines for the Authorization of PIV Card Issuers and Derived PIV Credential Issuer* and the [ORGANIZATION] policy on authorization. The attached authorization package contains— (i) the operations plan; (ii) the assessment report; (iii) a corrective actions plan (CAP); and (iv) an SP 800-37-1 authorization letter for each information system within the [PCI/DPCI].

The operations plan, its policies, procedures, and processes have been assessed by [ASSESSOR] using the assessment methods and procedures defined in SP 800-79-2 and specified in the assessment report to determine the extent to which the requirements under HSPD-12 and FIPS 201-2 are exhibited. The CAP describes the corrective actions that we plan to perform to remove or reduce any remaining deficiencies detected in our operations.

Signature

Title

Sample Authorization Decision Letter (Authorization to Operate)

From: Designated Authorizing Official Date:

To: Organization Identity Management Official

Subject: Authorization Decision for [PCI / DPCI]

After reviewing the results of the authorization package of the [PCI / DPCI], I have determined that its policies, procedures, and processes are in compliance both with FIPS 201-2 and our organization's own policies, regulations and standards. Accordingly, I am issuing an *authorization to operate* (ATO). [PIV Card and/or Derived PIV Credential] issuance services are authorized without any restrictions or limitations. This authorization is my formal declaration that the requirements of HSPD-12 are being satisfied.

This ATO also applies to issuing facilities under this [PCI / DPCI]. Included is a list of facilities authorized to operate under this authorization decision.

This authorization and ATO will remain in effect for 3 years from the date of this letter if— (i) all required documentation is updated annually; (ii) a lifecycle walkthrough is completed annually and the results sent to me within thirty (30) days of completion; and (iii) no deficiencies are identified during the walkthrough that would increase the risk to the organization's mission.

A copy of this letter and all supporting authorization documentation shall be retained in accordance with the organization's record retention schedule.

Signature

Title

Sample Authorization Decision Letter (Interim Authorization to Operate)

From: Designated Authorizing Official Date:

To: Organization Identity Management Official

Subject: Authorization Decision for [PCI / DPCI]

After reviewing the results of the assessment of the [PCI / DPCI], I have determined that the requirements identified in FIPS 201-2 and the organization's policies, regulations, and standards have not been implemented satisfactorily. However, I have determined that there is an overarching need for the issuance services to continue due to mission necessity and other considerations. Accordingly, I am issuing an *interim authorization to operate* (IATO). Operation of the [PCI /DPCI] shall be performed in accordance with the enclosed terms and conditions during the IATO period. The [PCI / DPCI] is *not* considered authorized during the IATO period.

This IATO also applies to facilities under the [PCI / DPCI]. Included is a list of facilities authorized to operate during this interim period, along with specific limitations or restrictions that apply.

This interim authorization to operate is valid for a maximum till close of business on <date [not to exceed three months]. This interim authorization will remain in effect as long as— (i) the required status reports for the [PCI / DPCI] are submitted to this office every month; (ii) the problems or deficiencies reported from the authorization do not result in additional risk that is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating the deficiencies in accordance with the corrective actions plan (CAP). At the end of IATO period, the [PCI / DPCI] must be ready to receive an authorization to operate. A second IATO will be granted only in extenuating circumstances. This office will review the CAP submitted with the authorization package during the IATO period and monitor progress on removal or reduction of concerns and discrepancies before re-authorization is initiated.

A copy of this letter and all supporting authorization documentation shall be retained in accordance with the organization's record retention schedule.

Signature

Title

Sample Authorization Decision Letter (Denial of Authorization to Operate)

From: Designated Authorizing Official Date:

To: Organization Identity Management Official

Subject: Authorization Decision for [PCI / DPCI]

After reviewing the results of the assessment of the [PCI / DPCI] and the supporting evidence provided in the associated authorization package, I have determined that the requirements identified in FIPS 201-2 and the organization's policies, regulations, and standards are not being exhibited by the [PCI / DPCI]. Accordingly, I am issuing a denial of authorization to operate (DATO) to the [PCI / DPCI] and its issuing facilities. The [PCI / DPCI] is *not* authorized and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED].

The corrective actions plan (CAP) is to be pursued immediately to ensure that proactive measures are taken to correct the deficiencies found during the assessment. Re- authorization is to be initiated at the earliest opportunity to determine the effectiveness of correcting the deficiencies.

A copy of this letter and all supporting authorization documentation shall be retained in accordance with the organization's record retention schedule.

Signature

Title

APPENDIX G: ISSUER CONTROLS AND ASSESSMENT PROCEDURES

Appendices G.1 and G.2 list issuer controls that are applicable to a PIV Card Issuer (PCI) and a Derived PIV Credential Issuer (DPCI). An issuer must comply with all applicable requirements, with applicability determined by whether the organization issues the mandatory PIV Cards, the optional Derived PIV Credentials (if implemented) or both.

Appendix G.1: Controls and Assessment Procedures for PIV Card Issuers (PCIs)

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Preparation and Maintenance of Documentation	DO-1	The organization develops and implements an issuer operations plan according to the template in Appendix D-1. The operations plan references other documents as needed. **Assessment** *Determine that:* *(i) the operations plan includes the relevant elements from the template in Appendix D-1 (review);* *(ii) the operations plan includes the list of issuer controls and the issuer control owner for each, how they were implemented and whether they are organization or facility specific (review);* *(iii) documentation that is not included in the operations plan is referenced accurately (review);* *(iv) the operations plan has been reviewed and approved by the DAO within the organization (review, interview).*	SP 800-79-2, Section 2.11 – Authorization Package and Supporting Documentation
	DO-2	The organization has a written policy and procedures for identity proofing and registration that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency. **Assessment** *Determine that*: *(i) the organization has developed and documented written policy and procedures for identity proofing and registration for personnel requiring a PIV Card (e.g. employees, contractors and foreign nationals) (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal department or agency (review);* (iv) *the organization will periodically review and update the policy and procedures as required (review, interview).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements
	DO-3	The organization has a written policy and procedures for issuance that are approved by the head or deputy secretary (or equivalent) of the Federal department or agency. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for issuance (review);*	FIPS 201-2, Section 2.8 – PIV Identity Proofing and Registration Requirements

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
		(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review); *(iii) the policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal department or agency (review);* (iv) *the organization will periodically review and update the policy and procedures as required (review, interview).*	
	DO-4	This control has been withdrawn. Renewal is now part of re-issuance in FIPS 201-2. Therefore, DO-4 is covered, as applicable, by DO-6.	-
	DO-5	The organization has a written policy and procedures describing the conditions for PIV Card termination. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for PIV Card termination (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization will periodically review and update the policy as required (review, interview).*	FIPS 201-2, Section 2.9.4 – PIV Card Termination
	DO-6	The organization has a written policy and procedures describing the conditions for PIV Card reissuance and post issuance update. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for card reissuance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization will periodically review and update the policy and procedures as required (review, interview).*	FIPS 201-2, Section 2.9.1 – PIV Card Reissuance Requirements FIPS 201-2, Section 2.9.2 - PIV Card Post Issuance Update Requirements
	DO-7	In cases where a PIV Card is not required, such as temporary employees, contractors employed for less than 6 months and visitors, the organization has a written policy and procedures describing the conditions for temporary badges. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for the issuance of temporary badges (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization will periodically review and update the policy and procedures as required (review, interview).*	OMB Memorandum 05-24

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	DO-8 (NEW)	The organization has a written policy and procedures for identity proofing and registration that apply to citizens of foreign countries who are working for the Federal government overseas (if applicable). **Assessment** *Determine that:* *(i) the organization uses a process that is approved by the U.S. State Department's Bureau of Diplomatic Security (review);* *(ii) the policy and procedures have been signed off by the head or deputy secretary (or equivalent) of the Federal department or agency (review).*	FIPS 201-2, Section 2.2.7 - Identity Proofing and Registration Requirements

2101

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Assignment of Roles and Responsibilities	RR-1	The organization has appointed the role of Senior Authorizing Official (SAO). **Assessment** *Determine that*: *(i) the organization has defined the role of Senior Authorizing Official and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of Senior Authorizing Official (review).*	SP 800-79-2, Section 2.6 – Issuer Roles and Responsibilities
	RR-2	The organization has appointed the role of Designated Authorizing Official (DAO). **Assessment** *Determine that*: *(i) the organization has defined the role of* Designated Authorizing Official *and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of* Designated Authorizing Official *(review, interview).*	SP 800-79-2, Section 2.6 – Issuer Roles and Responsibilities
	RR-3	The organization has appointed the role of Organization Identity Management Official (OIMO). **Assessment** *Determine that*: *(i) the organization has defined the role of Organization Identity Management Official and its responsibilities according to the requirements of SP 800-79-2 (interview);* *(ii) the organization has assigned the role of Organization Identity Management Official (review, interview).*	SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	RR-4	The organization has appointed the role of Assessor. **Assessment** *Determine that*: *(i) the organization has defined the role of Assessor and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of Assessor (review);* *(iii) the Assessor is a third party that is independent of, and organizationally separate from, the persons and office(s) directly responsible for the day-to-day operation of the organization (review, interview).*	SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities
	RR-5	The organization has appointed the role of Privacy Official (PO). **Assessment** *Determine that*: *(i) the organization has defined the role of Privacy Official and its responsibilities according to the requirements of SP 800-79-2 (review);* *(iv) the organization has assigned the role of Assessor (review);* *(ii) the Privacy Official does not have any other roles in the organization (review, interview).*	FIPS 201-2, Section 2.11 - PIV Privacy Requirements SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities
	RR-6	The issuer employs processes which adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV Card without the cooperation of another authorized person. **Assessment** *Determine that*: *(i) the standard operating procedures document the principle of separation of duties (review);* *(ii) the processes demonstrate adherence to the principle of separation of duties (interview, observe).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Facility and Personnel Readiness	**Facility**		
	FP-1	Minimum physical controls at the issuing facility are implemented. These include: (i) use of locked rooms, safes, and lockable cabinets (as appropriate); (ii) physical access to key areas within the facility is restricted to authorized personnel, (iii) security monitoring and automated alarms are implemented, (iv) emergency power and lighting are available, and (v) fire prevention and protection mechanisms are implemented. **Assessment** *Determine that:* *(i) the OIMO and Issuing Facility Manager(s) are aware of the minimum set of physical controls that need to be in place at the facility(ies) (interview);* *(ii) the minimum physical security controls are implemented by the issuing facility (observe).*	Commonly accepted security readiness measures
	FP-2	Issuer Documentation (e.g., operations plan, standard operating procedures, and contracts) are maintained at each issuing facility. **Assessment** *Determine that:* *(i) the most current versions of the issuer documentation is available at each issuing facility for reference as needed (interview, review).*	Commonly accepted security readiness measures
	Equipment		
	FP-3	The Issuing Facility Manager(s) has a copy of the contingency/disaster recovery plan for the information systems, which is stored securely. **Assessment** *Determine that*: *(i) the contingency plan/ disaster recovery plan is stored securely at the facility (interview, observe);* *(ii) the Issuing Facility Manager is knowledgeable on how to restore/reconstitute the information systems in case of system failures (interview).*	Commonly accepted security readiness measures
	FP-4	The information systems are managed using a system development life cycle (SDLC) methodology that includes information security considerations. **Assessment** *Determine that*: *(i) the information system used by the organization has been developed using an SDLC methodology (review, interview);* *(ii) information system security is considered as part of the development life cycle (review).*	Commonly accepted security readiness measures

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	FP-5	Card activation/issuance workstations are situated in an enclosed area (wall or partition) to provide privacy for an applicant or card holder. **Assessment** *Determine that*: *(i) Issuing facility workstations are situated in an enclosed area (wall or partition) such that other individuals cannot see an applicant or card holder's personal information (observe).*	Commonly accepted security readiness measures
	Key Personnel		
	FP-6	All operators who perform roles within an issuing facility in the areas of identity proofing and registration, issuance or maintenance are allowed access to information systems only when authenticated through a PIV Card. **Assessment** *Determine that*: *(i) the requirement that all operators who perform roles within an issuing facility in the areas of identity proofing and registration, issuance or maintenance are allowed logical access to information systems only when authenticated through a PIV Card, has been documented in the issuing facility's standard operating procedures (review);* *(ii) Operators use PIV Cards to access information systems in the course of performing their roles within the PIV Card lifecycle processes (observe).*	OMB Memorandum 11-11
	FP-7	All operators who perform roles within an issuing facility in the areas of identity proofing and registration, issuance and maintenance have undergone training that is specific to their duties prior to being allowed to perform in that function. **Assessment** *Determine that*: *(i) all operators who perform roles within an issuing facility in the areas of identity proofing and registration, issuance and maintenance are allowed access to information systems only after completing a training course specific to their duties. (interview, review);* *(ii) Records showing that the appropriate training course has been completed by issuing facility personnel are stored by the facility for audit purposes (interview, review).*	Commonly accepted security readiness measures

IAT = Organizational Preparedness			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	FP-8	All pre-personalized and personalized smart card stock received from card vendors and card production facilities are received only by authorized personnel who ensure that the card stock is stored, handled and disposed of securely at the issuing facility. **Assessment** *Determine that*: *(i) the issuing facility has an authorized list of personnel that are responsible for ensuring that smart card stock is received and stored securely. (interview);* *(ii) procedures for receiving, storing and destroying smart card stock are documented in the issuing facility's standard operating procedures (review);* *(iii) the authorized personnel are knowledgeable of the procedures on how to receive, store and destroy (in case of printing errors) smart card stock (interview).*	FIPS 201-2, Section 2.8 - PIV Card Issuance Requirements
	FP-9	The organization maintains a current list of designated points of contact and alternate points of contact for all issuing facilities used by the organization for identity proofing and registration and issuance and maintenance processes. **Assessment** *Determine that*: *(i) the organization maintains a \list of designated points of contact and alternate points of contact for all issuing facilities used by the organization (review);* *(ii) the list is current and the individuals named are the correct points of contact (review and interview).*	Commonly accepted security readiness measures

2117
2118

2119

IAT = Security Management & Data Protection			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Protection of Stored and Transmitted Data	ST-1	The issuer information systems that contain information in identifiable form are handled in compliance with Federal laws and policies, including the Privacy Act of 1974. **Assessment** *Determine that*: *(i) the organization does not disclose any record which is contained in the system of records to any person, or to another organization unless written consent has been given by the individual to whom the record pertains unless one of the exceptions for disclosure in the Privacy Act are met (review, interview);* *(ii) individuals are permitted to gain access to their personal record and the information is provided in a form comprehensible to them (review, interview);* *(iii) individuals are able to request amendments to records pertaining to them, corrections are made promptly and if not, the individual is provided with a reason for the refusal and is able to request a review of the refusal (review, interview);* *(iv) the organization notifies an individual when their record is made available to any person under a compulsory legal process when such a process becomes a matter of public record (review, interview).*	FIPS 201-2, Section 2.11 - PIV Privacy Requirements
	ST-2	The information systems protect the integrity and confidentiality of transmitted information. **Assessment** *Determine that*: *(i) the integrity of transmitted information is protected (interview, test, review);* *(ii) the confidentiality of transmitted information is protected (interview, test, review).*	FIPS 201-2, Section 2.11 - PIV Privacy Requirements

2120
2121

IAT = Security Management & Data Protection			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Enforcement of Privacy Requirements	PR-1	Privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies are developed and posted by the organization in multiple locations at the issuing facility (e.g., internet site, human resource offices, regional offices, and contractor orientation handouts). **Assessment** *Determine that*: *(i) the issuing facility has posted privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies (interview, review).*	OMB Memorandum 05-24
	PR-2	The organization has conducted a Privacy Impact Assessment of their issuer information system (s), compliant with Section 208 of the E-Government Act of 2002 and based on guidance found in Appendix E of OMB Memorandum 06-06. **Assessment** *Determine that:* *(i) the organization has conducted a Privacy Impact Assessment of their issuer information system (s) based on guidance found in Appendix E of OMB Memorandum 06-06 (review);* *(ii) the organization has submitted the Privacy Impact Assessment of their issuer information system (s) to OMB (interview, review).*	OMB Memorandum 05-24 OMB Memorandum 06-06 (Appendix E)
	PR-3	The organization's employee and contractor identification systems of records notices (SORN's) are updated to reflect any changes in the disclosure of information to other organizations in order to be consistent with the Privacy Act of 1974 and OMB Circular A-130, Appendix 1. **Assessment** *Determine that:* *(i) the organization updates SORN's to reflect changes in the disclosure of information (review, interview).*	OMB Memorandum 05-24
	PR-4	The applicant is notified of what information in identifiable form is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information. **Assessment** *Determine that:* *(i) Before receiving the PIV Card, the issuing facility requires the applicant to be notified of the personally identifiable information that is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (review, observe);* *(ii) the applicant is informed of what personally identifiable information is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (interview).*	FIPS 201-2, Section 2.11 – PIV Privacy Requirements

IAT = Security Management & Data Protection			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	PR-5	The issuing facility employs technologies that allow for continuous auditing of compliance with privacy policies and practices. **Assessment** *Determine that:* *(i) the issuing facility employs technologies that allow for the continuous auditing of compliance with privacy policies and practices. This could include the use of technology to monitor data access, data flows between information systems and the use of personally identifiable information (interview, test).*	FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	PR-6	In the case of termination, any personally identifiable information that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies. **Assessment** *Determine that:* *(i) as part of PIV Card termination, the organization disposes of personally identifiable information in accordance with its privacy and data retention policies while taking in account the grace period provisions (review, interview).*	FIPS 201-2, Section 2.9.4 – PIV Card Termination Requirements FIPS 201-2, Section 2.8.2 – Grace Period

2122

IAT = Infrastructure Elements			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Deployed Products & Information Systems	DP-1	In order to be compliant with the provisions of OMB Circular A-130, App III, the issuer information system(s) are authorized to operate in accordance with NIST SP 800-37-1, Guide for Applying the Risk Management Framework to Federal Information Systems *A Security Life Cycle Approach* **Assessment** *Determine that:* *(i) the organization has a letter showing the current authorization decision of each information system used to support the issuer (review).*	FIPS 201-2, Appendix A.2 Application of Risk Management Framework to IT System(s) Supporting PCI FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	DP-2	Every product utilized by an issuer facility is from the GSA FIPS 201/FICAM testing program's Approved Product List (APL) where applicable. **Assessment** *Determine that:* *(i) for each product that falls within one of the categories in the GSA* FIPS 201/FICAM testing program*, its presence (make, model, versions) is checked on the APL (review);* *(ii) there is no product in operation that has been moved to the GSA FIPS 201/FICAM testing program's Removed Product List (RPL).*	OMB Memorandum 05-24 Federal Acquisition Regulation (**FAR**), Section **4.1302** Acquisition of approved products and services for personal identity verification.

IAT = Infrastructure Elements			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	DP-3	The organization has submitted to GSA for testing a personalized PIV Card, issued from their production system. **Assessment** *Determine that:* *(i) the organization has a test report from GSA showing successful conformance of the PIV credentials on the PIV Card to the PIV Data Model (review);* *(ii) The organization continues to submit personalized PIV Cards on an annual basis to GSA for testing (review).*	OMB Memorandum 07-06

2123

IAT = Infrastructure Elements			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Implementation of Credentialing Infrastructures	CI-1	For legacy Public Key Infrastructures (PKI's), the organization's CA is cross-certified with the Federal Bridge (FBCA) and issues certificates with the id-fpki-common-authentication and id-fpki-common-authentication policy OIDs of the U.S. Federal PKI Common Policy Framework **Assessment** *Determine that:* *(i) the organization's CA is listed on http://www.idmanagement.gov/entities-cross-certified-federal-bridge as being cross-certified and authorized to issue certificates with the appropriate OIDs (review).*	FIPS 201-2, Section 5.4 – Legacy PKI
	CI-2	For non-legacy PKI's, all certificates issued to support PIV Card authentication are issued under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. **Assessment** *Determine that:* *(i) the PKI provider is listed on http://www.idmanagement.gov/list-certified-shared-service-providers as being a shared service provider (review).*	FIPS 201-2, Section 5.2 – PKI Certificate
	CI-3	When cards are personalized, PIV Card Application Administration Keys are set to be specific to each PIV Card. That is, each PIV Card contains a unique PIV Card Application Administration Keys. **Assessment** *Determine that:* *(i) the CMS vendor's documentation shows the use of unique PIV Card Application Administration Keys (review);* *(ii) the OIMO indicates that PIV Card Application Administration Keys are unique (interview).*	FIPS 201-2, Section 4.3.2 – Activation by Card Management System

IAT = Infrastructure Elements			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	CI-4	Fingerprint images retained by organizations are formatted according to SP 800-76-2. **Assessment** *Determine that:* *(i) the fingerprint images are formatted according to Table 4 in SP 800-76-2 and INCITS 381-2004 (review, test).*	SP 800-76-2, Section 3.3 – Fingerprint image format for images retained by agencies
	CI-5	Facial images collected during identity proofing and registration are formatted such that they conform to SP 800-76-2. **Assessment** *Determine that:* *(i)the facial images are formatted according to Table 12 in SP 800-76-2 and INCITS 385 (review, test).*	SP 800-76-2, Section 7.2 – Acquisition and Format
	CI-6	The fingerprint templates stored on the PIV Card (which is used for off-card comparison) are (i) prepared from images of the primary and secondary fingers where the choice of fingers is based on the criteria described in SP 800-76-2 Section 4.2, and (ii) formatted such that they conform to SP 800-76-2. **Assessment** *Determine that:* *(i) the procedures used to fingerprint the applicant are based on the primary and secondary finger selection criteria as detailed in SP 800-76-2 Section 4.2 (review, observe);* *(ii) the fingerprint templates are prepared from images of the primary and secondary fingers (test);* *(iii) the fingerprint templates are formatted according to Table 6 in SP 800-76-2 and INCITS 378-2004 (review, test).*	SP 800-76-2, Section .4.2 – Source Images
	CI-7 (NEW)	The identity management system (IDMS) should reflect the adjudication status of each PIV cardholder. **Assessment** *Determine that:* *(i) the issuer's identity management system is capable of recording the adjudication status of each PIV Cardholder (observe).*	FIPS 201-2, Section 2.8 – PIV Card Issuance Requirements
	CI-8 (NEW)	If implemented, iris images collected during identity proofing and registration are formatted such that they conform to SP 800-76-2, if applicable. **Assessment** *Determine that:* *(i) the iris images are formatted according to Table 9 in SP 800-76-2 and ISO/IEC 19794-6:2011 (review, test)*	SP 800-76-2, Section 6.3 – Iris image specification for PIV Cards

IAT = Infrastructure Elements			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	CI-9 (NEW)	If implemented, Fingerprint templates, for on-card comparison, collected during identity proofing and registration are formatted such that they conform to SP 800-76-2, if applicable. **Assessment** *Determine that:* *(i) the fingerprint templates for on-card comparison are formatted according to Table 7 in SP 800-76-2 and ISO/IEC 19794-2:2011 (review, test).*	SP 800-76-2, Section 5.5.1 – Biometric Information Template
	CI-10 (NEW)	For issuers that implement the chain of trust, this data is represented in an XML schema in accordance with SP 800-156. The chain of trust include the following items: (i) a log of activities, (ii) enrollment data record, (iii) most recent unique identifiers, (iv) Information about the authorizing entity, (v) current status of the background investigation, (vi) the evidence of authorization if the credential is issued under a pseudonym, (vii) Any data or any subsequent changes in the data about the cardholder. **Assessment** *Determine that:* *(i) the chain of trust implemented by the issuer is conformant to the XML specification (review, test).*	SP 800-156, Section 2 - Chain-of-Trust Data Representation

2124

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Sponsorship Process	SP-1	A PIV Card is issued only upon request by proper authority. **Assessment** *Determine that:* *(i) the process for making a request is documented (review);* *(ii) A request from a valid authority is required to issue a PIV Card (observe).*	FIPS 201-2, Section 2.1 – Control Objectives
	SP-2	The issuing facility collects personal information using only forms approved by OMB under the Paperwork Reduction Act of 1995. **Assessment** *Determine that*: *(i) forms used to collect personal information have been approved by OMB (review, observe).*	OMB Memorandum 07-06

2125

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Identity Proofing Process / Registration	EI-1	The issuing facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the applicant. **Assessment** *Determine that:* *(i) the issuing facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the applicant (interview, observe);* *(ii) the issuing facility has materials used to train identity proofing officials on how to verify the authenticity of the source documents (review).*	FIPS 201-2, Section 2.1 – Control Objectives
	EI-2	The issuing facility requires the applicant to appear in-person at least once before the issuance of a PIV Card. **Assessment** *Determine that:* *(i) the requirement that an applicant appear in-person at least once before the issuance of a PIV Card is documented (review);* *(ii) the applicant appears in-person at least once before the issuance of a PIV Card (observe).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements
	EI-3	Two identity source documents are checked based on those listed in Section 2.7 of FIPS 201-2 and are neither expired nor cancelled. **Assessment** *Determine that:* *(i) the requirement to check two identity source documents based on the list provided in Section 2.7 of FIPS 201-2,is documented (review);* *(ii) two identity source documents are checked in accordance, during identity proofing process (observe);* *(iii) If the two identity source documents bear different names, evidence of a formal name change is provided (review, observe).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements
	EI-4	One of the identity source documents used to verify the claimed identity of the applicant is a valid Federal or state government-issued photo identification. **Assessment** Determine that: *(i) the requirement that one of the identity source documents is a valid Federal or state government issued photo ID is documented (review);* *(ii) one of the identity source documents used to verify the claimed identity of the applicant is a valid Federal or state government-issued photo identification (observe).*	FIPS 201-2, Section 2.1 - Control Objectives
	EI-5	Moved to MP-9.	-

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	EI-6	This control has been withdrawn. Biometrics (fingerprint, facial image and the optional iris images) can be reused for up to 12 years.	-
	EI-7	The biometrics (fingerprints, facial image and the optional iris images) that are used to personalize the PIV Card must be captured during the identity proofing and registration process. **Assessment** Determine that: *(i) the requirement to capture biometrics (fingerprints, facial image and optional iris images) that are used to personalize the PIV Card must be captured during identity proofing and registration process is documented (review);* *(ii) The biometrics (fingerprints, facial image, and the optional iris image) that are used to personalize the PIV Card are captured during the identity proofing and registration process (observe).*	FIPS 201-2, Section 2.8 - PIV Card Issuance Requirements
	EI-8	This control has been withdrawn. FIPS 201-2 does not require that a PIV Card be reissued within 6 weeks before expiration of the old PIV Card.	-
	EI-9	The issuing facility captures the applicant's fingerprints in accordance with any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card. **Assessment** *(i) the issuing facility captures the applicant's fingerprints in accordance with any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card (observe).*	SP 800-76-2, Section 3.2 – Fingerprint Image Acquisition
	EI-10	The issuing facility has an attending official present at the time of biometric (fingerprint and optional iris images) capture. **Assessment** *Determine that:* *(i) the requirement that the issuing facility has an attending official present at the time of biometric (fingerprint and optional iris images) capture is documented (review);* *(i) the issuing facility has an attending official present at the time of biometric (fingerprint and optional iris images) capture (observe).*	SP 800-76-2, Section 3.2 – Fingerprint Image Acquisition SP 800-76-2, Section 6.6 - Iris image quality control

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	EI-11	The issuing facility acquires fingerprint images in accordance with Table 3 in 800-76-2. **Assessment** *Determine that:* *(i) fingers are inspected for the absence dirt, coatings, gels, and other of foreign materials (observe);* *(ii) scanner and card surfaces are clean (observe);* *(iii) the presentation of fingers for a plain live scan, rolled live scan, and rolled ink card are based on procedures in Table 2 of 800-76-2 (observe);* *(ii) multi-finger plain impression images are properly segmented into single finger images (observe).*	SP 800-76-2, Section 3.2 – Fingerprint Image Acquisition
	EI-12	The issuing facility captures the 10 fingerprints of the applicant. In the case where less than ten fingers are available, the missing fingers are labeled before transmitting to the FBI for the purpose of conducting a background investigation. **Assessment** *Determine that:* *(i) the requirement that the issuing facility captures the 10 fingerprints of the applicant and labels any missing fingers is documented (review);* *(ii) the issuing facility captures the 10 fingerprints of the applicant and labels any missing fingers (observe).*	SP 800-76-2, Section 3.2 – Fingerprint Image Acquisition
	EI-13 (NEW)	If the biometric (fingerprint) data collected to personalize the PIV Card and the biometric data (fingerprints) collected to support background investigations are collected on separate occasions, then a 1:1 biometric match of the applicant is performed at each visit against biometric data collected during a previous visit. . **Assessment** *Determine that:* *(i) the requirement that if the biometric data for personalization and background investigation are collected on separate occasions a 1:1 biometric match of the applicant is performed at each visit against biometric data collected during a previous visit (review, observe).*	FIPS 201-2, Section 2.4 - Biometric Data Collection for PIV Card

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Adjudication Process	AP-1	The organization ensures: (a) the initiation of a Tier 1 or higher federal background investigation and (b) the completion of the National Agency Check (NAC) of the background investigation prior to issuance of the PIV Card; when a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record cannot be referenced. **Assessment:** *Determine that:* *(i) the organization references a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record for the applicant (review, observe);* *(ii) the organization conducts the appropriate level of background investigation prior to PIV Card issuance if a previously completed and favorably adjudicated result cannot be obtained(review, observe).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements
	AP-2	In cases where the NAC results are not received within 5 days of the NAC initiation, the FBI NCHC (fingerprint check) portion of the NAC is completed before PIV Card issuance. **Assessment** *Determine that:* (i) *the PIV Card is issued only after successful completion of the NCHC (fingerprint check) portion of the NAC (review, observe).*	FIPS 201-2, Section 2.7 – PIV Identity Proofing and Registration Requirements
	AP-3 (NEW)	The organization follows credentialing guidance issued by the Director of the Office of Personnel Management (OPM) and Office of Management and Budget (OMB). **Assessment:** *Determine that:* *(i) the facility has documented procedures follow the credentialing guidance issued by OPM and OMB (review).*	FIPS 201-2, Section 2.2 – Credentialing Requirements Springer Memo (http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf)and the Federal Investigative Standards OMB Memorandum 05-24
	AP-4 (NEW)	In the absence of an FBI NCHC (e.g., due to unclassifiable fingerprints) the NAC results are required prior to issuing a PIV Card. **Assessment:** *Determine that:* *(i) If FBI NCHC check cannot be completed, the organization does not issue PIV Cards until the results of the NAC are obtained (review, interview).*	FIPS 201-2, Section 2.8 – PIV Card Issuance Requirements.

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	AP-5 (NEW)	The PIV Card is terminated if the results of the background investigation so justify. **Assessment:** *Determine that:* *(i) The organization revokes the PIV Card if it is issued on the basis of the FBI NCHC check and the NAC results once obtained are unfavorable (review, interview)*	FIPS 201-2, Section 2.8 – PIV Card Issuance Requirements. Springer Memo (http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf)and the Federal Investigative Standards

2140
2141

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Card Production Process	CP-1	The PIV Card implements security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. **Assessment** *Determine that:* *(i) the PIV Card contains at least one security feature. Examples of these security features include the following: (i) Optical varying structures, (ii) Optical varying inks, (iii) Laser etching and engraving, (iv) Holograms, (v) Holographic images, (vi) Watermarks (interview, observe).* *(ii) Incorporation of security features—(i) are in accordance with durability requirements; (ii) are free of defects, such as fading and discoloration; (iii) do not obscure printed information; and (iv) do not impede access to machine-readable information (interview, observe)*	FIPS 201-2, Section 4.1.2 – Tamper Proofing and Resistance
	CP-2	The PIV Card is not embossed. **Assessment** *Determine that:* *(i) the PIV Card is not embossed (review, observe)*	FIPS 201-2, Section 4.1.3 – Physical Characteristics and Durability
	CP-3	Decals are not adhered to the PIV Card. **Assessment** *Determine that:* *(i) decals are not adhered to the PIV Card (review, observe).*	FIPS 201-2, Section 4.1.3 – Physical Characteristics and Durability
	CP-4	If organizations choose to punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard, all such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity is not adversely impacted. **Assessment** *Determine that:* *(i) the integrity of a PIV Card is not affected by a punched opening (test);* *(ii) Documentation from the PIV Card vendor shows that durability and operational requirements have not been compromised (review).*	FIPS 201-2, Section 4.1.3 – Physical Characteristics and Durability

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	CP-5 (NEW)	If organization choose to use tactilely discernible marks (Edge Ridging or Notched Corner Tactile Marker or Laser Engraving Tactile Marker) to indicate card orientation, such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted. **Assessment** *Determine that:* *(i) the integrity of a PIV Card is not affected by the use of the tactile marker(s) (test);* *(ii) Documentation from the PIV Card vendor shows that durability and operational requirements have not been compromised (review).*	FIPS 201-2, Section 4.1.3 – Physical Characteristics and Durability
	CP-6 (NEW)	PIV Cards that contain topographical defects (e.g., scratches, poor color, fading, etc.) or that are not properly printed are destroyed. **Assessment** *Determine that:* *(i) The organization has a procedure to destroy PIV Card that contain topographical defects or that are not printed properly (review);* *(ii) the organization destroys PIV Cards that contain topographical defects or that are not printed properly (observe).*	FIPS 201-2, Section 2.8 – PIV Card Issuance Requirements
	CP-7 (NEW)	PIV Cards are printed using the color representation as specified in Table 4-2 Color Representation in FIPS 201-2, Section 4.1.5. **Assessment** *Determine that:* *(i) the issuer uses an appropriate color representation for printing PIV Cards (review, test);* *(ii) the card production system is configured to use an appropriate color representation system (review).*	FIPS 201-2, Section 4.1.5 – Color Representation

2142

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Activation/Issuance Process	AI-1	The personalized PIV Card complies with all the mandatory items on the front of the PIV Card. **Assessment** *Determine that:* *(i) the PIV Card meets specific requirements in FIPS 201-2 for: (i) photograph; (ii) name; (iii) employee affiliation; (iv) agency, department, or organization (v) card expiration dates (zones 14f & 19f); (vi) color coding for employee affiliation(; (vii) affiliation color code symbol (observe, test).*	FIPS 201-2, Section 4.1.4.1 – Mandatory Items on the Front of the PIV Card

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	AI-2	The personalized PIV Card complies with all the mandatory items on the back of the PIV Card. **Assessment** *Determine that:* *(i) the PIV Card meets specific requirements in FIPS 201-2 for (i) an agency card serial number; (ii) and issuer identification number (observe, test).*	FIPS 201-2, Section 4.1.4.2 – Mandatory Items on the Back of the Card
	AI-3	If one or more optional items are printed on the front of the PIV Card, they comply with the requirements for the optional items on the front on the PIV Card. **Assessment** *Determine that:* *(i) the PIV Card meets specific requirements in FIPS 201-2 if it includes optional items on the front of the card, such as (i) a signature; (ii) agency specific text area; (iii) rank; (iv) portable data file; (v) header; (vi) agency seal; (vii) footer; (viii) issue date; (ix); (x) photo border; (xi) agency specific data; (xii) organizational affiliation abbreviation; and (xiii) edge ridging or notched corner tactile marking; (xiv) laser tactile marker (observe, test).*	FIPS 201-2, Section 4.1.4.3 – Optional Items on the Front of the Card
	AI-4	If one or more optional items are printed on the back of the PIV Card, they comply with the requirements for the optional items on the back on the PIV Card. **Assessment** *Determine that:* *(i) the PIV Card meets specific requirements in FIPS 201-2 if it includes optional items on the back of the card, such as (i) magnetic stripe; (ii) return to address (iii) physical characteristics of the cardholder; (iv) additional language for emergency responder officials; (v) standard Section 499, Title 18 language; (vi) linear 3 of 9 bar code; (vii) agency-specific text (zones 9 & 10) (observe, test).*	FIPS 201-2, Section 4.1.4.4 – Optional Items on the Back of the Card
	AI-5	The PIV Card includes mechanisms to block activation of the card after a number of consecutive failed activation attempts. . **Assessment** *Determine that:* *(i) the PIV Card can block activation if the number of consecutive failed attempts has exceeded that set by the issuer (test, observe).*	FIPS 201-2, Section 4.3.1 – Activation by Cardholder

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	AI-6	The PIV Card is valid for no more than six years. **Assessment** *Determine that:* *(i) the expiration date printed on the PIV Card is no more than six years from the issuance date (observe);* *(ii) the expiration date is printed in the CHUID (test);* *(iii) the two dates (printed on the card and the expiration date in the CHUID) are the same (test).* *(iv) the biometric that is used for reissuance is not older than 12 years (review)*	FIPS 201-2, Section 2.8 – PIV Card Issuance Requirements FIPS 201-2, Section 2.9.1 – PIV Reissuance Requirements
	AI-7	Before the PIV Card is provided to the applicant, the issuer performs a 1:1 biometric match of the applicant against biometrics available on the PIV Card or in the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. If the match is unsuccessful, or if no biometric data is available, the cardholder provides two identity source documents (as specified in Section 2.7), and an attending operator inspects these and compares the cardholder with the facial image printed on the PIV Card. **Assessment** *Determine that:* *(i) the issuer performs a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV chain of trust prior to releasing the card (review);* *(ii) the issuer has alternate processes in place for situations where biometric matches are not possible (review, observe).*	FIPS 201-2, Section 2.8 – PIV Card Issuance
	AI-8	This control has been withdrawn. Renewal is covered as part of re-issuance in FIPS 201-2.	-
	AI-9	The issuer advises applicants that the PIN on the PIV Card should not be easily-guessable or otherwise individually-identifiable in nature. **Assessment** *Determine that:* *(i) the requirement that the issuer advises applicants that the PIN on the PIV Card should not be easily guessable or otherwise individually-identifiable in nature is documented (review);* *(ii) the issuer advises applicants that the PIN on the PIV Card should not be easily guessable or otherwise individually-identifiable in nature (observe).*	FIPS 201-2, Section 4.3.1 Activation by Cardholder

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
	AI-10	PIV cards issued have the PIV NACI indicator set appropriately based on whether the subject's background investigation was incomplete at the time of credential issuance. **Assessment** Determine that: *(i) the PIV NACI indicator is set to TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed, and (2) a background investigation has been initiated but has not completed (review, observe, test);* *(ii) The PIV NACI indicator is set to FALSE if, at the time of credential issuance, the subject's background investigation has been completed and successfully adjudicated (review, observe, test).*	FIPS 201-2, Appendix B.2 - PIV Certificate Extension
	AI-11	This control has been moved to MP-12.	-
	AI-12	The organization issues electromagnetically opaque holders or other technology to protect against any unauthorized contactless access to information stored on a PIV Card. **Assessment** *Determine that:* *(i) the requirement that electromagnetically opaque holders or other technology is provided at the time of PIV Card issuance (review, observe).*	FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	AI-13	This control has been moved to MP-8.	-
	AI-14 (NEW)	If pseudonyms are required to protect an employee or contractor, the issuance of a PIV Card uses agency-approved pseudonyms and follows normal procedures for PIV Card issuance. **Assessment** *Determine that:* *(i) The organization has determined that use of a pseudonym is necessary to protect employees or contractors (review).* *(ii) The organization maintains a list of pseudonyms that have been issued and can link them to employees or contractors authorized to receive the such pseudonyms (review);* (iii) *Issuance procedures for pseudonyms are consistent with procedures for issuing regular PIV Cards (review, observe).*	FIPS 201-2, Section 2.8.1 - Special Rule for Pseudonyms

2143

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
Maintenance Process	MP-1	A post-issuance update doesn't modify the PIV Card expiration date, FASC-N, or UUID. **Assessment** *Determine that:* *(i) the PIV Card expiration date, FASC-N or UUID is not modified post-issuance (review, interview).*	FIPS 201-2, Section 2.9.2 – PIV Card Post Issuance Update Requirements
	MP-2	In the case of re-issuance and termination, the PIV Card is collected and destroyed whenever possible. If the PIV Card cannot be collected and destroyed, the CA is informed and the certificates corresponding to the PIV Authentication key and the asymmetric Card Authentication key on the PIV Card are revoked. The certificates corresponding to the digital signature and key management keys are also revoked, if present. **Assessment** *Determine that:* *(i) in the case of reissuance and termination, the requirement that the PIV Card is collected and destroyed whenever possible is documented and performed (review, observe);* *(ii) the issuer has procedures to notify the CA in the event the PIV Card cannot be collected (review, observe).*	FIPS 201-2, Section 2.9.1 – PIV Reissuance Requirements FIPS 201-2, Section 2.9.4 - PIV Card Termination Requirements
	MP-3	During PIV Card re-issuance and termination any databases maintained by the PIV Card issuer that indicate current valid (or invalid) FASC-N or UUID values are updated to reflect the change in status. **Assessment** *Determine that:* *(i) databases maintained by the issuer that indicate FASC-N or UUID values are updated to reflect the change in status (review, observe);*	FIPS 201-2, Section 2.9.1 – PIV Reissuance Requirements FIPS 201-2, Section 2.9.4 - PIV Card Termination Requirements
	MP-4	If the PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification. **Assessment** *Determine that:* *(i) documentation includes the requirement that if PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification (review);* *(ii) if the PIV Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification (observe).*	FIPS 201-2, Section 2.9.1 – PIV Reissuance Requirements FIPS 201-2, Section 2.9.4 - PIV Card Termination Requirements
	MP-5	Upon PIV Card termination, the organization enforces a standard methodology of updating systems of records to indicate employee termination, and this status is distributed effectively throughout systems used for physical and logical access to organization facilities and resources.	Commonly accepted security readiness measures

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
		Assessment *Determine that:* *(i) the issuing facility has procedures to update information systems and disseminate information to indicate PIV Card termination (review);* *(ii) the organization's information systems are updated to indicate PIV Card termination (observe).*	
	MP-6	This control has been withdrawn. The requirement to post a quarterly report to the organization's website (and report the website to OMB) is already covered in OMB Memorandum 07-06.	OMB Memorandum 07-06-
	MP-7	The organization has completed a lifecycle walkthrough at one year intervals since the last authorization date, and the results are documented in a report to the DAO. **Assessment** *Determine that*: *(i) the organization has completed a lifecycle walkthrough to cover sponsorship, identity proofing, card production, activation/issuance and maintenance processes (interview);* *(ii) a lifecycle walkthrough has been completed at one year intervals since the last authorization date (interview);* *(iii) the results of the issuer lifecycle walkthrough have been documented and reviewed by the DAO (review, interview).*	SP 800-79-2, Section 5.4 - Monitoring Phase
	MP-8 (NEW)	The card issuer reissues a PIV Card without repeating the identity proofing and registration process if: (i) the issuer has access to the applicant's chain-of-trust record and the applicant can be reconnected to the chain-of-trust record, or (ii). if the match is unsuccessful, or if no biometric data is available, the cardholder provides two identity source documents (as specified in Section 2.7 of FIPS 201-2), and an attending operator inspects these and compares the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV Card. **Assessment** *Determine that:* *(i) the issuing facility verifies that PIV Card issuance has been authorized by a proper authority and that the employee's or contractor's background investigation is valid (review, observe);* *(ii) Re-investigations are performed if required, in accordance with OPM guidance (review);* *(iii) The issuing facility is able to reconnect the applicant to the chain-of-trust per FIPS 201-2 issuance requirements (observe).* *(iv) The issuing facility has alternate procedures to release the PIV Card when the biometric match is unsuccessful (review, observe);* *(v) Any data change about the cardholder, is recorded by the issuer in the chain-of-trust, if applicable (review, observe);* *(vi) Name changes are performed in accordance with Section*	FIPS 201-2, Section 2.8.2 – Grace Period FIPS 201-2, Section 2.9.1 - PIV Card Reissuance Requirements FIPS 201-2, Section 2.9.1.1 - Special Rule for Name Change by Cardholder

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
		2.9.1.1 of FIPS 201-2 (review, observe).	
	MP-9 (NEW)	The entire identity proofing, registration, and issuance process is repeated if the issuer: (i) does not maintain a chain-of-trust record for the cardholder or (ii) if the reissuance process was not started before the old PIV Card expired. **Assessment** *Determine that:* *(i) the issuing completes the entire identity proofing, registration and issuance process if they don't maintain a chain of trust or if the reissuance process was not started before the old PIV Card expired (review, observe).*	FIPS 201-2, Section 2.9.1 - PIV Card Reissuance Requirements
	MP-10 (NEW)	Previously collected biometric data is not reused with the new PIV Card if the expiration date of the new PIV Card is no later than 12 years after the date that the biometric data was obtained. **Assessment** *Determine that:* *(i) the issuing facility ensures that new biometric data is collected if the new PIV Card's expiration is 12 years after the collection of the initial biometric data available with the issuer (review, observe).*	FIPS 201-2, Section 2.9.1 - PIV Card Reissuance Requirements
	MP-11 (NEW)	Post issuance updates (either performed with the issuer in physical custody of the PIV Card or remotely) is performed with issuer security controls equivalent to those applied during PIV Card reissuance. These include the following: (i) communication between the PIV Card issuer and the PIV Card occurs only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card); (ii) data transmitted between the issuer and PIV Card is encrypted and contain data integrity checks; (iii) the PIV Card Application will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update. **Assessment** *Determine that:* *(i) post issuance updates include all required security controls be implemented by the issuer and the issuer information systems (review).*	FIPS 201-2, Section 2.9.2 - PIV Card Post Issuance Update Requirements
	MP-12 (NEW)	When a PIN reset is performed in-person at the issuing facility, before providing the reset PIV Card back to the cardholder, the issuer performs a 1:1 biometric match to ensure that the cardholder's biometric matches either the stored biometric on the PIV Card or biometric data stored in the chain-of-trust. In cases where a biometric match is not possible, the cardholder provides the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator inspects these and compares the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the card.	FIPS 201-2, Section 2.9.3 - PIV Card Verification Data Reset

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
		Assessment *Determine that:* *(i) the issuer performs a 1:1 biometric match of the cardholder against the biometric included in the PIV Card or in the PIV chain of trust prior to providing the reset PIV Card back to the cardholder (observe, test);* *(ii) the issuer has alternate processes in place for situations where biometric matches are not possible (review, observe).*	
	MP-13 (NEW)	When a PIN reset is performed at an unattended issuer-operated kiosk, the issuer ensures that the PIV Card is authenticated and that the cardholder's biometric matches either the stored biometric on the PIV Card, through an on-card 1:1 biometric match, or biometric data stored in the chain-of-trust, through an off-card 1:1 biometric match. If the biometric match or card authentication is unsuccessful, the kiosk does not reset the PIV Card. **Assessment** *Determine that:* *(i) the issuer's kiosk performs a 1:1 biometric match of the cardholder against the biometric included in the PIV Card or in the chain of trust prior to resetting the PIV Card (observe, test).*	FIPS 201-2, Section 2.9.3 - PIV Card Verification Data Reset
	MP-14 (NEW)	Remote PIN reset on a general computing platform (e.g., desktop, laptop) is only performed by the issuer if the following requirements are met: (i) the cardholder initiates a PIN reset with the issuer operator, (ii) the operator authenticates the owner of the PIV Card through an out-of-band authentication procedure (e.g., pre-registered knowledge tokens); (iii) the cardholder's biometric matches the stored biometric on the PIV Card through a 1:1 on-card biometric comparison. **Assessment** *Determine that:* *(i) remote PIN resets meet all security requirements to be implemented by the issuer and the issuer information systems (review, observe, test).*	FIPS 201-2, Section 2.9.3 - PIV Card Verification Data Reset
	MP-15 (NEW)	Before any verification data (e.g., PIN, OCC fingerprint templates templates, etc.) is reset, the issuer performs a 1:1 biometric match of the cardholder to reconnect to the chain-of-trust. The type of biometric used for the match is not the same as the type of biometric data that is being reset. If no alternative biometric data is available, the cardholder provides the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator inspects these and compares the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the PIV Card. **Assessment**	FIPS 201-2, Section 2.9.3 - PIV Card Verification Data Reset

IAT = Processes			
Authorization Focus Area	**Identifier**	**Issuer Control**	**Source**
		Determine that: *(i) the issuer performs a 1:1 biometric match of the cardholder against the biometric included in the PIV Card or in the chain of trust prior to providing the reset PIV Card back to the cardholder (observe, test);* *(ii) The same type of biometric used for the match is not the same as the type of biometric data that is being reset (observe, test);* *(iii) the issuer has alternate processes in place for situations where biometric matches are not possible (review, observe).*	

2144
2145

Appendix G.2: Controls and Assessment Procedures for Derived PIV Credential Issuers (DPCIs)

This appendix specifies the controls and assessment procedures for the Derived PIV Credential and its related token. The controls in this section are mapped to the PCI controls in G.1 to assist issuers that intend to issue both types of credentials. Unlike for a PIV Card Issuer, not all issuer controls are applicable to a Derived PIV Credential Issuer. Certain issuer controls are applicable to only LOA-3 or to only LOA-4 PIV Derived Credentials and therefore must be implemented by the issuer only if they are issuing that level of a Derived PIV Credential. This is represented via the "*applicability*" column within this Appendix. Controls with an applicability column marked with DPCI (e.g., without LOA-4 or 3 postfix) apply to both LOA-3 and LOA-4 Derived PIV Credential.

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Preparation and Maintenance of Documentation	DO(DC)-1	The organization develops and implements an issuer operations plan according to the template in Appendix D.2. The operations plan references other documents as needed. **Assessment** *Determine that:* *(i) the operations plan includes the relevant elements from the template in Appendix D.2 (review);* *(ii) the operations plan includes the list of issuer controls and the issuer control owner for each, how they were implemented and whether they are organization or facility specific (review);* *(iii) documentation that is not included in the operations plan is referenced accurately (review);* *(iv) the operations plan has been reviewed and approved by the DAO within the organization (review, interview).*	DPCI	SP 800-79-2, Section 2.11 – Authorization Package and Supporting Documentation
	DO(DC)-3	The organization has a written policy and procedures for initial issuance that are approved by the Federal department or agency. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for issuance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the policy and procedures have been signed off by the Federal department or agency*	DPCI	SP 800-157, Section 2 Lifecycle Activities and Related Requirements SP 800-157, Section 2.1 – Initial Issuance

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
		(review); (iv) *the organization will periodically review and update the policy and procedures as required (review, interview).*		
	DO(DC)-5	The organization has a written policy and procedures describing the conditions for Derived PIV Credential termination. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for Derived PIV Credential termination (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization will periodically review and update the policy as required (review, interview).*	DPCI	SP 800-157, Section 2 Lifecycle Activities and Related Requirements SP 800-157, Section 2.3 – Termination
	DO(DC)-6	The organization has a written policy and procedures describing the conditions for Derived PIV Credential maintenance. **Assessment** *Determine that*: *(i) the organization has developed and documented a written policy and procedures for Derived PIV Credential maintenance (review);* *(ii) the policy is consistent with the organization's mission and functions, FIPS 201-2 and applicable laws, directives, policies, regulations, standards, and guidance (review);* *(iii) the organization will periodically review and update the policy and procedures as required (review, interview).*	DPCI	SP 800-157, Section 2 Lifecycle Activities and Related Requirements SP 800-157, Section 2.2 -Maintenance

2159
2160

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Assignment of Roles and Responsibilities	RR(DC)-1	The organization has appointed the role of Senior Authorizing Official (SAO). **Assessment** *Determine that*: *(i) the organization has defined the role of Senior Authorizing Official and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of Senior Authorizing Official (review).*	DPCI	SP 800-79-2, Section 2.6 –Issuer Roles and Responsibilities
	RR(DC)-2	The organization has appointed the role of Designated Authorizing Official (DAO). **Assessment** *Determine that*: *(i) the organization has defined the role of Designated Authorizing Official and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of Designated Authorizing Official (review, interview).*	DPCI	SP 800-79-2, Section 2.6 – Issuer Roles and Responsibilities
	RR(DC)-3	The organization has appointed the role of Organization Identity Management Official (OIMO). **Assessment** *Determine that*: *(i) the organization has defined the role of Organization Identity Management Official and its responsibilities according to the requirements of SP 800-79-2 (interview);* *(ii) the organization has assigned the role of Organization Identity Management Official (review, interview).*	DPCI	SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities
	RR(DC)-4	The organization has appointed the role of Assessor. **Assessment** *Determine that*: *(i) the organization has defined the role of Assessor and its responsibilities according to the requirements of SP 800-79-2 (review);* *(ii) the organization has assigned the role of Assessor (review);* *(iii) the Assessor is a third party that is independent of, and organizationally separate from, the persons and office(s) directly responsible for the day-to-day operation of the organization (review, interview).*	DPCI	SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	RR(DC)-5	The organization has appointed the role of Privacy Official (PO). **Assessment** *Determine that*: *(i) the organization has defined the role of Privacy Official and its responsibilities according to the requirements of SP 800-79-2 (review);* *(iv) the organization has assigned the role of Assessor (review);* *(ii) the Privacy Official does not have any other roles in the organization (review, interview).*	DPCI	FIPS 201-2, Section 2.11 - PIV Privacy Requirements SP 800-79-2, Section 2-6 – Issuer Roles and Responsibilities

2161
2162

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Facility and Personnel Readiness	**Facility**			
	FP(DC)-1	Minimum physical controls at the issuing facility are implemented. These include: (i) use of locked rooms, safes, and lockable cabinets (as appropriate); (ii) physical access to key areas within the facility is restricted to authorized personnel, (iii) security monitoring and automated alarms are implemented, (iv) emergency power and lighting are available, and (v) fire prevention and protection mechanisms are implemented. **Assessment** *Determine that:* *(i) the OIMO and Issuing Facility Manager(s) are aware of the minimum set of physical controls that need to be in place at the facility(ies) (interview);* *(ii) the minimum physical security controls are implemented by the issuing facility (observe).*	DPCI - LOA 4 Only	Commonly accepted security readiness measures
	FP(DC)-2	Issuer Documentation (e.g., operations plan, standard operating procedures, and contracts) are maintained. **Assessment** *Determine that:* *(i) the most current versions of the issuer documentation is available \ for reference as needed (interview, review).*	DPCI	Commonly accepted security readiness measures
	Equipment			

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	FP(DC)-3	The issuer has developed and maintains a contingency/disaster recovery plan for the information systems, which is stored securely. **Assessment** *Determine that*: *(i) the contingency plan/ disaster recovery plan is stored securely (interview, observe);* *(ii) the issuer personnel are knowledgeable on how to restore/reconstitute the information systems in case of system failures (interview).*	DPCI	Commonly accepted security readiness measures
	FP(DC)-4	The information systems are managed using a system development life cycle (SDLC) methodology that includes information security considerations. **Assessment** *Determine that*: *(i) the information system used by the organization has been developed using an SDLC methodology (review, interview);* *(ii) information system security is considered as part of the development life cycle (review).*	DPCI	Commonly accepted security readiness measures
	FP(DC)-5	Derived PIV Credential activation and issuance workstations are situated in an enclosed area (wall or partition) to provide privacy for the subscriber and the operator. **Assessment** *Determine that*: *(i) Issuing facility workstations are situated in an enclosed area (wall or partition) such that unauthorized individuals cannot see subscriber information (observe).*	DPCI - LOA 4 Only	Commonly accepted security readiness measures
	Key Personnel			

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	FP(DC)-6	All operators who perform roles of initial issuance, maintenance, or termination are allowed access to information systems only when authenticated through a PIV Card. **Assessment** *Determine that*: *(i) the requirement that all operators who perform roles in the areas of initial issuance, maintenance or termination are allowed logical access to information systems only when authenticated through a PIV Card, has been documented in the standard operating procedures (review);* *(ii) Operators use PIV Cards to access information systems in the course of performing their roles within the Derived PIV Credential lifecycle processes (observe).*	DPCI	OMB Memorandum 11-11
	FP(DC)-7	All operators who perform roles within the areas of initial issuance, maintenance and termination have undergone training that is specific to their duties prior to being allowed to perform in that function. **Assessment** *Determine that*: *(i) all operators who perform roles in the areas of initial issuance, maintenance and termination are allowed access to information systems only after completing a training course specific to their duties. (interview, review);* *(ii) Records showing that the appropriate training course has been completed by issuer personnel are stored for audit purposes (interview, review).*	DPCI	Commonly accepted security readiness measures

IAT = Organizational Preparedness				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	FP(DC)-8	All pre-personalized removable (non-embedded) hardware cryptographic tokens (e.g., SD Card, UICC, USB) received from token vendors are received only by authorized personnel who ensure that these tokens is stored, handled and disposed off securely at the issuing facility. **Assessment** *Determine that*: *(i) the issuing facility has an authorized list of personnel that are responsible for ensuring that smart card stock is received and stored securely (interview);* *(ii) procedures for receiving, storing and destroying tokens are documented in the issuing facility's standard operating procedures (review);* *(iii) the authorized personnel are knowledgeable of the procedures on how to receive, store and destroy the tokens (interview).*	DPCI - LOA 4 Only	Commonly accepted security readiness measures
	FP(DC)-9	The organization maintains a current list of designated points of contact and alternate points of contact for all issuing facilities used by the organization for Derived PIV Credential issuance, maintenance and termination processes. **Assessment** *Determine that*: *(i) the organization maintains a list of designated points of contact and alternate points of contact for all issuing facilities used by the organization (review);* *(ii) the list is current and the individuals named are the correct points of contact (review and interview).*	DPCI - LOA 4 Only	Commonly accepted security readiness measures

2163
2164

IAT = Security Management & Data Protection				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Protection of Stored and Transmitted Data	ST(DC)-1	The issuer information systems that contain information in identifiable form are handled in compliance with Federal laws and policies, including the Privacy Act of 1974. **Assessment** *Determine that*: *(i) the organization does not disclose any record which is contained in the system of records to any person, or to another organization unless written consent has been given by the individual to whom the record pertains unless one of the exceptions for disclosure in the Privacy Act are met (review, interview);* *(ii) individuals are permitted to gain access to their personal record and the information is provided in a form comprehensible to them (review, interview);* *(iii) individuals are able to request amendments to records pertaining to them, corrections are made promptly and if not, the individual is provided with a reason for the refusal and is able to request a review of the refusal (review, interview);* *(iv) the organization notifies an individual when their record is made available to any person under a compulsory legal process when such a process becomes a matter of public record (review, interview).*	DPCI	FIPS 201-2, Section 2.11 - PIV Privacy Requirements
	ST(DC)-2	The information systems protect the integrity and confidentiality of transmitted information. **Assessment** *Determine that*: *(i) the integrity of transmitted information is protected (interview, test, review);* *(ii) the confidentiality of transmitted information is protected (interview, test, review).*	DPCI	FIPS 201-2, Section 2.11 - PIV Privacy Requirements SP 800-157, Section 2.1 - Initial Issuance

2167

IAT = Security Management & Data Protection				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Enforcement of Privacy Requirements	PR(DC)-1	Privacy act statement/notice, complaint procedures, appeals procedures for those denied Derived PIV Credentials or whose credentials are revoked, and sanctions for employees violating privacy policies are developed and posted by the organization in multiple locations (e.g., internet site, human resource offices, regional offices, and contractor orientation handouts). **Assessment** *Determine that*: *(i) the issuer has posted privacy act statement/notice, complaint procedures, appeals procedures for those denied a token or whose token are revoked, and sanctions for employees violating privacy policies (interview, review).*	DPCI	OMB Memorandum 05-24
	PR(DC)-2	The organization has conducted a Privacy Impact Assessment of their issuer information system (s), compliant with Section 208 of the E-Government Act of 2002 and based on guidance found in Appendix E of OMB Memorandum 06-06. **Assessment** *Determine that:* *(i) the organization has conducted a Privacy Impact Assessment of their issuer information system(s) based on guidance found in Appendix E of OMB Memorandum 06-06 (review);* *(ii) the organization has submitted the Privacy Impact Assessment of their issuer information system (s) to OMB (interview, review).*	DPCI	OMB Memorandum 05-24 OMB Memorandum 06-06 (Appendix E)
	PR(DC)-3	The organization's employee and contractor identification systems of records notices (SORN's) are updated to reflect any changes in the disclosure of information to other organizations in order to be consistent with the Privacy Act of 1974 and OMB Circular A-130, Appendix 1. **Assessment** *Determine that:* *(i) the organization updates SORN's to reflect changes in the disclosure of information (review, interview).*	DPCI	OMB Memorandum 05-24

IAT = Security Management & Data Protection				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	PR(DC)-4	The subscriber is notified of what information in identifiable form is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information. **Assessment** *Determine that:* *(i) Before receiving the Derived PIV Credential , the issuer requires the subscriber to be notified of the personally identifiable information that is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (review, observe);* *(ii) the subscriber is informed of what personally identifiable information is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (interview).*	DPCI	FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	PR(DC)-5	The issuer employs technologies that allow for continuous auditing of compliance with privacy policies and practices. **Assessment** *Determine that:* *(i) the issuer employs technologies that allow for the continuous auditing of compliance with privacy policies and practices. This could include the use of technology to monitor data access, data flows between information systems and the use of personally identifiable information (interview, test).*	DPCI	FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	PR(DC)-6	In the case of termination, any personally identifiable information that has been collected from the subscriber is disposed of in accordance with the stated privacy and data retention policies. **Assessment** *Determine that:* *(i) as part of Derived PIV Credential termination, the organization disposes of personally identifiable information in accordance with its privacy and data retention policies (review, interview).*	DPCI	FIPS 201-2, Section 2.9.4 – PIV Card Termination Requirements

2168
2169

2170

IAT = Infrastructure Elements				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Deployed Products & Information Systems	DP(DC)-1	In order to be compliant with the provisions of OMB Circular A-130, App III, the issuer information system(s) are authorized to operate in accordance with NIST SP 800-37-1, Guide for Applying the Risk Management Framework to Federal Information Systems *A Security Life Cycle Approach* **Assessment** *Determine that:* *(i) the organization has a letter showing the current authorization decision of each information system used to support the issuer (review).*	DPCI	FIPS 201-2, Appendix A.2 Application of Risk Management Framework to IT System(s) Supporting PCI FIPS 201-2, Section 2.11 – PIV Privacy Requirements
	DP(DC)-2	Products utilized by an issuer are from the GSA FIPS 201/FICAM testing program's Approved Product List (APL) where applicable.[17] **Assessment** *Determine that:* *(i) for each product that falls within one of the categories in the GSA* FIPS 201/FICAM testing program*, its presence (make, model, versions) is checked on the APL (review);* *(ii) no product in operation has been moved to the GSA FIPS 201/FICAM testing program's Removed Product List (RPL).*	DPCI	OMB Memorandum 05-24 Federal Acquisition Regulation (**FAR**), Section **4.1302** Acquisition of approved products and services for personal identity verification.
	DP(DC)-3	The organization has submitted to GSA for testing Derived PIV Credential tokens in the chosen target formats the organization supports.[18] **Assessment** *Determine that:* *(i) the organization has test report(s) from the GSA showing successful conformance of each format supported by the organization to the PIV Derived Credential Data Model (review).* *(ii) The organization continues to submit personalized PIV Cards on an annual basis to GSA for testing (review).*	DPCI	OMB Memorandum 07-06

2171
2172

[17] This control will be applicable when approval procedures, test procedures and test tools for Derived PIV Credentials are available through GSA.

[18] This control will be applicable when GSA commences testing activities for Derived PIV Credentials.

IAT = Infrastructure Elements				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Implementation of Credentialing Infrastructures	CI(DC)-2	PIV Derived Authentication certificates are issued under either: (i) the id-fpki-common-pivAuth-derived-hardware (LOA-4) or the id-fpki-common-pivAuth-derived (LOA-3) policy of the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. **Assessment** *Determine that:* *(i) the PKI is listed on the Federal PKI Policy Authority's website as being a provider of Derived PIV Credential certificates (review).*	DPCI	SP 800-157, Section 3.1 – Certificate Policies
	CI(DC)-11 (NEW)	For PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived-hardware, the PIV Derived Authentication key pair is generated within a hardware cryptographic module that has been validated to FIPS 140-2 Level 2 or higher that provides Level 3 physical security to protect the PIV Derived Authentication private key while in storage and that does not permit exportation of the private key. **Assessment** *Determine that:* *(i) the organization ensures that PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived-hardware certificate policy are generated on cryptographic modules validated against FIPS 140-2 at Level 2 or higher with Level 3 physical security (review).*	DPCI - LOA 4 Only	SP 800-157, Section 3.2 – Cryptographic Specifications
	CI(DC)-12 (NEW)	For PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived, the PIV Derived Authentication key pair is generated within a cryptographic module that has been validated to FIPS 140-2 Level 1 or higher. **Assessment** *Determine that:* *(i) the organization ensures that PIV Derived Authentication certificates issued under id-fpki-common-pivAuth-derived certificate policy are generated on FIPS 140-2 validated cryptographic modules (review).*	DPCI - LOA 3 Only	SP 800-157, Section 3.2 – Cryptographic Specifications

IAT = Infrastructure Elements				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	CI(DC)-13 (NEW)	The issuer of the Derived PIV Credential maintains a link between the subscriber's PIV Card and the Derived PIV Credential to enable the issuer of the latter credential to track the status of the PIV Card in order to perform timely maintenance and termination activities in response to changes in the status of the PIV Card. Examples of such linkages include: (i) if the Derived PIV Credential is issued by the same organization that issued the subscriber's PIV Card, the linkage between the two credentials is maintained through the common Identity Management System (IDMS) database, (ii) the Backend Attribute Exchange is queried for the termination status of the PIV Card, if an attribute providing this information is defined and the issuer of the PIV Card maintains this attribute for the subscriber, (iii) the issuer of the PIV Card maintains a list of corresponding Derived PIV Credential issuers and sends notification to the latter set when the PIV Card is terminated, (iv) if a Uniform Reliability and Revocation Service (URRS) is implemented in accordance with Section 3.7 of NISTIR7817, the issuer of a Derived PIV Credential obtains termination status of the Subscriber's PIV Card through the URRS. **Assessment** *Determine that:* *(i) the issuer has developed procedures for updating Derived PIV Credentials data as a result of a change to PIV Card information (review);* *(ii) the issuer of the Derived PIV Credential does not solely rely on tracking the revocation status of the PIV Authentication certificate as a means of tracking the termination status of the PIV Card (review);* *(iii) The issuer has implemented one or more mechanisms to trigger an update to the Derived PIV Credential as a result of a change to the PIV Card (review, observe).*	DPCI	SP 800-157, Section 2.2 – Maintenance SP 800-157, Section 2.4 – Linkage with PIV Card
	CI(DC)-14 (NEW)	The issuer retains for future reference the biometric sample used to validate the Applicant. **Assessment** *Determine that:* *(i) the issuer has implemented a process/system to retain the Applicant's biometric for maintenance of the Derived PIV Credential (review).*	DPCI – LOA 4 Only	SP 800-157, Section 2.1 – Initial Issuance

2173

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Sponsorship Process	SP(DC)-1	A Derived PIV Credential is issued only upon request by proper authority. **Assessment** *Determine that:* *(i) the process for making a request is documented (review);* *(ii) A request from a valid authority is made in order to issue a Derived PIV Credential (observe).*	DPCI	FIPS 201-2, Section 2.1 – Control Objectives
	SP(DC)-2	The issuing facility collects personal information using only forms approved by OMB under the Paperwork Reduction Act of 1995. **Assessment** *Determine that*: *(i) forms used to collect personal information have been approved by OMB (review, observe).*	DPCI	OMB Memorandum 07-06

2174
2175

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Identity Proofing (i.e., Derivation) / Registration Process	EI(DC)-1	A Derived PIV Credential is issued following verification of the subscriber's identity using the PIV Authentication key on his or her existing PIV Card by performing: (i) the PIV Authentication certificate is validated as being active and not revoked prior to issuance of a Derived PIV Credential, (ii) the subscriber must demonstrate possession and control of the related PIV Card via the PKI-AUTH authentication mechanism as per section 6.2.3.1 of FIPS 201-2, (iii) the revocation status of the subscriber's PIV Authentication certificate is rechecked seven (7) calendar days following issuance of the Derived PIV Credential. **Assessment** *Determine that:* *(i) the issuer has a documented process in place to verify the identity of the subscriber's identity (review);* *(ii) the issuer's process is compliant with the requirements for initial issuance of Derived PIV Credentials (observe).*	DPCI	SP 800-157, Section 2.1 – Initial Issuance

2176
2177

2178

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Issuance/ Activation Process	AI(DC)-5	At LOA-4, the hardware cryptographic module for the removable or embedded PIV includes a mechanism to block use of the PIV Derived Authentication private key after a number of consecutive failed authentication attempts as stipulated by the organization. **Assessment** *Determine that:* *(i) the hardware-based Derived PIV Credential can block use if the number of consecutive failed attempts has exceeded that set by the issuer (test, observe).*	DPCI – LOA 4 Only	SP 800-157, Section 3.4.1 – Hardware Implementations
	AI(DC)-9	For (removable or embedded) hardware-based implementations of Derived PIV Credentials, subscriber activation is based on a Personal Identification Number (PIN) which meets the requirements for operator authentication as specified in FIPS 140-2. **Assessment** *Determine that:* *(i) Derived PIV Credentials are issued with PIN activation that meets the requirements for operator authentication as specified in FIPS 140-2 (review);* *(ii) the issuer advises applicants that the PIN should not be easily guessable or otherwise individually-identifiable in nature (observe).*	DPCI – LOA 4 Only	SP 800-157, Section 3.4.1 – Hardware Implementations
	AI(DC)-15 (NEW)	For software implementations (LOA-3) of Derived PIV Credentials, a password-based mechanism is used to activate the cryptographic module containing the private key corresponding to the Derived PIV Credential. The password meets the requirements of an LOA-2 memorized secret token as specified in Table 6 of SP 800-63-2. **Assessment** *Determine that:* *(i) the issuer implements a password-based mechanism for activating the private key of the LOA 3 Derived PIV Credential (review);* *(ii) the password advised by the issuer meets the requirements of a LOA-2 memorized secret token (review, observe).*	DPCI – LOA 3 Only	SP 800-157, Section 3.4.2 – Software Implementations

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	AI(DC)-16 (NEW)	If the issuance process involves two or more electronic transactions, the subscriber identifies himself/herself in each new encounter by presenting a temporary secret that was issued in a previous transaction, as described in Section 5.3.1 of SP 800-63-2. **Assessment** *Determine that:* *(i) the issuer implements a process conformant to SP 800-63 when multiple transactions are involved in issuing a Derived PIV Credential at LOA 3 (review, observe).*	DPCI – LOA 3 Only	SP 800-157, Section 2.1 - Initial Issuance
	AI(DC)-17 (NEW)	An LOA-4 Derived PIV Credential is issued in person, in accordance with SP 800-63-2, and the subscriber identifies himself/herself using a biometric sample that can be verified against the subscriber's PIV Card. **Assessment** *Determine that:* *(i) the issuer implements a process conformant to SP 800-63-2 and where a biometric sample of the subscriber is verified prior to issuance of the Derived PIV Credential (review, observe);*	DPCI – LOA 4 Only	SP 800-157, Section 2.1 - Initial Issuance
	AI(DC)-18 (NEW)	If there are two or more transactions during the issuance process of an LOA-4 Derived PIV Credential, the subscriber identifies himself/herself using a biometric sample that can either be verified against the PIV Card or against a biometric that was recorded in a previous transaction. **Assessment** *Determine that:* *(i) the issuer implements a compliant process when multiple transactions are involved in issuing a Derived PIV Credential at LOA4 (review, observe);*	DPCI – LOA 4 Only	SP 800-157, Section 2.1 - Initial Issuance

2179

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
Maintenance Process	MP(DC)-2	If the token corresponding to the Derived PIV Credential is lost, stolen, damaged or compromised, the PIV Derived Authentication certificate is revoked in accordance with the underlying certificate policy. **Assessment** *Determine that:* *(i) in the case of lost, stolen, damaged or compromised credential the issuer has processes in place to revoke the PIV Derived Authentication certificate (review, observe, test)*	DPCI	SP 800-157, Section 2.2 - Maintenance

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
	MP(DC)-5	Upon Derived PIV Credential termination, the organization enforces a standard methodology of updating systems of records to indicate employee termination, and this status is distributed effectively throughout systems used for physical and logical access to organization facilities and resources. **Assessment** *Determine that:* *(i) the issuer has procedures to update information systems and disseminate information to indicate Derived PIV Credential termination (review);* *(ii) the organization's information systems are updated to indicate Derived PIV Credential termination (observe).*	DPCI	Commonly accepted security readiness measures
	MP(DC)-7	The organization has completed a lifecycle walkthrough at one year intervals since the last authorization date, and the results are documented in a report to the DAO. **Assessment** *Determine that*: *(i) the organization has completed a lifecycle walkthrough to cover initial issuance, maintenance and termination processes (interview);* *(ii) a lifecycle walkthrough has been completed at one year intervals since the last authorization date (interview);* *(iii) the results of the issuer lifecycle walkthrough have been documented and reviewed by the DAO (review, interview).*	DPCI	SP 800-79-2, Section 5.4 - Monitoring Phase
	MP(DC)-9 (NEW)	For LOA3 Derived PIV Credentials, the initial issuance process is repeated if the password for the Derived PIV Credential is forgotten. **Assessment** *Determine that:* *(i) the issuer completes the entire initial issuance process when the password is forgotten for LOA 3 Derived PIV Credentials (review, observe).*	DPCI – LOA3 Only	SP 800-157, Section 3.4.2- Software Implementations
	MP(DC)-11 (NEW)	When certificate re-key or modification is performed remotely for an LOA-4 Derived PIV Credential, the following applies: (i) communication between the issuer and the cryptographic module in which the PIV Derived Authentication private key is stored occurs only over mutually authenticated secure sessions between tested and validated cryptographic modules, (ii) data transmitted between the issuer and the cryptographic module in which the PIV Derived Authentication private key is stored is encrypted and contain data integrity checks. **Assessment** *Determine that:* *(i) maintenance of LOA-4 Derived PIV Credentials*	DPCI – LOA 4 Only	SP 800-157, Section 2.2 - Maintenance

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
		issued remotely meet all required security controls to be implemented by the issuer and the issuer information systems (review).		
	MP(DC)-12 (NEW)	When PIN reset is performed in-person at the issuer's facility, or at an unattended kiosk operated by the issuer, it is implemented through one of the following processes: (i) the Subscriber's PIV Card is used to authenticate the Subscriber (via PIV-AUTH mechanism as per section 6.2.3.1 of FIPS 201-2) prior to PIN reset, (ii) a 1:1 biometric match is performed against the biometric sample retained during initial issuance of the Derived PIV Credential. **Assessment** *Determine that:* *(i) the issuer's performs a PIN reset using a conformant process (review, observe).*	DPCI - LOA 4 Only	SP 800-157, Section 3.4.1 - Hardware Implementations
	MP(DC)-13 (NEW)	For remote PIN reset for LOA 4 Derived PIV Credentials, the subscriber's PIV Card is used to authenticate the subscriber (via PIV-AUTH authentication mechanism as per Section 6.2.3.1 of FIPS 201-2) prior to PIN reset. If the reset occurs over a session that is separate from the session over which the PIV-AUTH authentication mechanism was completed, strong linkage (e.g., using a temporary authenticator) is established between the two sessions. The remote PIN reset is completed over a protected session (e.g., using TLS). **Assessment** *Determine that:* *(i) remote PIN resets meet all security requirements to be implemented by the issuer and the issuer information systems (review, observe, test).*	DPCI – LOA 4 Only	SP 800-157, Section 3.4.1 - Hardware Implementations
	MP(DC)-16 (NEW)	Rekey (and reissuance) of Derived PIV Credentials in cases of expiration, loss, damage, or compromise, as well as issuance of a new hardware token is performed in accordance with the initial issuance process. **Assessment** *Determine that:* *(i) the issuer follows their entire initial issuance process while re-keying or re-issuing a Derived PIV Credential (review, observe).*	DPCI	SP 800-157, Section 2.2 - Maintenance
	MP(DC)-17 (NEW)	If the PIV Derived Authentication private key was created and stored on a hardware cryptographic token that does not permit the user to export the private key, then termination of the Derived PIV Credential is performed by collecting and either zeroizing the private key or destroying the token. Otherwise, termination is performed by revoking the PIV Derived Authentication certificate. **Assessment** *Determine that:*	DPCI – LOA 4 Only	SP 800-157, Section 2.3 – Termination

IAT = Processes				
Authorization Focus Area	**Identifier**	**Issuer Control**	**Applicability**	**Source**
		(i) the issuer has developed and follows compliant processes to terminate Derived PIV Credentials (review, observe).		
	MP(DC)-18 (NEW)	The linkage between the Derived PIV Credential and the subscriber's PIV Card is updated when the subscriber obtains a new PIV Card (e.g., the subscriber obtains a replacement PIV Card after compromise of their original PIV Card). **Assessment** *Determine that:* *(i) the issuer has developed procedures for updating the link between the Derived PIV Credentials data and the PIV Card when a new PIV Card is issued (review);* *(ii) The issuer has implemented one or more mechanisms to update the linkage between the Derived PIV Credential and a PIV Card as a result of a new PIV Card issuance (review, observe).*	DPCI	SP 800-157, Section 2.4 – Linkage with PIV Card

2180

2181
2182
2183
2184

APPENDIX H: ASSESSMENT AND AUTHORIZATION TASKS

Phases, Tasks, and Sub-tasks	Person(s) Responsible
Initiation Phase	
Task 1: Preparation	
Subtask 1.1: Confirm that the operations of the issuer have been fully described and documented in an operations plan which fully encompasses the scope of the issuance process (i.e., issuance of PIV Cards and/or PIV Derived Credentials).	OIMO
Subtask 1.2: Confirm that processes conducted by the issuing facility are in accordance with the policies and procedures specified in the operations plan and are documented in Standard Operating Procedures.	OIMO, Issuing Facility Manager
Task 2: Resource Identification	
Subtask 2.1: Identify the Senior Authorizing Official (SAO), Designated Authorizing Official (DAO), Privacy Official (PO), Issuing Facility Managers, Assessor, and other key personnel at the facility level, who are performing identity proofing/registration, card production, activation/issuance and other lifecycle functions.	OIMO
Subtask 2.2: Determine the authorization boundary for the issuer.	OIMO, DAO
Subtask 2.3: Determine the resources and the time needed for the issuer authorization, and prepare for execution of the assessment.	OIMO, DAO
Task 3: Operations Plan Analysis and Acceptance	
Subtask 3.1: Review the list of required issuer controls documented in the operation plan to confirm that they have been implemented properly.	DAO, OIMO
Subtask 3.2: Analyze the operations plan to determine if there are deficiencies in satisfying all the policies, procedures, and other requirements in FIPS 201-2 that could result in a DATO being issued.	DAO, OIMO
Subtask 3.3: Verify that the operations plan is acceptable.	DAO

Phases, Tasks, and Sub-tasks	Person(s) Responsible
Assessment Phase	
Task 4: Issuer Control Assessment	
Subtask 4.1: Review the suggested and select assessment methods for each issuer control in preparation for the assessment; identify controls that are applicable based on whether the organization established a PIV Card Issuer (PCI) and/or Derived PIV Credentials Issuer (DPCI).	Assessor
Subtask 4.2: Assemble all documentation and supporting materials necessary for the assessment of the issuer; if these documents include previous assessments, review the findings and determine if they are applicable to the current assessment.	OIMO, Assessor
Subtask 4.3: Assess the required issuer controls using the prescribed assessment procedures found in Appendix G.	Assessor
Subtask 4.4: Prepare the assessment report.	Assessor
Task 5: Assessment Documentation	
Subtask 5.1: Provide the OIMO with the assessment report.	Assessor
Subtask 5.2: Revise the operations plan (if necessary) and implement its new provisions.	OIMO
Subtask 5.3: Prepare the corrective actions plan (CAP).	OIMO
Subtask 5.4: Assemble the authorization submission package and submit to the DAO.	OIMO
Authorization Phase	
Task 6: Authorization Decision	
Subtask 6.1: Review the authorization decision package to see if it is complete and that all applicable issuer controls have been fully assessed using the designated assessment procedures.	DAO
Subtask 6.2: Determine that the risk to the organization's operations, assets, or potentially affected individuals is acceptable and that the issuer controls have been adequately assessed.	DAO
Subtask 6.3: Share the authorization decision package with an independent party for review and prepare the final authorization decision letter.	DAO

Phases, Tasks, and Sub-tasks		Person(s) Responsible
Task 7: Authorization Documentation		
Subtask 7.1:	Provide copies of the final authorization package, in either paper or electronic form, to the OIMO and any other officials having interests, roles, or responsibilities in the issuing organization.	DAO
Subtask 7.2:	Update the operations plan.	OIMO

Monitoring Phase

Task 8: Operations Plan Update		
Subtask 8.1:	Document all relevant changes to the issuer within the operations plan.	OIMO
Subtask 8.2:	Analyze the proposed or actual changes to the issuer, and determine the impact of such changes.	OIMO
Task 9: Annual Lifecycle Walkthrough		
Subtask 9.1:	Observe all the processes involved in obtaining a PIV Card or a Derived PIV Credential, including those from sponsorship to maintenance. Observe each process, and compare its implementation against the applicable list of required issuer controls. If an issuer has several facilities, this process should be repeated using randomly selected issuing facilities.	OIMO (or designated appointee)
Subtask 9.2:	The results of the lifecycle walkthrough are summarized in a report to the DAO. Deficiencies must be highlighted along with corrective actions that must be implemented to correct any deficiencies.	OIMO, DAO