NIST Special Publication
NIST SP 800-79r3 ipd

Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Sarbari Gupta
Nabil Ghadiali

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-79r3.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-79r3 ipd

Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Sarbari Gupta
Nabil Ghadiali
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-79r3.ipd

December 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. 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.

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication.]

How to Cite this NIST Technical Series Publication:

Ferraiolo H, Regenscheid A, Gupta S, Ghadiali N (2023) Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-79r3 ipd. https://doi.org/10.6028/NIST.SP.800-79r3.ipd

NIST Author ORCID iDs

Hildegard Ferraiolo: 0000-0002-7719-5999
Andrew Regenscheid: 0000-0002-3930-527X
Sarbari Gupta: 0000-0003-1101-0856
Nabil Ghadiali: 0009-0008-0874-3817

Public Comment Period
December 13, 2023 - January 29, 2024

Submit Comments
piv_comments@nist.gov

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

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The document provides 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 the standards published in response to HSPD-12. The reliability of an issuer is of utmost importance when an organization (e.g., a federal agency) is required to trust identity credentials that were created and issued by another organization. This trust relies on having the necessary level of assurance that the reliability of the issuing organization has been established through a formal authorization process.

Keywords

assessment; authorization; compliance; derived PIV credentials; HSPD-12; issuer controls; personal identity verification; PIV Card.

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.

Note to Reviewers

NIST SP 800-79r3 ipd, *Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers*, expands the set of issuer controls to include new and updated requirements from FIPS 201-3, its supporting updated publications (e.g., SP 800-157r1, SP 800-76r2, etc.) and newly-issued OMB Memoranda aimed at achieving compliance with federal requirements with regard to identity proofing and the issuance of a common and reliable form of a primary and derived identity credential.

NIST is specifically interested in comments on and recommendations for the following topics:

1. Are the new and updated controls for identity proofing and the issuance and maintenance of PIV Cards and derived PIV credentials clear and practical to implement?
2. Is it easy to determine where the updated controls need to be implemented (i.e., at the enterprise level, issuing facility level, or both)?
3. Are the new controls for derived PIV credentials sufficient to provide comparable assurance for PIV Cards?

NIST requests that all comments be submitted by 11:59 p.m. Eastern Standard Time (EST) on January 29, 2024. Please submit comments to piv_comments@nist.gov. NIST will review all comments and make them available on the NIST Computer Security Resource Center (CSRC) website. Commenters are encouraged to use the comment template provided on the NIST CSRC website.

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: piv_comments@nist.gov.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors — Hildegard Ferraiolo and Andrew Regenscheid of NIST and Sarbari Gupta and Nabil Ghadiali of Electrosoft Services, Inc. — gratefully acknowledge the contributions of Dennis Branstad, Alicia Clay, Joan Hash, Ramaswamy Chandramouli, Jason Mohler, Dennis Bailey, and Scott Shorter, who co-authored prior versions of this publication. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Executive Summary

Homeland Security Presidential Directive 12 [HSPD-12] established a policy for the creation, issuance, and use of personal identification credentials to identify federal employees and contractors securely and reliably. In response, NIST developed and published FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS201], as well as several NIST Special Publications (SPs) to provide additional specifications and supporting information. Together, these documents provide a foundation for standardizing the processes related to the adoption and use of government-wide personal identification credentials as a means to verify the identities of credential holders. The implementation of PIV specifications involves the collection, protection, and dissemination of personal information, which itself requires privacy protection.

In light of the requirements for both improved security and the protection of personal privacy, [HSPD-12] established four control objectives, one of which includes the call for forms of identification that are "issued by providers whose reliability has been established by an official accreditation process." In response, Appendix A.1 of [FIPS201] specifies that NIST "…develop a new accreditation methodology that is objective, efficient, and will result in consistent and repeatable accreditation decisions…" This led to the development of SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers.*[1]

This update to SP 800-79 reflects the third revision of [FIPS201], which was published in 2022. It provides appropriate and useful guidelines for assessing the reliability of PIV Card issuers and derived PIV credential issuers, which is of utmost importance when an organization (e.g., a federal agency) is required to trust identity credentials that were created and issued by another organization (i.e., another federal agency). This trust only exists if the relying organization has the necessary level of assurance that the credential is established via a formal and reliable authorization process.

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

- Controls derived from specific requirements in [FIPS201] and relevant documents for a PIV Card issuer (PCI) and a derived PIV credential issuer (DPCI)
- Procedures for verifying and monitoring adherence to the requirements through an assessment of the implementation of the controls (i.e., control assessment)
- Guidance for evaluating the result of an assessment in order to arrive at the authorization 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 the commitment of time, energy, and resources are required. These guidelines are designed to assist the organization in creating the needed roles, assigning responsibilities,

[1] SP 800-37-2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP800-37], has deprecated the use of the term "accreditation" in favor of the term "authorization." This is reflected in the title of the present revision.

developing an acceptable operations plan, drawing the issuer's authorization boundary, evaluating the findings of all control assessments, and making a proper authorization decision.

Since organizations may vary significantly in how they choose to structure their operations, these guidelines have been developed to support organizational flexibility and minimize the effort needed to assess, authorize, and monitor the reliability of issuers. The authorization methodology also generates assessment findings and resulting authorization decisions that are consistent and repeatable. These characteristics provide assurance to an organization's management that an issuer who has been authorized based on these guidelines 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 (i.e., federal departments and agencies) and can be applied whether their issuance processes are:

- Centrally located,
- Geographically dispersed, or
- Outsourced in varying degrees to other organizations or service providers.

1. Introduction

Homeland Security Presidential Directive 12 [HSPD-12], *Policy for a Common Identification Standard for Federal Employees and Contractors*, was issued on August 27, 2004, to enhance security, increase Federal Government efficiency, reduce identity fraud, and protect personal privacy. This Directive established a federal policy to create and use secure and reliable forms of identification for federal employees and contractors. It further defined *secure and reliable forms of identification* as those that:

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

NIST developed and published Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors* [FIPS201], and several Special Publications that provide additional specifications in response to [HSPD-12]. These documents provide the foundation for personal identification, verification, and access control systems across the Federal Government.

To standardize the operations of PIV Card issuers, NIST developed a set of attributes to assess reliability and published the first version of SP 800-79 in July of 2005. Lessons learned through various implementation approaches, experience in credential management and PIV Card issuance, and the introduction of mobile device-integrated PIV credentials (i.e., derived PIV credentials) motivated NIST to update the set of issuer controls and associated methodology to ensure that they were objective and efficient and would result in consistent and repeatable authorization decisions. With advancements in technology and the need for flexibility, [FIPS201] expanded the set of derived credentials beyond those that are PKI-based and broadened their use to other types of devices in addition to mobile devices. The technical details for the expanded set of derived PIV credentials is specified in SP 800-157r1, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [SP800-157]. This revision of SP 800-79 (i.e., SP 800-79r3) reflects the updates to [FIPS201], [SP800-157], and other supporting publications.

This document uses the common term "issuer" to refer to issuers of both PIV Cards and derived PIV credentials unless it is necessary to differentiate them. An issuer is considered to be owned, managed, or outsourced (in part or as a whole) by an organization that is a federal department or agency. Ensuring the reliability of an issuer is of critical importance to establishing secure and reliable forms of identification and protecting the privacy of millions of government employees and contractors. Controlling access to physical and logical resources through the use of standard credentials provides assurance that certain predefined levels of security can be achieved. All relying-party organizations must also have confidence in the credentials that it issues to its own employees and contractors as well as those 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 developing assessment and authorization methodologies, most significantly with the widely accepted approach to authorization in SP 800-37r2 [SP800-37] and its family of related documents. While [SP800-37] focuses on the authorization of the security of information systems rather than the authorization of the reliability of an issuer, it offers a practical foundation for the authorization programs envisioned by [HSPD-12]. This document utilizes the various aspects of [SP800-37] and applies them to authorizing the reliability of an issuer. The authorization of an issuer by a federal organization requires prior assessment of the security of all information systems used by that issuer in accordance with [SP800-37]. Since PIV Cards and derived PIV credentials are typically issued through the use of information systems, an assessment of their security (through the methodology in [SP800-37]) is critical for determining the ability to comply with [FIPS201] requirements.

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 [SP800-37] authorization (particularly in implementing security controls) but have little room for variation when it comes to the authorization of an issuer. Much of the flexibility in [SP800-37] 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 for an issuer to be deemed reliable. Allowing too much latitude in how a requirement is met undermines its reliability.

Although organizations may feel constrained by the uniformity required by [FIPS201], standardization greatly contributes to achieving the objectives of [HSPD-12] across issuer implementations. For all federal organizations to accept the PIV Cards and derived PIV credentials of other federal organizations, one set of rules (i.e., [FIPS201]) must be followed by all PIV system participants. This document provides a way to determine whether 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 [FIPS201] and relevant documents as verified through applicable assessment procedures and maintains consistency in their operations with respect to meeting these criteria, they can be considered reliable, as is required by [HSPD-12].

The objectives of this document are to:

- Outline the requirements for PIV Card issuers and derived PIV credentials issuers, including the rationale for the requirements and the assessment procedures for determining 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 meeting all of the control objectives stated in [HSPD-12]
- Emphasize the role of risk associated with an authorization decision based on assessment outcomes that consider 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 or local government, educational institution, non-profit group) that wishes to align with [FIPS201] and associated PIV credentials.

All federal organizations are required to adopt [HSPD-12] and implement [FIPS201]. They must use the methodology and issuer controls outlined in this document to assess the adequacy of their implementations as well as the reliability of the directly controlled and subcontracted services involved in creating and issuing the mandatory PIV Cards and the optional derived PIV credentials (if implemented).

This document is consistent and compatible with the control objectives in [HSPD-12], [FIPS201], [SP800-157], and [SP800-37]. It includes the roles, requirements, definitions, specifications, and procedures needed to assess the reliability of an issuing organization. If an issuer fails to meet the prescribed assessment criteria, they must immediately halt operations.

Once an issuer is authorized to operate using these guidelines, trust can be established in the issued PIV credentials throughout their life cycles.

1.2. Requirements, Notations, and Conventions

This standard uses the following typographical conventions in text:

- Specific terms in CAPITALS represent normative requirements. When these same terms are not in CAPITALS, the term does not represent a normative requirement.
    - The terms “SHALL” and “SHALL NOT” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.
    - The terms “SHOULD” and “SHOULD NOT” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
    - The terms “MAY” and “NEED NOT” indicate a course of action that is permissible within the limits of the publication.
    - The terms “CAN” and “CANNOT” indicate a material, physical, or causal possibility or capability or — in the negative — the absence of that possibility or capability.

1.3. Organization of This Publication

The remainder of this publication is organized as follows:

- Section 2 provides the 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) the definition of the target entities (i.e., issuer, issuer facilities, issuer boundaries); (ii) the relationship between

authorization under [SP800-37] and authorization under this revision of SP 800-79; (iii) preparatory tasks for the assessment of an issuer organization, including the assignment of roles and responsibilities; (iv) two alternative authorization decisions; (v) the acceptance of risk in the authorization decision; and (vi) the contents of the authorization package.

- Section 3 describes the building blocks of the issuer assessment and authorization methodology, including Authorization Topics, Authorization Focus Areas, and the control requirements (i.e., issuer controls) within each area.
- Section 4 provides a detailed description of the assessment methods for the issuer controls whose outcomes form the basis for the authorization decision.
- Section 5 describes the four phases of the authorization process and the tasks involved in each phase.
- The References section lists all of the sources and documents referenced in this publication.
- The Appendices include:
    - Appendix A, Acronyms
    - Appendix B, Glossary
    - Appendix C, Issuer Readiness Review Checklist
    - Appendix D, Operations Plan Templates
    - Appendix E, Assessment Report Template
    - Appendix F, Sample Transmittal and Decision Letters
    - Appendix G, Issuer Controls and Assessment Procedures
    - Appendix H, Assessment and Authorization Tasks
    - Appendix I, Revision History

2. Preparation for Assessment and Authorization

This section presents the fundamentals of an authorization of an issuer, including (i) definitions for an issuer and issuing facility, (ii) outsourcing issuer services or functions, (iii) the differences between an assessment and authorization, (iv) the authorization boundaries of an issuer, (v) roles and responsibilities, (vi) the relationship between authorization under [SP800-37] and this revision of SP 800-79, (vii) preparing for the assessment, (viii) the types of authorization decisions, (xi) the use of risk in authorization decisions, and (x) the contents of the authorization package.

2.1. Organization

An *organization* in the context of this document is a federal department or agency that is responsible for issuing PIV Cards and, optionally, derived PIV credentials to their employees and contractors in accordance with [HSPD-12] and [FIPS201] requirements. An organization SHALL be responsible for maintaining the enterprise identity management system (IDMS) and associated PIV identity accounts for its employees and contractors. The organization SHALL also be responsible for authorizing an issuer (Sec. 2.2) via an authorization to operate (ATO) (Sec. 2.10) prior to issuing PIV credentials.

An organization is responsible for completely describing its PIV credential issuance functions in an operations plan. This comprehensive document incorporates all of the information about the organization that is needed for any independent party to review and assess the capability and reliability of its issuance functions, as implemented by the issuers. An operations plan includes a description of the issuer's structure, its facilities, any external service providers, roles and responsibilities, the policies and procedures that govern its operations, and a description of how the requirements of [FIPS201] are being met. A template for an operations plan is provided in Appendix D.

2.2. Issuer

At the highest level, an *issuer* is considered to be owned by an organization (e.g., federal agency) or a private entity outsourced by the organization to provide PIV credential services. An issuer SHALL provide a full set of functions required to produce, issue, and maintain PIV Cards or derived PIV credentials for the organization. An issuer is considered operational if the organization has relevant roles and responsibilities defined and appointed; suitable policies and compliant procedures have been implemented for all relevant PIV processes,[2] including sponsorship, identity proofing/registration (to include supervised remote identity proofing, if implemented), adjudication, card/token production, activation/issuance, and maintenance; and information system components that are utilized to perform the above-mentioned functions (i.e., processes) have been assessed and shown to meet all technical and operational requirements prescribed in [FIPS201] and related documents.

In order to comply with [HSPD-12], an organization SHALL first establish an issuer to issue PIV Cards or derived PIV credentials that conforms to and satisfies the requirements of [FIPS201]

[2] Some of the processes may not apply to issuers of derived PIV credentials. For example, identity proofing is not required for the issuance of derived PIV credentials since it is a post-enrollment binding process based on the issued PIV Card and identity record previously created.

and related documents. The issuer SHALL then be authorized (i.e., using the guidelines specified in this document). An organization has certain flexibility in implementing its issuance functions, such as outsourcing some of the required processes or establishing multiple units to fulfill these processes. Regardless of its structure, the organization is responsible for the management and oversight of its issuers and SHALL maintain full responsibility as required in [HSPD-12]. Given that the issuer is responsible for issuing PIV credentials on behalf of an organization, the issuer is sometimes referred to as a Credential Service Provider (CSP).

2.3. 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 production, (iii) activation/issuance, and (iv) maintenance, including reissuance. An issuing facility operates under the auspices of a PIV Card or derived PIV credential issuer and implements the policies and 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, etc.), an issuer can have its services and functions provided centrally, distributed across multiple locations, or performed remotely. For example, in the case of PIV Card issuance, a geographically dispersed organization may decide to set up issuing facilities to have identity proofing/registration and activation/issuance functions performed in different parts of the country so that applicants can minimize travel. In this example, the different issuing facilities fall under the purview (i.e., policy and management) of a single issuer that encompasses all of the functions necessary to issue PIV Cards for the organization.

2.4. Outsourcing Issuing Facilities

An organization MAY outsource the issuance of PIV Cards or derived PIV credentials in part or in full. As the complexity and cost of new technologies 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 federal agency, a private entity, or some other organization that offers the services or functions necessary to issue PIV Cards or derived PIV credentials. Regardless of the outsourcing arrangement, the organization is responsible for ensuring that all PIV credential issuance functions are being performed according to the approved processes for issuing an authorization to operate to an issuer (Sec. 2.10).

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, optionally, a derived PIV credential (i.e., via sponsorship, wherein a responsible official of the organization provides the biographic and organizational affiliation of the applicant) and under what conditions the application will be approved (e.g., via adjudication, or the kind of background information that will form the basis for authorization to issue the PIV Card). Therefore, these two functions SHALL NOT be outsourced.

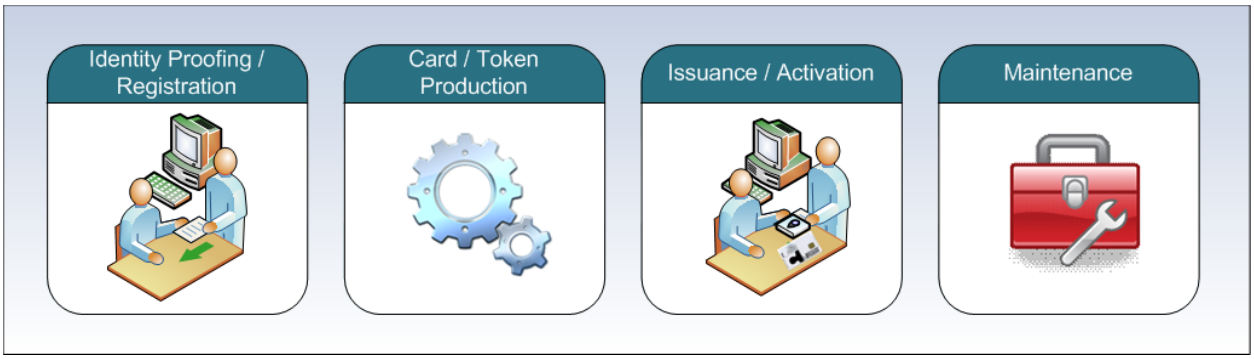


Fig. 1. Outsourcing issuer functions[3]

An organization that outsources services must make sure that all privacy-related requirements are being met both internally and by every external service provider used as part of the PIV credential issuance function.

If an organization is considering using PIV or derived PIV services set up by another organization's issuer, the operations plan and associated documents — including the authorization decision and evidence that the issuer is complying with [FIPS201] requirements — SHALL be reviewed by the designated authorizing official (DAO) of the organization requesting these services. Similarly, if an issuer is selectively using the services of an external service provider for one or more of its processes, the provider's capability to meet [FIPS201] requirements for those processes SHALL be reviewed as well. In both cases, the information gathered as part of this review activity SHALL be included in the issuer's assessment leading to authorization. Outsourced functions SHALL be assessed prior to the authorization of an issuer.

2.5. Assessment and Authorization

[HSPD-12] requires identification credentials to 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 closely related, they are two distinct activities.

Assessment occurs before authorization and is the process of gathering evidence regarding an issuer's satisfaction of the requirements of [FIPS201], including all functions performed (i) locally, (ii) at a supervised remote identity proofing (SRIP) station (if used), or (iii) at issuing facilities. Assessment activities include interviews with the issuer, the issuing facility's personnel, and the SRIP live operators; a review of documentation; an observation of processes; and an execution of tests to determine the 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.

Authorization is the decision to permit the operation of the issuer once it has been established that the requirements of [FIPS201] have been met and the risks regarding security and privacy are acceptable. The individual making the authorization decision SHALL be knowledgeable of

[3] The term "token" refers to a derived PIV credential in physical form, as detailed in [SP800-157].

[HSPD-12] and aware of the potential risks to the organization's operations, assets, and personnel (e.g., applicants, operation staff).

The assessment (Sec. 5.2) and the authorization (Sec. 5.3) are both carried out by the organization that "owns" (i.e., manages, controls, or contracts) the issuance of PIV Cards and/or derived PIV credentials.[4] 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 [FIPS201] and, optionally, [SP800-157] (in the case of derived PIV credential issuance) in a 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 the services and functions at the issuer, its facilities, and/or SRIP stations (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? Have current and potential impacts on security and privacy been highlighted? Have the recommendations and timelines for correction or mediation been included in the assessment report?

2.6. Authorization Boundary of the Issuer

The organization's first step is to identify the appropriate authorization boundary of the issuer. The authorization boundary defines the specific operations that are to be the target of the assessment and authorization. A PIV Card issuer (PCI) comprises the complete set of functions required for the issuance and maintenance of PIV Cards, while a derived PIV credential issuer (DPCI) comprises the complete set of functions required for the issuance and maintenance of derived PIV credentials. In determining the authorization boundary, the organization SHALL consider whether all of the necessary functions required for the issuance and maintenance of PIV Card or derived PIV credentials are included within the scope. The organization SHALL also consider whether these functions are being performed identically in all issuing facilities, are using identical information technology components, and are under the same direct management control. For example, 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, and each assessment would result in an independent authorization decision.

In drawing an authorization boundary, an organization MAY only want to include a subset of its issuing facilities. For example, if an issuer 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 only those issuing facilities that are ready to be assessed. If the authorization is successful, the organization would authorize the issuer along with its subset of issuing facilities to operate and begin issuing PIV Cards. The remaining issuing

[4] The trust in PIV Cards and derived PIV credentials stems from the guidelines in Task 6 of Sec. 5.3.

facilities can continue with implementation and be included in the authorization boundary at a later date.

In the case of outsourcing PIV or derived PIV services that are not under direct management control of the organization nor physically located within its facilities, the organization SHALL include the functions provided by any external service providers within the authorization boundary to ensure that they are included within the scope of issuer 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. From an issuer point of view, this translates to applying the necessary due diligence process with respect to the assessment of controls to ensure that outsourced functions are conducted in an acceptable and compliant manner.

Care should be used in defining the authorization boundary for the issuer. A boundary that is unnecessarily expansive (i.e., includes many dissimilar processes and business functions) makes the assessment and authorization processes extremely complex. Establishing a boundary and its subsequent authorization are organization-level activities that SHOULD include the participation of all key personnel. An organization SHOULD strive to define the authorization boundary of its issuers 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 their flexibility in establishing a practical boundary that promotes an effective [HSPD-12]-compliant implementation. The scope of an authorization is an issuer whose boundaries are formed by included issuing facilities, not individual issuing facilities.

2.7. Issuer Roles and Responsibilities

PIV Card and derived PIV credential issuance roles and their processes should be selected based on the organization's structure, its mission, and operating environment. The organization SHALL make sure that a separation of roles has been established and that the processes follow the requirements of [FIPS201].

This subsection identifies the roles and responsibilities of key personnel involved in the setup, day-to-day operations, assessment, and authorization of an issuer.[5] 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).

2.7.1. Senior Authorizing Official (SAO)

The senior authorizing official (SAO) 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 related to the issuance of PIV Cards and derived PIV credentials for the organization.

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

2.7.2. Designated Authorizing Official (DAO)

The designated authorizing official (DAO) has the authority within an organization to review the assessment results of the organization's established issuers and related issuing facilities and to provide an authorization decision as required by [HSPD-12]. Through authorization, the DAO accepts responsibility for the operation of the issuers at an acceptable level of risk and attests that the organization is issuing PIV Cards and, optionally, derived PIV credentials in accordance with the requirements of [FIPS201] such that issued PIV credentials have the commensurate level of identity assurance. The SAO may also fulfill the role of the DAO. The DAO SHALL NOT assume the role of the EIMO.

2.7.3. Enterprise Identity Management Official (EIMO)

The organization's enterprise identity management official (EIMO) is responsible for implementing the policies of the organization and ensuring that all identity-proofing, card/token production, issuance, and maintenance processes are being performed reliably, consistently, securely, and in compliance with [FIPS201] and, optionally, [SP800-157] (in the case of derived PIV credentials) by the issuer. The EIMO is responsible for the organization's identity management system and the enrolled PIV identity accounts. The EIMO ensures that the PIV identity account remains current at all times and that all issued PIV credentials are represented within this PIV identity account for the cardholder.

Furthermore, the organization's EIMO implements and manages the operations plan; ensures that all issuing facility roles are filled with capable, trustworthy, knowledgeable, and trained staff; ensures that all services, equipment, and processes meet [FIPS201] requirements; monitors and coordinates activities with issuing facility managers; provides guidance to the issuing facilities and SRIP operators as needed; and supports the authorization process.

2.7.4. Issuing Facility Manager

An issuing facility manager manages the day-to-day operations of an issuing facility, remote SIRP center, or SIRP station. 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 ensures that all PIV processes adhere to the requirements of [FIPS201] and that all PIV and derived 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 direction of the organization's EIMO. In some cases (e.g., small organizations), the EIMO MAY fulfill the role of the issuing facility manager.

2.7.5. Operator

An operator is responsible for executing all operating procedures for all functions, whether in-person or remotely observed (e.g., identity proofing, registration, issuance of the PIV Card or post-enrollment binding of a derived PIV credential, etc.) All operators SHALL receive comprehensive training to perform their assigned responsibilities, detect fraudulent identity source documents, and properly capture biometrics when needed. Multiple operators CAN be assigned to an issuing facility, depending on the size of that facility. The issuer is responsible for

ensuring that all identity proofing, registration, card/token production, issuance, post-enrollment binding, and reissuance processes are carried out and adhere to the principle of separation of duties wherever necessary to comply with [HSPD-12] and [FIPS201].

2.7.6. Assessor

The assessor is responsible for performing a comprehensive, third-party assessment of an issuer. The assessor (usually supported by an assessment team) verifies that the issuer's PIV processes comply with the control objectives of [FIPS201]. The EIMO reviews the assessment findings and prepares recommended corrective actions to reduce or eliminate any discrepancies or shortcomings prior to submission to the DAO for an authorization decision. The assessor is also responsible for providing recommendations for reducing or eliminating deficiencies and security weaknesses and describing the potential impacts if those deficiencies are 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 SHALL be a third-party that is independent of the offices and personnel that are directly responsible for the day-to-day operation of the issuer. The assessor SHALL also be independent of those individuals responsible for correcting the deficiencies and discrepancies identified during the assessment phase. The independence of the assessor is important for maintaining the credibility of the assessment results and ensuring that the DAO receives objective information in order to make an informed authorization decision.

2.7.7. Applicant Representative (AR)

The applicant representative (AR) is an optional role that 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 a PIV Card or derived PIV credential. ARs are responsible for assisting an applicant who is denied a PIV credential because of missing or incorrect information and for ensuring that all applicants obtain useful information and assistance when needed. This role is typically assigned to someone in the organization's personnel or human resources office.

2.7.8. Privacy Official (PO)

The responsibilities of the privacy official (PO) are defined in [FIPS201]. The person filling this role SHALL not assume any other operational role within the organization. The PO issues policy guidelines with respect to the collection and handling of personally identifiable information from applicants to ensure that the issuer complies 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., Senior Agency Official for Privacy or Chief Privacy Officer).

2.7.9. Role Assignment Policies

Although organizational 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 the assessor and PO and the separation of duty

provision under Sec. 2.7.2, one person MAY perform more than one role if needed. If an organization has established multiple issuers, an individual MAY be assigned the same role in several or all of them. For example, an issuing facility manager MAY be responsible for a number of issuing facilities. Of the roles described, the SAO, DAO, EIMO, AR, assessor, and PO SHALL be employees of the organization that owns the PCI or DPCI (e.g., federal employees.)

2.7.10. Assessment and Authorization Roles

Figure 2 illustrates a possible role structure when an issuer has multiple issuing facilities.

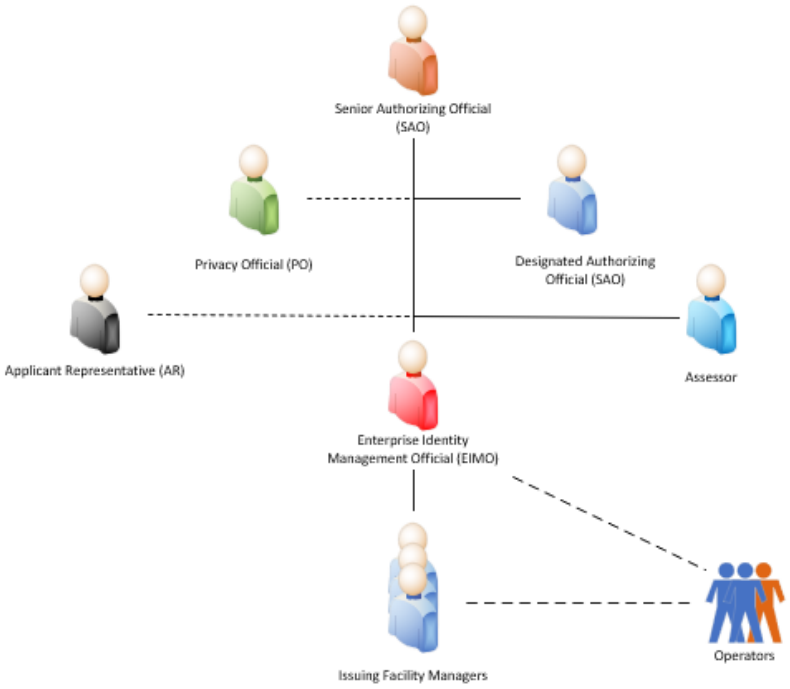


Fig. 2. Issuer assessment and authorization roles

The SAO has the primary authority and responsibility for the organization. The EIMO and the DAO report to the SAO. An issuing facility manager is responsible for managing operations at each issuing facility and reports to the EIMO. The dotted lines leading to the PO and the assessor indicate their independence from the day-to-day operations of the issuer. Depending on the structure of the PCI or DPCI, operators MAY work at the issuing facilities under the supervision and guidance of the issuing facility manager or MAY report directly to the EIMO.

2.8. Relationship Between SP 800-79 and SP 800-37

While authorization is the major topic of both SP 800-79 and [SP800-37], the goals of authorization are different in each. Authorization compliant with [SP800-37], as mandated by Appendix III of the Office of Management and Budget (OMB) Circular A-130, focuses on authorizing the processing of information systems based on an assessment of security at the information system level. An authorization decision granted under [SP800-37] signifies that an organization official accepts responsibility for the security (i.e., the confidentiality, integrity, and

availability of the information) of the information system. Authorization in SP 800-79 and as mandated by [HSPD-12] is concerned with the assessment of the "reliability" of an issuer to perform its functions in accordance with [FIPS201]. The authorization of an issuer's reliability under SP 800-79 indicates that an organization official asserts that the issuer meets and has the ability to 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 (i.e., the authorizing official [AO] in [SP800-37] and the DAO in SP 800-79) is fully accountable for any adverse impacts to the organization if a breach in security, privacy, or policy occurs.

SP 800-79 focuses on the authorization of an organization's capability and reliability but depends on adequate security for all of the supporting information systems that have been authorized under [SP800-37]. Therefore, before the DAO authorizes the issuer and its facilities, all relevant PCI or DPCI information systems used must be authorized. In many cases, authorization under [SP800-37] will be granted by an organization official other than the official responsible for authorizing the issuer. The former is an organization official tasked with deciding whether to authorize the operation of an information system based on its security posture. The latter SHALL be someone specifically designated to authorize the operation of an issuer after it has been assessed and determined to be compliant with [FIPS201] control objectives.

2.9. 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 operation staff, 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.

2.9.1. Issuer Duties

Before the assessment can begin, an assessor SHALL be designated. The assessor conducts the assessment and oversees the assessment team. The assessment team MAY be made up of employees from the organization or personnel from a public or private-sector entity contracted to provide assessment services. Members of the assessment team should have capabilities 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 SHALL be made up of individuals who 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.

Once an assessment team is in place, the EIMO and other relevant personnel SHOULD begin the preparation for the assessment. Thorough preparations by both the issuer 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 for the assessment team to interview all issuer personnel. Personnel, operators, and officials SHALL be notified of the pending

assessment, SHOULD understand their roles in the process, and SHALL be made available in accordance with the planned assessment schedule.

The EIMO SHALL ensure that all relevant documentation has been completed and organized before the assessment begins. This documentation includes policies, procedures, organizational structure, information system architecture, product and vendor details, and specifics regarding the implementation of all of the requirements in [FIPS201] and related publications. If the issuer has outsourced functions to an external service provider, all necessary documentation SHALL be obtained from the provider regarding the outsourced operations. The EIMO SHALL review any documentation to make certain that it is complete, current, and approved before providing it to the assessment team.

Another significant activity during the assessment involves the assessment team observing the actual processes performed by the issuer staff. In order for the assessment team to confirm that processes are implemented in accordance with the operations plan, the issuer organization SHALL 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.

Appendix C includes an issuer readiness review checklist to aid the issuer's planning and preparation for the assessment. Satisfying the list of items before the assessment commences will facilitate efficient utilization of the assessment team's time and contribute toward the overall effectiveness of the assessment activity.

2.9.2. Assessment Team Duties

The independence of the assessment team is important for 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 SHALL NOT be involved in the development, day-to-day maintenance, or 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 may not want to publicly disclose. The assessment team is obligated to store and protect the confidentiality of all security assessment-related records and information, including limiting access to individuals who need to know the information. When using, storing, and transmitting information related to the assessment, the assessment team shall follow any established guidelines as agreed upon under the rules of engagement in addition to all relevant laws, regulations, and standards regarding the need, protection, and privacy of information.

2.10. Authorization Decision

An authorization decision is a judgment made by the DAO to authorize the operation of an issuer and its facilities. The DAO reviews the results of the assessment, considers the impacts of any identified deficiencies on the organization, and 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 (if any) of issuing and maintaining PIV Cards or derived PIV credentials.

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

An authorization decision by a DAO SHALL always be granted for a specific issuer before the commencement of operations, and there can only be one authorization decision for each issuer. In issuing this decision, the DAO SHALL 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 of its authorized issuing facilities to begin operations while remaining facilities focus on addressing the deficiencies identified during the assessment. At a later date, these facilities can be reassessed. After reviewing the new findings, the DAO can reissue the authorization for the issuer and expand the authorization boundary by including the newly assessed facilities.

The major input to the authorization decision is the assessment report. To ensure that the assessment report is properly interpreted and the justification for the authorization decision properly communicated, the DAO SHOULD meet with the assessor, the EIMO, and the issuing facility managers 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:

1. Authorization to operate,
2. Interim authorization to operate, or
3. Denial of authorization to operate.

2.10.1. Authorization to Operate (ATO)

An *authorization to operate* (ATO) may be issued[6] if — after reviewing the results of the assessment phase — the DAO deems that the operations of the issuer and its facilities conform to the control objectives of [FIPS201] to an acceptable degree and will continue to do so reliably during the authorization validity period. The issuer and its issuing facilities are authorized to perform services in compliance with all relevant policies, in conformance with all relevant standards, and in 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 EIMO.

After receiving an ATO that conforms to SP 800-79, reauthorization SHALL be performed (i) within three years; (ii) when there is a significant change in personnel or operating procedures, including the improvement or degradation of operations; or (iii) when additional issuing facilities are being added to the issuer. There may also be cases in which one or more issuing facilities cease operation. If this situation results in a PIV Card or derived PIV credential issuance-related

[6] The issuer ATO can be affected by the underlying system authorization status (see Sec. 2.10.4).

function identified in the operations plan becoming unavailable, then the DAO SHALL issue a denial of authorization to operate (DATO) (Sec. 2.10.3). However, if the issuer can continue to provide all of the services in the operations plan, then the authorization decision letter SHALL be modified to exclude those issuing facilities that have ceased operations, thus revising the authorization boundary. The required reauthorization activities are at the discretion of the DAO and based on the extent and type of change.

2.10.2. Interim Authorization to Operate (IATO)

An interim authorization is an authorization to operate under specific terms and conditions. An *interim authorization to operate* (IATO) SHOULD be issued[7] 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 IATO is rendered to an issuer when the identified deficiencies are significant but can be addressed and remediated in a timely manner. The deficiencies SHALL be documented so that they can be addressed during the planning of corrective actions. The DAO SHALL indicate exactly which facilities are included in the IATO authorization decision during this interim period, along with any limitations or restrictions. The maximum duration of an IATO is three months, and a maximum of two consecutive IATOs MAY be granted. Failure to correct deficiencies before the expiration of the second IATO SHALL result in an issuance of a DATO for the issuer. The authorization boundary SHOULD be revised to exclude issuing facilities that exhibit significant deficiencies in performing their functions. The IATO is transmitted to the EIMO.

An issuer SHALL NOT be considered to be 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.

2.10.3. Denial of Authorization to Operate (DATO)

A *denial of authorization to operate* (DATO) SHALL be transmitted to the EIMO if — after reviewing the results of the assessment phase — the DAO deems operation of the issuer to be unacceptable. Failure to receive an ATO indicates that there are major deficiencies in reliably meeting the requirements of [FIPS201] and its related documents. The issuer is not authorized and SHALL NOT be allowed to operate. If issuance services are currently in operation, all functions SHALL be halted, including all operations at any issuing facility. If an issuer was previously authorized and had issued PIV Cards or derived PIV credentials under an ATO, the EIMO and issuing facility managers SHOULD consider whether a revocation of PIV Cards and derived PIV credentials is necessary. The DAO and the assessor SHOULD work with the EIMO and issuing facility managers to ensure that proactive measures are taken to correct the deficiencies.

[7] The issuer IATO can be affected by the underlying system authorization status (see Sec. 2.10.4).

2.10.4. Authorization Impact of Information Systems Under SP 800-37

An issuer SHALL NOT be authorized to operate if one or more of its critical information systems is deemed insecure and it is therefore issued a DATO according to [SP800-37]. If an IATO has been issued for an information system, the DAO MAY NOT issue greater than an IATO for the issuer. Once the [SP800-37] IATO is replaced with an [SP800-37] ATO, the DAO can issue an SP 800-79 ATO. If the [SP800-37] ATO expires for one or more information systems during the course of operation of an issuer, the EIMO SHALL assess the criticality of the system for operations and present the analysis to the DAO. The DAO can then exercise the following options:

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

2.11. Use of Risk in the Authorization Decision

Authorization is the official management decision by the DAO to permit the 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 impacts to the organization or any other organization from the use of issued PIV Cards or derived PIV credentials.

The assessment of an issuer enables the DAO to determine its reliability and whether to accept the risk to the organization in granting an ATO. As the requirements in [FIPS201] 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.

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 alternative form factors greatly improve the usability of electronic authentication to remote IT resources while maintaining identity assurance through post-enrollment binding. The incorrect or inconsistent implementation of an [HSPD-12] program exposes an organization to an unacceptable level of risk since any problem with an issued PIV Card or derived PIV credential that undermines this assurance could allow unauthorized access to sensitive organizational resources and expose an organization to harm. Furthermore, the collection, processing, and dissemination of personal information is required to issue these credentials and increases the threat of this information being used for malicious purposes[8] 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 that allows 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 federal organization becomes the source of trust for another organization to grant access to physical and

[8] The collection of personally identifiable information (PII) is minimized for derived PIV credentials because of the derivation process.

logical resources based on verification of that identity. The DAO's signature on the authorization letter thus signifies their acceptance of responsibility (i.e., accountability) for the operations of the issuer for their organization as well as other organizations in the federated circle of trust.

2.12. Authorization Submission Package and Supporting Documentation

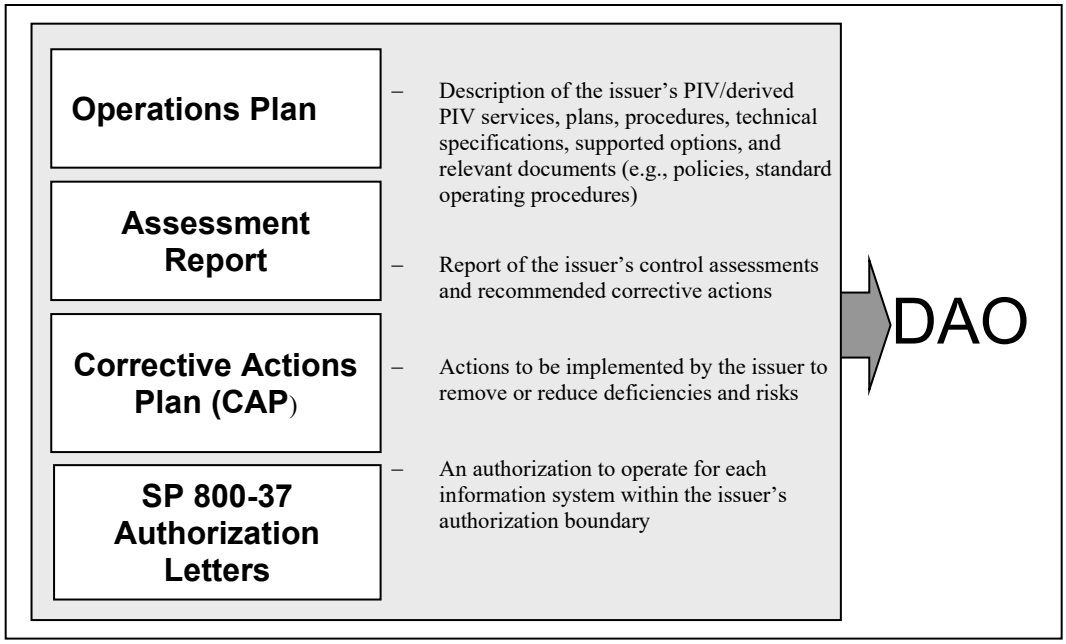
The *authorization submission package* documents the results of the assessment phase and provides the DAO with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the issuer. Unless specifically designated otherwise by the DAO, the EIMO SHALL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

- Operations plan, including standard operating procedures (SOPs) and attachments for all issuing facilities
- [SP800-37] authorization letters
- Assessment report
- Corrective actions plan (CAP), if required

The operations plan contains the policies, procedures, and processes for all of the major PIV functional areas. It gives the assessor and DAO a complete picture of the structure, management, and operations of an issuer, including issuing facilities. Appendix D provides templates of what to include in the operations plan. One of the most significant pieces of information contained in the operations plan is the list of issuer controls, which enables the assessor to quickly ascertain how they are implemented and by whom.

If certain functions described in the operations plan are outsourced, the operations plan SHOULD reference or point to the external service provider's operations plan and related documentation, such as support agreements and any contracts. In this manner, the assessor has access to information about the external service provider's operations without requiring the issuer to duplicate documentation. Upon receiving and reviewing the authorization package and in consultation with the assessor, the DAO decides whether to authorize the operations of the issuer. The authorization decision letter transmits the authorization decision from the DAO to the EIMO and contains the following information:

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



991

Fig. 3. Authorization submission package

992

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

1000 The DAO sends the authorization decision package to the EIMO and retains a copy of it. The
1001 EIMO carefully reviews the terms and conditions of authorization before initiating the necessary
1002 steps for issuer operations. Both parties mark the authorization decision package appropriately
1003 for storage under the organization's record retention policy.

3. Taxonomy of Issuer Controls

3.1. Introducing Issuer Controls

The assessment of a PCI or DPCI is broader than an assessment of the security of an information system under [SP800-37]. The requirements specified in [FIPS201] cover all major aspects of an issuer, including organizational preparedness, security management, data protection, infrastructure, and issuance processes. In this document, each broad area is defined as an *issuer authorization topic* (IAT). IATs are used to summarize the assessment results for reporting and to structure the report for senior organization management to provide an analysis of the strengths and weaknesses of an issuer and its level of compliance.

IATs include the following:

- **Organizational preparedness** relates to the capability, knowledge, and understanding of senior management regarding the formation and operation of the issuer. Under this area, roles and responsibilities are clearly identified, and policies and procedures are defined, documented, implemented, and enforced.
- **Security management and 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** represent the activities required to procure, deploy, and maintain the information system components used for the issuance of PIV Cards and derived PIV credentials. These information system components (e.g., PKI, card or token personalization, printers, tokens, etc.) must meet the technical specifications defined in [FIPS201] and related documents and must be authorized under [SP800-37] for FISMA compliance.
- **Processes** are classes of functions that collectively span the entire life cycle,[9] such as sponsorship, identity proofing/registration, adjudication, card/token production, activation/issuance, and maintenance of the PIV Card and derived PIV credential.

Each IAT is subdivided 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, there is a procedure or technical product (termed an "issuer control") that is used to satisfy a particular requirement. However, the manner in which the requirements are satisfied and how the specifications are implemented and managed may vary from organization to organization. For example, each PCI is required to identity-proof their applicants. This process can be implemented in one of several ways, depending on the structure, size, and geographical distribution of the organization's headquarters and remote locations. The process could be conducted at a central location or distributed in regional centers across the country. It could be operated directly by the organization or by an external service provider. However, irrespective of the implementation approach, this identity proofing/registration activity needs to be reliably and accurately performed.

[9] Some of the processes may not apply to derived PIV credential issuers.

Issuers need to implement the PIV requirements derived from [FIPS201] and its supporting publications, Office of Personnel Management (OPM) requirements related to background investigations, and applicable OMB Memoranda. The capability of an issuer is determined through the verification of these requirements using appropriate assessments. However, authorization is generally based on both the demonstration of capability and 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, the 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 (e.g., insider attacks) and risks (e.g., physical security lapses). In addition to the controls provided herein, an organization may develop additional mission-specific controls that will contribute toward the overall reliability of the issuer to meet the organization's mission needs.

Table 1 lists the four IATs with associated authorization focus areas under each topic.

Table 1. IATs and associated authorization focus areas

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

Appendices G.1 and G.2 contain required issuer controls grouped by IAT and the associated authorization focus area for PCIs and DPCIs, respectively. Each issuer control represents how one or more requirements from [FIPS201] 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 that are applicable to both PCIs and DPCIs are aligned for ease of reference. In addition, controls for DPCIs are marked with "derived credential (DC)" for quick identification. For example, DO-1 applies to a PCI, and DO(DC)-1 applies to a DPCI. Both of these issuer controls are targeted at assessing the same requirement.

Table 2 shows the "Preparation and Maintenance of Documentation" authorization focus area under the "Organizational Preparedness" IAT.

1075 **Table 2.** Sample IAT, authorization focus area, and issuer controls (PCI)

Identifier	Issuer Control	Source
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.	SP 800-79, Sec. 2.12 – Authorization Submission 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 (or equivalent) of the federal department or agency.	[FIPS201], Sec 2.7 – PIV Identity Proofing and Registration Requirements

1076 Unlike for a PIV Card issuer, not all issuer controls are applicable to a derived PIV credential
1077 issuer. Certain issuer controls are applicable to only Authentication Assurance Level 2 (AAL2)
1078 or AAL3 derived PIV credentials and must therefore be implemented by the issuer only if they
1079 are issuing a derived PIV credential at that level of authentication assurance. This is represented
1080 via the "applicability" column in the tables in Appendix G.2. **Table 3** shows the "Maintenance
1081 Process" authorization focus area under the "Processes" IAT. The "applicability" column
1082 identifies whether the issuer control needs to be met by a PKI-based AAL2 or AAL3 derived
1083 PIV credential issuer or a non-PKI-based AAL2 or AAL3 derived PIV credential issuer. If the
1084 "applicability" column states "DPCI," then the issuer control is applicable to all derived
1085 credential issuers, regardless of what type of derived PIV credential is issued by the issuer.

1086 **Table 3.** Sample IAT, authorization focus area, issuer control, and applicability (DPCI)

Identifier	Issuer Control	Applicability	Source
MP(DC)-17	If the derived PIV authentication private key was created and stored on a hardware cryptographic token that permits export of the private key, then the derived PIV authentication certificate is revoked upon termination, even if the token is collected and either zeroized or destroyed.	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 2.4.1 – PKI-Based Derived PIV Credential Invalidation

1087 All issuer controls apply, regardless of an individual system's FIPS 199, *Standards for Security*
1088 *Categorization of Federal Information and Information Systems* [FIPS199], impact level.
1089 Furthermore, nothing precludes an issuer from implementing additional controls to ensure a
1090 higher level of confidence in mitigating risks associated with issuing PIV Cards or derived PIV
1091 credentials.

1092 3.2. Implementing Issuer Controls

1093 Each issuer control SHALL be properly implemented, managed, and monitored in order for the
1094 issuer to be authorized. Depending on how an organization decides to implement its [HSPD-12]
1095 program, certain functions might be outsourced to external service providers. However, it is still
1096 the responsibility of the organization's management to ensure that the issuer controls are being
1097 implemented, enforced, and maintained by the issuer, its service providers (if any), and all
1098 issuing facilities that are within scope of the authorization boundary.

3.2.1. Issuer Controls Implemented at the Organizational or Facility Level

The nature of each issuer control dictates where it is implemented. Controls are generally considered organizational level controls if they apply to the entire organization, regardless of the structure of the issuer and its issuing facilities, or are common to or impact multiple PIV processes. The development of the operations plan is an example of an issuer control implemented at the organizational level. Generally, controls that are specific to a process are implemented at the issuing facility where that process or function is carried out. For example, the control that states, "The issuer advises applicants that the PIN on the PIV Card should not be easily guessable or otherwise individually identifiable in nature," is implemented at an activation/issuance facility.

Derived PIV credentials MAY be issued remotely. In such cases, the issuer MAY NOT need to use an issuing facility, and issuing facility-specific controls may not be applicable. Regardless of the system and process architecture on how PIV Cards and derived PIV credentials are issued, it is the responsibility of the issuer organization to ensure that all applicable controls are implemented.

4. Issuer Controls Assessment and the Authorization Decision Process

An assessment is a set of activities performed by the assessor to gain assurance that the applicable issuer controls for a PCI or 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 for determining the risk to the organization's overall mission and forms the basis for the authorization decision by the DAO.

An assessor SHALL (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 [FIPS201] and related documents. The objective for the assessor is to use the assessment procedures associated with each issuer control (described in Appendix G) 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:

1. Determine 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.
2. Review the operations plan to determine which issuer controls are implemented at the organizational level and 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.

If 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 responsibility of the EIMO to collect any service provider's documentation and make it available to the assessor. It is recommended that organizations include appropriate language in contractual agreements with external service providers to ensure that the relevant documentation and necessary evidence is furnished by the provider in a timely manner for a successful authorization. If results from a previous assessment of the service provider (provided that the current assessment is part of reauthorization after substantial changes) can be referenced, the assessor may elect to incorporate these results (not exceeding one year) or redo part or all of the assessment. Reusing 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 they span the entire issuer and its issuing facilities. In other words, these controls MAY NOT need to be reassessed when the authorization boundary changes (e.g., due to the 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 need to be reviewed at the issuing facility level even if they are put in place at the organizational 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, it must be reviewed when new information systems in the existing facilities or new facilities are added to ensure that the new systems are brought within the scope of the plan.

Unlike organizational-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). For example, if there are multiple facilities for identity proofing/registration (e.g., multiple registration centers), assessment of the issuer controls under the identity proofing/registration focus area should take place in each of the registration centers. However, if all facilities are operating using uniform operational procedures and underlying information systems, assessments may be performed 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 and technology, and turnover among employees and contractors. Any significant changes in one or more of these factors SHOULD trigger a new assessment. The assessor SHALL 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 the EIMO 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 since security and reliability depend on many factors, including an individual's training, knowledge, motivation, experience, and management. Relying on humans rather than automated security mechanisms for data protection makes it critical that trust and reliability assessments of management, operators, and maintenance personnel are current and up to date. Many 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. The assessor SHOULD NOT rely solely on documentation to determine whether 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:[10]

- *Review* — An evaluation of documentation that describes plans, policies, and procedures in order to verify that they are adequate, understood by management and operations

[10] The assessment methods associated with an assessment procedure are given in parenthesis in Appendices G.1 and G.2.

personnel, and 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 preestablished 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 of the information system components of the issuer involved in the 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 procedures in Appendices 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 whether 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 the "Preparation and Maintenance of Documentation" authorization focus area under the "Organizational Preparedness" IAT. The "applicability" column identifies whether the issuer control needs to be met by a PKI-based AAL2 or AAL3 derived PIV credential issuer or a non-PKI AAL2 or AAL3 derived PIV credential issuer. If the "applicability" column states "DPCI," then the issuer control is applicable to all derived PIV credential issuers, regardless of what type of derived PIV credential is issued by the issuer.

Table 4. Sample issuer controls with assessment procedures (DPCI)

Identifier	Issuer Control	Applicability	Source
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 (i) the list of issuer controls from Appendix G, (ii) the owner for each owner, (iii) a description of how the control is implemented, and (iv) whether the control is organization or facility-specific (review).* *(iii) Relevant operating procedures and associated documentation are referenced accurately (review).* *(iv) The operations plan has been reviewed and approved by the DAO within the organization (review, interview).*	DPCI	SP 800-79, Sec. 2.12 – 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 (to include in-person, remote, or both) (review).*	DPCI	[SP800-157], Sec. 2 – Life Cycle Activities and Related Requirements [SP800-157], Sec. 2.2 – Initial Issuance

Identifier	Issuer Control	Applicability	Source
	(ii) The policy is consistent with the organization's mission and functions, [FIPS201], [SP800-157], *and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The policy and procedures are approved by the federal department or agency (review).* *(iv) The organization periodically reviews and updates the policy and procedures as required (review, interview).*		

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 or augmented to ensure proper implementation of the controls.

4.2. Issuer Assessment Report

The assessment report contains the results of the assessment in a format that facilitates reviewing by the DAO. The DAO SHALL 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.

Appendix E provides an assessment report template organized by authorization focus. For each issuer control, it SHALL document which entity is responsible for the implementation of that control (e.g., the organization or an external service provider) and whether 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 operator performs a one-to-one comparison of the applicant against the biometric data records available on the PIV Card or in the PIV enrollment record. If the biometric verification decision is negative, or if no biometric data records are available, the cardholder provides two identity source documents (as specified in [FIPS201], Sec. 2.7), which are inspected and compared by the operator with the photograph 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 one-to-one comparison of the applicant against the biometric data records available on the PIV Card or in the PIV enrollment record 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 a biometric match is unsuccessful 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 the biometric match is not successful.

Fig. 4. Sample issuer control assessment result (PCI)

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 their conclusion in one of two ways: MET or NOT MET. Using the list of conclusions pertaining to the assessment procedures associated with an issuer control, the assessment result (i.e., one of the four 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 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). **Figure 4** shows an example of an assessment that resulted in "Partially Satisfied." 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.

When drawing a conclusion after 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. Assessment and Authorization Life Cycle

The authorization of a PCI or DPCI consists of four phases: (i) Initiation, (ii) Assessment, (iii) Authorization, and (iv) Monitoring. Each phase consists of tasks and subtasks to be carried out by the responsible officials (e.g., the DAO, assessor, EIMO, and issuing facility managers). **Figure 5** provides a view of the authorization phases, including the tasks associated with each phase. A table of authorization phases, tasks, subtasks, and the official responsible for each is provided in Appendix H.

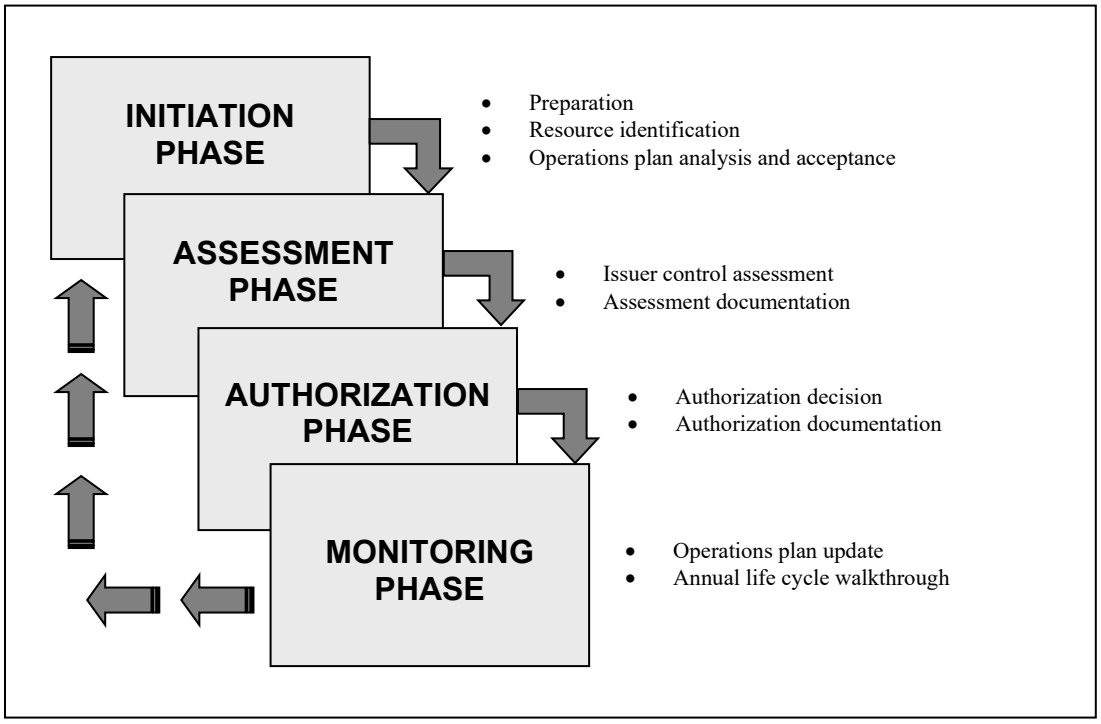


Fig. 5. Assessment and authorization life cycle phases

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 resources and documentation in place. The other purpose of this phase is to include the DAO early in the process to ensure the 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 confirm that the plan is consistent with [FIPS201] and the template provided in Appendix D.

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

Responsibility: EIMO

Guidance: The operations 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 could develop a single operations plan that addresses both without repeating common elements. It is the EIMO's responsibility to ensure that the 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 need to be documented and incorporated by reference in the issuer's operations plan. In such cases, the operations plan could point readers to additional documentation and information.

Subtask 1.2: Confirm that the 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: EIMO, Issuing Facility Manager

Guidance: Even though an issuer follows the requirements of [FIPS201], its processes need to be consistent within the 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 (iii) prepare a plan of assessment activities that indicate the proposed schedule and key milestones.

Subtask 2.1: Identify the SAO, DAO, PO, issuing facility managers, assessor, and other key personnel at the facility level who are performing functions, such as identity proofing/registration, card/token production, and activation/issuance (of the PIV Card or derived PIV credential). Maintenance personnel also need to be contacted to provide requested assessment information to the assessor.

Responsibility: EIMO

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: EIMO, DAO

Guidance: The authorization boundary determines the target of the assessment. In preparation for the issuer assessment, the EIMO and DAO need to identify which issuing facilities and external service providers are to be included. This ensures that the functions performed and processes managed by the external service provider are considered during the authorization process. An organization could consider including only those issuing facilities that are ready to operate within the scope of the issuer assessment; 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 to execute the assessment.

Responsibility: EIMO, Assessor, DAO

Guidance: The level of effort required for an assessment depends on numerous factors, such as (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 PIV credentials being issued. By examining factors that could influence the complexity of the assessment, the organization can make an informed judgment 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 to (i) determine whether the requirements of [FIPS201] have been implemented, (ii) evaluate the operations plan and revise as needed, and (iii) obtain acceptance of the plan by the DAO prior to assessing the issuer controls.

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

Responsibility: DAO, EIMO

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

Subtask 3.2: Analyze the operations plan to determine whether there are deficiencies in satisfying all of the policies, procedures, and other requirements in [FIPS201] that could result in a DATO being issued. After discussing the discovered deficiencies in the documentation and operations plan with the EIMO, 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 either authorizes continuation of the assessment or terminates the assessment effort, depending on the evaluation of the issuer's ability to address the deficiencies.

Responsibility: DAO, EIMO

Guidance: The operations plan adequately addresses the policies, procedures, and processes of the issuer so that after an initial review, deficiencies that could lead to an eventual DATO can 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 authorizes 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 can 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 [FIPS201] are implemented correctly, operating as intended, and producing the desired outcomes. This phase also specifies the actions to be taken to correct all identified deficiencies. An analysis of the impacts of identified deficiencies that cannot be corrected or mitigated efficiently on the reliable operation of the issuer is conducted and documented. The successful completion of this phase provides 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 assess the applicable issuer controls and (ii) document the results of the assessment. The assessor first verifies 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 then commences. The assessor also schedules interviews and real-time observations of issuance processes and initiates 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, they prepare descriptions of all discovered deficiencies along with recommendations for addressing and remediating those deficiencies.

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

Responsibility: Assessor

Guidance: The scope of the assessment is established based on the authorization boundary. The assessor reviews the selected assessment procedures (based on the scope of the assessment) in order to plan and coordinate activities for the assessment. For example, if a particular issuer control requires the observation of a particular process, the assessor needs to schedule the activity in a timely fashion after coordinating 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 the supporting materials necessary for the assessment of the issuer. If these documents include previous assessments, review the findings, and determine whether they are applicable to the current assessment.

Responsibility: EIMO, Assessor

Guidance: The EIMO assists the assessor in gathering all relevant documents and supporting materials from the organization that are required during the assessment of the issuer. The operations plan is central to this effort. The issuer's operations are completely described in the operations plan. The operations plan also includes or points to the supporting materials. In this case, the EIMO needs to gather the 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; and (vi) signed authorization letters under [SP800-37] for all information systems.

The assessor is strongly encouraged to review the results of any previous assessments, including the one on which the current ATO is based. The assessor might satisfy some of the issuer control assessment requirements by reviewing and referencing previous assessment reports. Although previous assessments cannot be used as a substitute for the current assessment, they provide insight on problems that could have existed in the past.

Subtask 4.3: Assess the required issuer controls using the prescribed assessment procedures found in Appendices 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 determine whether they have been implemented correctly, are operating as intended, and producing the desired outcomes. The assessor uses the assessment methods specified in Sec. 4.1. The 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 and to determine the expertise of the personnel performing key PIV functions. Processes need to be observed to ensure that 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 or derived PIV services have been outsourced to an external provider, the assessor verifies that the issuer controls that apply to those services are assessed, and the reliability of the service provider is found to be 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 to the authorization letter, the assessor can reuse the results of a previous assessment for the organization-level issuer controls and 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 in Appendix E provides a template 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 EIMO, who then adds the issuer's operations plan (revised, if necessary) and the CAP to generate an authorization submission package for the DAO. If the assessment report contains deficiencies, the EIMO might choose to address some deficiencies based on the assessor's recommendations and revise the operations plan (if needed) before submitting the package for authorization.

Subtask 5.1: Provide the EIMO with the assessment report.

Responsibility: Assessor

Guidance: The EIMO 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) understand the potential impacts of those deficiencies. The EIMO can choose to act on selected recommendations of the assessor before the authorization package is finalized. Any actions taken by the EIMO prior to the final authorization decision need to be coordinated with the DAO to optimize the utilization of resources across the organization. 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: EIMO

Guidance: The revised operations plan includes all of the changes made in response to the assessor's recommendations for corrective actions.

Subtask 5.3: Prepare the CAP.

Responsibility: EIMO

Guidance: The CAP is one of the three primary documents in the authorization submission package and describes actions that need to be taken by the EIMO to correct the deficiencies identified in Task 4, Issuer Control Assessment. 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 responsible for completing each of the tasks.

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

Responsibility: EIMO

Guidance: The EIMO is responsible for the assembly and compilation of the authorization submission package. The authorization submission package contains

(i) the final assessment report, (ii) the CAP, (iii) the revised operations plan, and (iv) the [SP800-37] authorization letters for all information systems used by the issuer. The EIMO 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 need to 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 EIMO will have one of the following: (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 whether the assessment phase has been satisfactorily completed so that a recommendation on the operation of the issuer can be made with assurance. The DAO works with the assessor to review the contents of the assessment submission package, the identified and uncorrected or uncorrectable deficiencies, the potential impacts of using the issuer's services, and the CAP to determine the final risk to the organization 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 if all applicable issuer controls are 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 help create confidence in assessment findings and is the main objective of the assessment review. Part of the assessment review also includes understanding the impacts of the identified deficiencies on the organization's operations, assets, and individuals.

Subtask 6.2: Determine whether 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 impacts of deficiencies. This helps the DAO 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 when determining the risk to the organization in terms of when and how the EIMO intends to address the known deficiencies. The DAO may consult the EIMO, assessor, or other organization officials before completing the final risk evaluation. This risk evaluation then determines the degree of acceptability of

issuer operations. The logic for using the latter as the basis for an authorization decision is described in Sec. 2.10.

Subtask 6.3: Share the authorization package with an independent party for review, and arrive at an authorization decision.

Responsibility: DAO

Guidance: Before providing the final authorization decision, the DAO may seek an independent review of the risks involved in the issuer operations. If the DAO finds it necessary, 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 EIMO and any other organization officials who have interests, roles, or responsibilities in the issuer's operations.

Responsibility: DAO

Guidance: The authorization decision package, including the authorization decision letter, is transmitted to the EIMO. Upon receipt of the authorization decision package, the EIMO reviews the authorization and its terms and conditions. The original authorization decision package is kept on file by the EIMO. The DAO retains copies of the contents of the authorization decision package. The authorization decision package needs to be appropriately safeguarded and stored in a centralized organization filing system whenever possible to ensure accessibility. The authorization decision package is made available to authorized auditors and oversight organizations upon request. The authorization decision package needs to be retained in accordance with the organization's records retention policy. The issuer and specific facilities are authorized for a maximum of three years from the date of the ATO. After the period ends, reauthorization is performed.

Subtask 7.2: Update the operations plan.

Responsibility: EIMO

Guidance: The operations plan needs to be updated to reflect all changes made as a result of the assessment and authorization. All conditions of the issuer's operations that are set forth in the authorization decision need to be noted in the plan and addressed in a timely manner, as conveyed by the DAO.

5.4. Monitoring Phase

The Monitoring Phase consists of two tasks: (i) operations plan maintenance and (ii) an annual life cycle 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's operations are 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 need to be monitored so that the organization minimizes exposing itself to security and privacy threats that exist or arise after the authorization of the issuer. For example, if there is significant staff turnover, the organization needs to be sure that new staff are performing the PIV functions using the same reliable processes that were previously approved. The overall responsibility for monitoring lies with the EIMO and the DAO.

An annual life cycle walkthrough of issuer operations involves reviewing all of the services and functions of an issuer and its facilities for continued reliability. The annual walkthrough covers the life cycle of PIV Card and derived PIV credential from sponsorship to maintenance. Observation of the full life cycle ensures that all processes are still reliably operating as assessed during the authorization.

Task 8: Operations Plan Update

An operations plan serves as the primary description on how PIV Cards or derived PIV credentials are being issued 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 impacts of changes as they occur and be significantly better prepared when reauthorization is required.

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

Responsibility: EIMO

Guidance: If changes are made to the information system, the issuer needs to update the operations plan, PIV Card, derived PIV credential, privacy policies, roles and responsibilities, and issuer controls.

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

Responsibility: EIMO

Guidance: If the results of the impact analysis indicate that changes to the issuer affect the reliability of its operations, the changes and impacts need to be reported to the DAO, corrective actions need to be initiated, and the CAP needs to be updated. If major changes have occurred, the issuer will need to be reauthorized.

Task 9: Annual Life Cycle Walkthrough

The annual life cycle walkthrough is a monitoring activity to be performed by the issuer when its PIV Card or derived PIV credential issuing services begin and annually thereafter. The EIMO (or designated appointee) is responsible for observing and reviewing the entire life cycle of the PIV Card or derived PIV credential. This

walkthrough is intended to provide an accurate and holistic view of the issuer's operations and reliability at a point in time. Any potential impacts to the reliability of the issuer's operations and risks to the organization need to be documented and presented to the EIMO and the DAO.

Subtask 9.1: Observe all of 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 needs to be repeated using randomly selected issuing facilities.

Responsibility: EIMO (or designated appointee)

Guidance: As part of the walkthrough, the EIMO (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 EIMO (or designated appointee) observes each process and compares it to the documented steps for the issuer and the associated issuer controls. An annual walkthrough is required until reauthorization is initiated.

Subtask 9.2: The results of the life cycle walkthrough are summarized in a report to the DAO. The report highlights any deficiencies and the corrective actions that need to be implemented to correct those deficiencies.

Responsibility: EIMO, DAO

Guidance: The EIMO (or designated appointee) documents the results of the walkthrough, which are recorded in the assessment report template included in Appendix E. All deficiencies need to be highlighted, and a plan for correcting each deficiency needs to be documented. The DAO decides whether any deficiency is significant enough to require a change of the issuer's ATO status.

References

[A-130] Office of Management and Budget (2016) *Managing Information as a Strategic Resource*. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[COMMON] Federal Public Key Infrastructure Policy Authority (2023) *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*. (Federal CIO Council), Version 2.5 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

[CSP] U.S. Office of Personnel Management (2020) *Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials* (U.S. Office of Personnel Management, Washington, DC), December 15, 2020. Available at https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf

[E-GOV] E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. Available at https://www.govinfo.gov/app/details/PLAW-107publ347

[FCS] U.S. Office of Personnel Management (2008) *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*. (U.S. Office of Personnel Management, Washington, DC), July 31, 2008. Available at https://www.opm.gov/suitability/suitability-executive-agent/policy/final-credentialing-standards.pdf

[FIPS140] National Institute of Standards and Technology (2019) *Security Requirements for Cryptographic Modules*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3 [or as amended]. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS199] National Institute of Standards and Technology (2004) *Standards for Security Categorization of Federal Information and Information Systems*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199 [or as amended]. https://doi.org/10.6028/NIST.FIPS.199

[FIPS200] National Institute of Standards and Technology (2006) *Minimum Security Requirements for Federal Information and Information Systems*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200 [or as amended]. https://doi.org/10.6028/NIST.FIPS.200

[FIPS201] National Institute of Standards and Technology (2022) *Personal Identity Verification (PIV) of Federal Employees and Contractors.* (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3 January 2022. https://doi.org/10.6028/NIST.FIPS.201-3

[FPKI] Federal Public Key Infrastructure Policy Authority (2022) *Federal Public Key Infrastructure (FPKI) Annual Review Requirements*. (Federal CIO Council),

Version 1.2 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf

[HSPD-12] Bush, GW (2004) *Policy for a Common Identification Standard for Federal Employees and Contractors*. (The White House, Washington, DC), Homeland Security Presidential Directive HSPD-12. Available at https://www.dhs.gov/homeland-security-presidential-directive-12

[NIST IR 7817] Ferraiolo H (2012) *A Credential Reliability and Revocation Model for Federated Identities*. (National Institute of Standard and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7817. https://doi.org/10.6028/NIST.IR.7817

[M-03-22] Office of Management and Budget (2003) *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. (The White House, Washington, DC), OMB Memorandum M-03-22, September 26, 2003. Available at https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/

[M-05-24] Office of Management and Budget (2005) *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, (The White House, Washington, DC), OMB Memorandum M-05-24, August 05, 2005. Available at https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-24.pdf

[M-19-17] Office of Management and Budget (2019) *Enabling Mission Delivery through Improved Identity, Credential, and Access Management.* (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[PAPER-RED] Paperwork Reduction Act of 1995, Pub. L. 104-13, 109 Stat 163. https://www.govinfo.gov/content/pkg/PLAW-104publ13/pdf/PLAW-104publ13.pdf

[PRIVACY] Privacy Act of 1974, Pub. L. 93-579, 88 Stat 1896. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

[REAL-ID] "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule," 73 Federal Register 5271 (January 29, 2008), pp 5271-5340. https://www.federalregister.gov/d/08-140

[SP800-37] Joint Task Force (2018) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-53] Joint Task Force (2020) *Security and Privacy Controls for Information Systems and Organizations.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5 [or as amended]. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) *Digital Identity Guidelines*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST

Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) *Digital Identity Guidelines: Enrollment and Identity Proofing*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 02, 2020 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-63B] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) *Digital Identity Guidelines: Authentication and Lifecycle Management*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 02, 2020 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63B

[SP800-63C] Grassi PA, Nadeau EM, Richer JP, Squire SK, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) *Digital Identity Guidelines: Federation and Assertions*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C, Includes updates as of March 02, 2020 [or as amended]. https://doi.org/10.6028/NIST.SP.800-63C

[SP800-73] Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) *Interfaces for Personal Identity Verification*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016 [or as amended]. https://doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] Grother PJ, Salamon WJ, Chandramouli R (2013) *Biometric Specifications for Personal Identity Verification*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-76-2

[SP800-78] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4 [or as amended]. https://doi.org/10.6028/NIST.SP.800-78-4

[SP800-156] Ferraiolo H, Chandramouli R, Mehta KL, Mohler J, Skordinski S, Brady S (2016) *Representation of PIV Chain-of-Trust for Import and Export*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-156 [or as amended]. https://doi.org/10.6028/NIST.SP.800-156

[SP800-157] Ferraiolo H, Cooper DA, Francomacaro S, Regenscheid AR, Burr WE, Mohler J, Gupta S (2014) *Guidelines for Derived Personal Identity Verification (PIV) Credentials*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-157 [or as amended]. https://doi.org/10.6028/NIST.SP.800-157

Appendix A. Acronyms

AAL
Authentication Assurance Level

ATO
Authorization to Operate

CAP
Corrective Action Plan

CSP
Credential Service Provider

DAO
Designated Authorizing Official

DATO
Denial of Authorization to Operate

DPCI
Derived PIV Credential Issuer

EIMO
Enterprise Identity Management Official

FIPS
Federal Information Processing Standard

HSPD-12
Homeland Security Presidential Directive-12

IATO
Interim Authorization to Operate

IDMS
Identity Management System

OMB
Office of Management and Budget

OPM
Office of Personnel Management

PCI
PIV Card Issuer

PII
Personally Identifiable Information

PIV
Personal Identity Verification

SAO
Senior Authorizing Official

SOP
Standard Operating Procedures

SORN
System of Records Notice

SRIP
Supervised Remote Identity Proofing

Appendix B. Glossary

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 the 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 or a derived PIV credential.

assessment (as applied to an issuer)
A formal process for 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 [FIPS201].

assessment method
A focused activity or action employed by an assessor to evaluate a particular issuer control.

assessment procedure
A set of activities or actions employed by an assessor to determine the extent to which an issuer control is implemented.

assessor
The third-party individual responsible for conducting assessment activities under the guidance and direction of a designated authorizing official.

authorization to operate (ATO)
One of three possible decisions made by a designated authorizing official after all assessment activities have been performed that states that the issuer is authorized to perform PIV Card and/or derived PIV credential issuance services.

activation/issuance
A process that includes procuring FIPS-approved blank PIV Cards or hardware/software tokens (for derived PIV credentials), initializing them using appropriate software and data elements, personalizing the cards/tokens with the identity credentials or authenticators of authorized subjects, and picking up or delivering 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 [FIPS201] has defined specific requirements.

corrective action plan (CAP)
Corrective actions for an issuer to remove or reduce the deficiencies or risks that were 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.

credential
An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a PIV Card or a hardware/software device that is possessed and controlled by a cardholder or subscriber.

denial of authorization to operate (DATO)
Issued by a designated authorizing official 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 defined in [SP800-63]. A derived PIV credential token can be a hardware- or software-based token that meets the requirements of [SP800-157].

derived PIV credential issuer (DPCI)
An issuer of a derived PIV credential, as defined in [SP800-157].

designated authorizing official (DAO)
A senior organization official who has the authority to authorize the reliability of an issuer.

enterprise identity management official (EIMO)
The individual responsible for overseeing the operations of an issuer in accordance with [FIPS201] and for performing the responsibilities specified in this guideline.

Homeland Security Presidential Directive 12 (HSPD-12)
HSPD-12 established the policy for which [FIPS201] was developed.

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 (e.g., a name, a card number).

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.

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 [FIPS201].

interim authorization to operate (IATO)
Issued by a designated authorizing official 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).

issuer
An entity that performs the functions required to produce, issue, and maintain PIV Cards or derived PIV credentials for an organization.

issuing facility
A physical site or location that is responsible for carrying out one or more of the PIV functions, including all equipment, staff, and documentation.

maintenance
The process of managing PIV Cards or derived PIV credentials once they are issued, including reissuance, post-issuance updates, and termination.

mobile device
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.

personally identifiable information (PII)
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 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 (i.e., human-readable and verifiable) or an automated process (i.e., computer-readable and verifiable).

PIV credential
Evidence that attests to one's right to credit or authority that authoritatively binds an identity (and, optionally, additional attributes) to an individual.

PIV identity account
The logical record that contains credentialing information for a given PIV cardholder. This is stored within the issuer's identity management system and includes PIV enrollment data, cardholder identity attributes, and information regarding the cardholder's PIV Card and any derived PIV credentials bound to the account.

post-enrollment binding
An association of the issued derived PIV credential to the subscriber's PIV identity account, as specified in [SP800-63B].

registration
Making a person's identity known to the enrollment/identity management information system by associating a unique identifier with that identity and collecting and recording the person's relevant attributes into the information system. Registration is required for adjudication, card/credential personalization and issuance, and maintenance, which are necessary to issue or maintain a PIV Card or derived PIV credential. Attributes about a cardholder and derived PIV credential holder may also be recorded in the individual's PIV identity account.

risk
The level of potential impact on an organization's operations (including mission, functions, image, or reputation), its assets, or individuals of a threat or a given likelihood of that threat occurring.

senior authorizing official (SAO)
A senior organization official who has budgetary control, provides oversight, develops policy, and has authority over all functions and services provided by the issuer.

subscriber
A PIV cardholder to whom a derived PIV credential has been issued.

system of record (SOR)
A group of records under the control of a federal agency that contain a personal identifier (e.g., a name, date of birth, fingerprint, Social Security Number, Employee Number) and one other item of personal data (e.g., home address, performance rating, and blood type) from which information is retrieved using a personal identifier.

System of Records Notice (SORN)
Ensures that privacy considerations have been addressed in the implementation of a system. The Privacy Act requires each agency to publish a notice of its systems of records in the Federal Register.

Appendix C. Issuer Readiness Review Checklist

The readiness review checklist is to be used by the organization while preparing for an assessment of their issuer. The checklist may also be used to validate that all relevant documentation is collected and that appropriate individuals have been identified and made available to the assessment team.

Table 5. Issuer readiness review checklist

Activity	Completed	Comments
Identify a third-party assessment team to support the assessment of 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 required information.		
Ensure that the necessary roles have been designated.		
Validate that implementation and management responsibilities for issuer controls have been accurately assigned.		
Ensure that the information systems utilized by the issuer are assessed and authorized to operate in accordance with [SP800-37].		
Ensure that the following documentation has been developed and made available to the assessment team: • Operations plan • Results from any past assessment and authorization • Letters of appointment (if any) • Service-level agreements (SLA) and memoranda of understanding (MOU) between the organization and service providers • List of all HSPD-12 components used within the PIV system • Privacy-related documentation • All forms utilized by the issuer • Documentation from outsourced providers • Standard operating procedures for the issuing facilities within the authorization boundary • Signed authorization letter under [SP800-37] for each information system within scope of the assessment		

Activity	Completed	Comments
Prior to authorization, an independent third party has been consulted and has reviewed the assessment (if needed).		
The PIV system is operational, and actual PIV processes can be observed by the assessment team.		
PIV Cards or 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 credentials are submitted on an annual basis to the FIPS 201 Evaluation Program for testing and are issued from a production system.		

1954

Appendix D. Operations Plan Templates

Appendices D.1 and D.2 are suggested outlines for a PCI and DPCI, respectively. It is highly recommended that an organization follow these templates to comprehensively document its operations in support of a successful authorization. An issuer of both PIV Cards and derived PIV credentials can develop a single operations plan that addresses all requirements without repeating common elements of the plan.

D.1. Operations Plan Template for PIV Card Issuers

1. Background

<Provide a brief background on HSPD-12, FIPS 201, and PIV, as well as how the organization plans to meet the directive.>

2. Purpose and Scope

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

3. Applicable Laws, Directives, Policies, Regulations, and Standards

<Identify all laws, directives, policies, regulations, and standards that govern PIV Card issuance at the organization.>

4. PCI Roles and Responsibilities

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

5. 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.>

6. PCI Description

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

7. Issuing Facility Details

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

8. PCI Management

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

a. Coordination and interaction

<Describe the management interactions within the PCI, both at an organization level and between the organization and the facilities.>

b. Staffing

<Describe the procedures employed to ensure that adequate staff are available to perform PIV Card issuance-related functions.>

c. Training

<Describe the procedures employed to ensure that staff are 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).>

9. PCI Policies and Procedures

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

a. Sponsorship

b. Identity proofing and registration

c. Adjudication

d. PIV Card production

e. Activation/issuance

f. Maintenance

i. Reissuance

ii. Post-issuance updates

iii. Termination

g. Temporary/non-PIV badges

10. PCI Issuance Information System Description

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

a. Architecture

b. Interconnections and information sharing

c. Information system inventory

d. Public key infrastructure

e. [SP800-37] Authorization letters

11. Card Personalization and Production

<Describe the organization's PIV Card graphical layouts and the (optional) data of the containers being used. Provide details on PIV Card expiration date requirements levied by the organization, and 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

12. Issuer Controls

<This section documents the issuer controls (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 I — Memoranda of Appointment

<Attach copies of signed memoranda of appointment that record the various roles that have been assigned and the personnel who have accepted the roles and their associated responsibilities.>

Appendix II — Privacy Requirements

<Attach copies of 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 III — Service-Level Agreements and Memoranda of Understanding (MOU)

<Attach 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 PIV-related functions.>

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

1. Background

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

2. Purpose and Scope

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

3. Applicable Laws, Directives, Policies, Regulations, and Standards

<Identify all laws, directives, policies, regulations, and standards that govern derived PIV credential issuance at the organization.>

4. DPCI Roles and Responsibilities

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

5. Assignment of Roles

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

6. DPCI Description

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

7. Issuing Facility Details

<If applicable, identify all of the issuing facilities that are included and part of the authorization boundary. Provide details, such as the location, the derived PIV credential functions performed at the facility, and the types and approximate number of derived PIV credentials personalized at each facility. Indicate whether issuance is conducted remotely in 6.>

8. DPCI Management

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

a. Coordination and Interaction

<Describe the management interactions within the DPCI, both at an organization level and between the organization and facilities.>

b. Staffing

<Describe the procedures employed to ensure that adequate staff are available to perform derived PIV credential-related issuance functions.>

c. Training

<Describe the procedures employed to ensure that staff are 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 derived PIV credential functions being outsourced (if applicable).>

9. DPCI Policies and Procedures

<Describe the various policies and procedures that apply for (i) sponsorship, (ii) post-enrollment binding, (ii) token production, (ii) activation and issuance, and (iv) maintenance.

a. Sponsorship

b. Post-enrollment binding

c. Token production (if applicable)

d. Activation/issuance

e. Maintenance

i. Reissuance

ii. Post-issuance updates

iii. Termination

10. DPCI Issuance System Description

<Provide a description of the technical aspects of the organization's derived PIV credential issuance system, including system architecture, network connectivity, connections to external systems and information shared both internally and externally, the PKI provider (if applicable), and the information system authorization status.>

a. Architecture

b. Interconnections and information sharing

c. Information system inventory

d. Public key infrastructure

e. [SP800-37] Authorization letters

11. Derived PIV Credential Details

<Provide details about the organization's implementation of the derived PIV credential. Describe whether it is PKI or non-PKI-based and whether it is AAL2 or AAL3.>

a. Derived PIV credential data elements
b. Inventory management (for hardware-based)

12. 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 I — Memoranda of Appointment

<Attach copies of signed memoranda of appointment that record the various roles that have been assigned and the personnel who have accepted the roles and their associated responsibilities.>

Appendix II — Privacy Requirements

<Attach copies of 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 III — Service-Level Agreements and Memoranda of Understanding (MOU)

<Attach 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 derived 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.

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: (Artifacts)

Observe: (Name of Process)

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

Assessment Findings —

Assessment Deficiency and Potential Impact —

Recommendation —

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: Enterprise 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) 800-79r3, *Guidelines for the Authorization of PIV Card and Derived PIV Credential Issuers*, 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) [SP800-37] authorization letter(s) for each information system of the [ISSUER].

The operations plan and its policies, procedures, and processes have been assessed by [ASSESSOR] using the assessment methods and procedures defined in SP 800-79r3 and specified in the assessment report to determine the extent to which the requirements under [HSPD-12] and [FIPS201] have been met. 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: Enterprise Identity Management Official

Subject: Authorization Decision for [PCI/DPCI]

After reviewing the results of the authorization package of the [PCI/DPCI NAME], I have determined that its policies, procedures, and processes comply with both [FIPS201] 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 [ISSUER]. 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 life cycle walkthrough is completed annually, and the results are sent to me within 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: Enterprise Identity Management Official

Subject: Authorization Decision for [PCI/DPCI]

After reviewing the results of the assessment of [ISSUER NAME], I have determined that the requirements identified in [FIPS201] and the organization's policies, regulations, and standards have not been implemented satisfactorily. However, I have also 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 [ISSUER] shall be performed in accordance with the enclosed terms and conditions during the IATO period. The [ISSUER] is *not* considered authorized during this IATO period.

This IATO also applies to facilities under the [ISSUER]. 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 until 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 [ISSUER] 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 to reduce or eliminate the deficiencies in accordance with the corrective actions plan (CAP). At the end of IATO period, the [ISSUER] 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 the removal or reduction of concerns and discrepancies before reauthorization 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: Enterprise Identity Management Official

Subject: Authorization Decision for [PCI/DPCI]

After reviewing the results of the assessment of [ISSUER NAME] and the supporting evidence provided in the associated authorization package, I have determined that the requirements identified in [FIPS201] and the organization's policies, regulations, and standards are not being met by the [ISSUER]. Accordingly, I am issuing a denial of authorization to operate (DATO) to the [ISSUER] and its issuing facilities. The [ISSUER] 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. Reauthorization 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 PCI and DPCI, respectively. 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.

G.1. Controls and Assessment Procedures for PCIs

The following tables list the set of issuer controls applicable to PCIs. Control descriptions and assessment procedures have been updated in this revision of SP 800-79 based on updates to [FIPS201] and its supporting publications. Control identifiers have been labeled with "NEW" or "UPDATED" to clearly identify whether an existing issuer control has been added or updated, respectively. Additionally, controls that were either (i) withdrawn in the previous version of SP 800-79 or (ii) moved to or combined with another control in the previous version of SP 800-79 have been removed from this version for the sake of conciseness and brevity.

A control labeled with "NEW" represents an issuer control that has been added to the issuer control catalog. This does not necessarily represent a new requirement added to [FIPS201]. A "NEW" control signifies that a requirement in [FIPS201] needs to be explicitly assessed to ensure that the PCI is compliant with the necessary requirements associated with PIV Card issuance and maintenance. Controls labeled with "UPDATED" represent an existing issuer control for which the control description and assessment procedures have been revised considerably, though the overall intent of the control has not changed from the prior version.

Table 6. Preparation and Maintenance of Documentation for PCIs

Identifier	Issuer Control	Source
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 (i) the list of issuer controls from Appendix G.1, (ii) the owner for each issuer control, (iii) a description of how the control is implemented, and (iv) whether the control is organization- or facility-specific (review).* *(iii) Relevant operating procedures and associated documentation are referenced accurately (review).* *(iv) The operations plan has been reviewed and approved by the DAO within the organization (review, interview).*	SP 800-79, Sec. 2.12 – Authorization Submission 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 (or equivalent) of the federal department or agency. **Assessment** *Determine that*: *(i) The organization has developed and documented a written policy and procedures for identity proofing and registration (to include in-*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements

Identifier	Issuer Control	Source
	person, supervised remote identity proofing, interagency transfer, and extended enrollment if supported) (review). *(ii) The policy is consistent with the organization's mission, functions,* [FIPS201], *and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The policy and procedures have been approved by the head or deputy (or equivalent) of the federal department or agency (review).* *(iv) The organization periodically reviews and updates the policy and procedures, as required (review, interview).*	
DO-3	The organization has a written policy and procedures for issuance that are approved by the head or deputy (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 (to include in-person and supervised remote issuance if supported) (review).* *(ii) The policy is consistent with the organization's mission, functions,* [FIPS201]*, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The policy and procedures have been approved by the head or deputy secretary (or equivalent) of the federal department or agency (review).* *(iv) The organization periodically reviews and updates the policy and procedures, as required (review, interview).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements
DO-5	The organization has a written policy and procedures that describe 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, functions,* [FIPS201]*, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The organization periodically reviews and updates the policy as required (review, interview).*	[FIPS201], Sec. 2.9.4 – PIV Card Termination Requirements
DO-6	The organization has a written policy and procedures that describe the conditions for PIV Card reissuance and post-issuance updates. **Assessment** *Determine that*: *(i) The organization has developed and documented a written policy and procedures for card reissuance and post-issuance updates (review).* *(ii) The policy is consistent with the organization's mission, functions,* [FIPS201]*, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The organization periodically reviews and updates the policy and procedures as required (review, interview).*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements [FIPS201], Sec. 2.9.2 – PIV Card Post Issuance Update Requirements
DO-7 (UPDATED)	The organization has developed procedures in conjunction with the credentialing standards for making all decisions regarding the eligibility of individuals, such as guest researchers, volunteers, intermittent employees, seasonal employees, or employees on temporary appointments that last less than 6 months.	OPM Memorandum [CSP]

Identifier	Issuer Control	Source
	Assessment *Determine that*: *(i) The organization has developed and documented a written policy and procedures for the issuance of an alternative identity credential for short-term personnel who do not qualify for a PIV Card (review).* *(ii) The policy is consistent with the organization's mission, functions, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The organization periodically reviews and updates the policy and procedures as required (review, interview).*	
DO-8	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, except for employees under the command of a U.S. area military commander (review).* *(ii) The policy and procedures have been approved by the head or deputy (or equivalent) of the federal department or agency (review).*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements OPM Memorandum [CSP]

Table 7. Assignment of Roles and Responsibilities for PCIs

Identifier	Issuer Control	Source
RR-1	The organization has appointed the role of senior authorizing official (SAO). **Assessment** *Determine that*: *(i) The organization has defined the role of SAO and its responsibilities according to the requirements of SP 800-79 (review).* *(ii) The organization has assigned the role of SAO (review).*	SP 800-79, Sec. 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 DAO and its responsibilities according to the requirements of SP 800-79 (review).* *(ii) The organization has assigned the role of DAO (review, interview).*	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities
RR-3	The organization has appointed the role of enterprise identity management official (EIMO). **Assessment** *Determine that*: *(i) The organization has defined the role of EIMO and its responsibilities according to the requirements of SP 800-79 (interview).* *(ii) The organization has assigned the role of EIMO (review, interview).*	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities
RR-4	The organization has appointed the role of assessor. **Assessment** *Determine that*:	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities

Identifier	Issuer Control	Source
	(i) The organization has defined the role of assessor and its responsibilities according to the requirements of SP 800-79 (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 operations of the organization (review, interview).*	
RR-5	The organization has appointed the role of privacy official (PO). **Assessment** *Determine that*: *(i) The organization has defined the role of PO and its responsibilities according to the requirements of SP 800-79 (review).* *(ii) The organization has assigned the role of PO (review).* *(iii) The PO does not have any other roles in the organization (review, interview).*	[FIPS201], Sec. 2.11 – PIV Privacy Requirements SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities
RR-6	The organization employs processes that 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) Standard operating procedures for identity proofing, registration, issuance, and re-issuance demonstrate adherence to the principle of separation of duties (review, interview, observe).*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements

2310

2311 **Table 8.** Facility and Personnel Readiness for PCIs

Identifier	Issuer Control	Source
FP-1	Minimum physical controls at the issuing facility are implemented, including (i) door locks and restricted access (e.g., use of locked rooms, safes, and lockable cabinets, as appropriate); (ii) sensor devices on registration and issuance stations (e.g., fingerprint readers and cameras) that are integral to the station (for supervised remoted identity proofing only); (iii) protection of registration and issuance stations against tampering, removal, or replacement; (iii) security for registration and issuance stations to ensure that no malicious code is introduced to compromise or otherwise impair the station or PIV Card; (v) security monitoring and automated alarms; (v) emergency power and lighting; and (vi) fire prevention and protection mechanisms. **Assessment** *Determine that:* *(i) The EIMO and facility managers are aware of the minimum set of physical controls that need to be in place at the facilities (interview).* *(ii) The minimum physical security controls are implemented by the facility (observe).* *(iii) The facility has a process to report any problems with the station to the issuer (review).*	Commonly accepted security readiness measures [FIPS201], Sec. 2.7.1 – Supervised Remote Identity Proofing
FP-2	Issuer documentation (e.g., operations plan, standard operating procedures, contracts, etc.) is maintained at each issuing facility. **Assessment** *Determine that:*	Commonly accepted security readiness measures

Identifier	Issuer Control	Source
	(i) The most current versions of issuer documentation are available at each issuing facility for reference as needed (review, interview).	
FP-3	Issuing facility managers have a securely stored copy of the contingency/disaster recovery plan for the information systems. **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 intent of this control is covered by DP-1.	-
FP-5	Card activation/issuance workstations are situated in an enclosed area (e.g., 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 (e.g., wall or partition) such that other individuals cannot see an applicant or card holder's personal information (observe).*	Commonly accepted security readiness measures
FP-6	This control is withdrawn since M-11-11 has been rescinded.	-
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 (e.g., fraudulent source document detection, correct techniques for fingerprint capture, etc.) 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 (review, interview).* *(ii) Records showing that the appropriate training course has been completed by issuing facility personnel are stored by the facility for audit purposes (review, interview).*	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities Commonly accepted security readiness measures
FP-8	The issuing facility is responsible for the card stock, its management, and its integrity. All pre-personalized and personalized smart card stock from card vendors and card production facilities are only received by authorized personnel who ensure that the card stock is stored, handled, and disposed of securely. **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) Authorized personnel are knowledgeable about procedures for receiving, storing, and destroying (in case of printing errors) smart card stock (interview).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements

Identifier	Issuer Control	Source
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 issuer for identity proofing, registration, 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, interview).*	Commonly accepted security readiness measures

2312

2313 **Table 9.** Protection of Stored and Transmitted Data for PCIs

Identifier	Issuer Control	Source
ST-1 (UPDATED)	The issuer PIV information systems are implemented in accordance with the spirit and letter of all federal privacy laws and policies, including the E-Government Act of 2002 [E-GOV], the Privacy Act of 1974 [PRIVACY], and OMB [M-03-22], as applicable. **Assessment** *Determine that*: *(i) PIV information systems are operated and managed in accordance with federal privacy laws and applicable organizational policies (review).* *(ii) The organization does not disclose any record contained in the system of records to any person or organization unless written consent has been given by the individual to whom the record pertains or one of the exceptions for disclosure in the Privacy Act are met (review, interview).* *(iii) Individuals are permitted access to their personal record, and the information is provided in a form that is comprehensible to them (review, interview).* *(iv) 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 can request a review of the refusal (review, interview).* *(v) 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).*	[FIPS201], Sec. 2.11 - PIV Privacy Requirements E-Government Act [E-GOV] Privacy Act [PRIVACY] OMB Memorandum [M-03-22]
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).*	[FIPS201], Sec. 2.11 – PIV Privacy Requirements
ST-3 (NEW)	The organization ensures that only personnel (e.g., operators) with a legitimate need for access to PII in the PIV system are authorized to access the PII, including the information and databases maintained for registration and credential issuance. **Assessment**	[FIPS201], Sec. 2.11 – PIV Privacy Requirements

Identifier	Issuer Control	Source
	Determine that: *(i) The organization maintains a list of personnel who can access PII (review, interview).* *(ii) Personnel with access to PII have completed a privacy training course and are familiar with PII handling procedures (review, interview).* *(iii) Records showing that a privacy training course has been completed by personnel with access to PII are stored for audit purposes (review).*	

Table 10. Enforcement of Privacy Requirements for PCIs

Identifier	Issuer Control	Source
PR-1	Privacy Act statements/notices, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees who violate 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 posts Privacy Act statements/notices, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees who violate privacy policies (review, interview).* *(ii) The organization maintains appeal procedures for those who are denied a credential or whose credentials are revoked (review).*	OMB Memorandum [M-05-24]
PR-2 (UPDATED)	The organization conducts a comprehensive privacy impact assessment (PIA) and a periodic review and update of the assessment on systems that contain PII for the purpose of implementing PIV consistent with the methodology of [E-GOV] and the requirements of [M-03-22]. Assessment Determine that: *(i) The organization conducts a PIA of their issuer information systems based on guidance found in* [E-GOV] *and* [M-03-22] *(review).* *(ii) The organization submits the PIA of their issuer information systems to OMB (review, interview).*	[FIPS201], Sec. 2.11 – PIV Privacy Requirements E-Government Act [E-GOV] OMB Memorandum [M-03-22]
PR-3	The organization's employee and contractor identification system of records notices (SORNs) 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 [PRIVACY] and OMB Circular [A-130], Appendix 1. **Assessment** *Determine that:* *(i) The organization updates SORNs to reflect changes in the disclosure of information (review, interview).*	Privacy Act [PRIVACY] OMB Memorandum [M-05-24]
PR-4 (UPDATED)	The organization writes, publishes, and maintains a clear and comprehensive document that lists the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information.	[FIPS201], Sec. 2.11 – PIV Privacy Requirements

Identifier	Issuer Control	Source
	Assessment *Determine that:* *(i) The organization has developed, documented, and published the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information (review).* *(ii) The issuing facility requires the applicant to be notified of the PII 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 (interview, observe).*	
PR-5	The issuer employs technologies that allow for the 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 PII (review, interview, observe).*	[FIPS201], Sec. 2.11 – PIV Privacy Requirements
PR-6	In the case of termination, the PII collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the organization. **Assessment** *Determine that:* *(i) As part of PIV Card termination, the organization disposes of PII in accordance with its privacy and data retention policies while considering grace period provisions (review, interview).*	[FIPS201], Sec. 2.9.4 – PIV Card Termination Requirements
PR-7 (NEW)	Enrollment records contain PII that needs to be protected in a manner that protects the individual's privacy and maintains the integrity of the records both in transit and at rest. **Assessment** *Determine that:* *(i) The organization ensures that cardholder PII is protected following applicable policies and guidance (review).* *(ii) The issuer components that contain PII are authorized to operate in accordance with* [SP800-37] *(review).*	[FIPS201], Sec. 2.6 – PIV Enrollment Records
PR-8 (NEW)	The organization follows applicable federal laws and regulations regarding the retention and destruction of biometric data. **Assessment** *Determine that:* *(i) The organization follows a documented policy that addresses the retention and destruction of biometric data (review).* *(ii) The organization does not retain biometric data beyond the documented timelines (observe).* *(iii) The organization has an approved method for the destruction of biometric data (review, observe).*	[FIPS201], Sec. 2.5 – Biometric Data Use

2316 **Table 11.** Deployed Products and Information Systems for PCIs

Identifier	Issuer Control	Source
DP-1	In order to be compliant with the provisions of OMB Circular [A-130], App III, the issuer PIV information systems are authorized to operate in accordance with [SP800-37]. Controls described in [SP800-53] are used to accomplish security and privacy goals, where applicable. **Assessment** *Determine that:* *(i) The organization has a letter showing the current authorization decision of each PIV information system used to support the issuer (review).*	[FIPS201], Appendix A.2 Application of Risk Management Framework to IT System(s) Supporting PCI [FIPS201], Sec. 2.11 – PIV Privacy Requirements
DP-2	Products and services utilized by an issuing facility to issue a PIV Card are listed on the GSA FIPS 201 Evaluation Program's Approved Products List (APL), where applicable. **Assessment** *Determine that:* *(i) For each product or service that falls within one of the categories in the FIPS 201 Evaluation Program, its presence (i.e., make, model, version) is checked on the APL (review).* *(ii) There is no product in operation that has been moved to the GSA Removed Products List (RPL) (review).*	OMB Memorandum [M-05-24] Federal Acquisition Regulation (FAR), Sec. 4.1302 Acquisition of approved products and services for personal identity verification
DP-3 (UPDATED)	The organization annually submits a personalized PIV Card issued from their production system to the FIPS 201 Evaluation Program for conformance testing. **Assessment** *Determine that:* *(i) Printed information on the submitted PIV Card complies with the mandatory and optional items specified in* [FIPS201], *Sec. 4.1.4. (review).* *(ii) The PIV credentials on the PIV Card conform to the PIV Data Model (review).*	[COMMON], Sec. 8.1 – Frequency or Circumstances of Assessment

2317

2318 **Table 12.** Implementation of Credentialing Infrastructures for PCIs

Identifier	Issuer Control	Source
CI-1 (UPDATED)	For legacy public key infrastructures (PKIs), the organization's CA is cross-certified with the Federal Bridge Certificate Authority (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 cross-certified and authorized to issue certificates with the appropriate OIDs (review).* *(ii) The organization operating the legacy PKI conducts an annual CA review in accordance with https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf (review).* *(iii) The organization assembles and submits their annual review package to the FPKI Policy Authority (PA) by their coordinated due date (review, interview).*	[FIPS201], Sec. 5.4 – Legacy PKI [FPKI], Sec. 1.4 – Package Submission

Identifier	Issuer Control	Source
CI-2 (UPDATED)	For non-legacy PKIs, 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 as being a shared service provider (review).* *(ii) The organization leveraging a shared service provider for PIV certificates completes an annual registration authority audit in accordance with https://www.idmanagement.gov/docs/fpki-ra-audit-guidance.pdf (review).* *(iii) The organization leveraging a shared service provider for PIV certificates completes an annual key recovery audit in accordance with https://www.idmanagement.gov/docs/fpki-ra-audit-guidance.pdf (review).* *(iv) The organization submits the results of the annual audit of their registration authority and key recovery practices against the relevant CP/CPS to their shared service provider for submission to the FPKI Policy Authority (PA) by their coordinated due date (review, interview).*	[FIPS201], Sec. 5.2 – PKI Certificate [FPKI], Sec. 1.4 – Package Submission
CI-3	When cards are personalized, each PIV Card contains a unique PIV Card application administration key specific to that PIV Card. **Assessment** *Determine that:* *(i) The CMS vendor's documentation shows the use of unique PIV Card application administration keys (review).* *(ii) The EIMO indicates that the PIV Card application administration keys are unique to each card (interview).*	[FIPS201], Sec. 4.3.2 – Activation by Card Management System
CI-4	Fingerprint images retained by organizations are formatted according to [SP800-76]. **Assessment** *Determine that:* *(i) The fingerprint images are formatted according to Table 4 in* [SP800-76] *and INCITS 381-2004 (review, test).*	[SP800-76], Sec. 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 [SP800-76]. **Assessment** *Determine that:* *(i) The facial images are formatted according to Table 12 in* [SP800-76] *and INCITS 385 (review, test).*	[SP800-76], Sec. 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 [SP800-76], Sec. 4.2, and (ii) formatted such that they conform to [SP800-76]. **Assessment** *Determine that:* *(i) The procedures used to fingerprint the applicant are based on the primary and secondary finger selection criteria detailed in* [SP800-76], *Sec. 4.2 (review, observe).*	[SP800-76], Sec. 4.2 – Source Images

Identifier	Issuer Control	Source
	(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* [SP800-76] *and INCITS 378-2004 (review, test).*	
CI-7	The identity management system (IDMS) or Central Verification System (CVS) reflects the adjudication status of each PIV cardholder as part of the PIV identity account. **Assessment** *Determine that:* *(i) The issuer's IDMS or CVS is capable of recording the adjudication status of each PIV Cardholder as part of the PIV identity account (review, observe).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements
CI-8	Iris images collected during identity proofing and registration are formatted such that they conform to [SP800-76], if applicable. **Assessment** *Determine that:* *(i) Iris images are formatted according to Table 9 in* [SP800-76] *and ISO/IEC 19794-6:2011 (review, test).*	[SP800-76], Sec. 6.3 – Iris image specification for PIV Cards
CI-9	Fingerprint templates for on-card comparison (OCC) that are collected during identity proofing and registration are formatted such that they conform to [SP800-76], if applicable. **Assessment** *Determine that:* *(i) Fingerprint templates for on-card comparison are formatted according to Table 7 in* [SP800-76] *and ISO/IEC 19794-2:2011 (review, test).*	[SP800-76], Sec. 5.5.1 – Biometric Information Template
CI-10	The intent of this control is covered by CI-11.	-
CI-15 (NEW)	As part of the PIV identity account, the issuer maintains an enrollment record for each issued PIV Card. **Assessment** *Determine that:* *(i) The enrollment data record maintains an auditable sequence of enrollment events to bind an applicant to multiple transactions that might take place at different times and locations. These include activities that document (i) who took the action, (ii) what action was taken, (iii) when and where the action took place, and (iv) and what data was collected (review).* *(ii) The enrollment data record includes details of biometric acquisition, including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method (review).* *(iii) The enrollment data record includes (i) unique identifiers issued to the individual (e.g., FASC-N, UUID, etc.); (ii) information about the authorizing entity that has approved the issuance of a credential; (iii) the current status of the background investigation, including the results of the investigation once completed; (iv) the evidence of authorization if the credential is issued under a pseudonym; and (v) any other relevant data about the cardholder, including subsequent changes in the data (e.g., cardholder name changes) (review).* *(iv) The records are stored as part of the cardholder's PIV identity account, either as part of the issuer's IDMS or through links to*	[FIPS201], Sec. 2.6 – PIV Enrollment Records [SP800-156], Sec. 2 – Chain-of-Trust Data Representation

Identifier	Issuer Control	Source
	records in other related systems (e.g., card management systems) (review). *(v) Exchange/transfer of enrollment records are represented in an XML schema in accordance with* [SP800-156] *(review), if applicable.*	
CI-16 (NEW)	If the organization collects biometric data to conduct background investigations and for PIV Card personalization on separate occasions, a biometric comparison is performed to confirm that the two fingerprints collected for off-card one-to-one comparisons elicit a positive biometric verification decision when compared to the same two fingerprints from the original set of 10 fingerprints. **Assessment** *Determine that:* *(i) The organization has implemented a solution to perform a biometric comparison to confirm that the fingerprints collected on separate occasions elicit a positive biometric verification decision (review).* *(ii) The organization performs a biometric comparison to confirm that the fingerprints collected for off-card one-to-one comparison are compared to the same two fingerprints from the original set of 10 fingerprints (review, observe).*	[FIPS201], Sec. 2.2 – Biometric Data Collection for PIV Card
CI-17 (NEW)	PIV Card application administration keys meet the algorithm and key size requirements stated in [SP800-78]. **Assessment** *Determine that:* *(i) The PIV Card application administration keys meet the algorithm and key size requirements stated in Table 5-1 of* [SP800-78] *(review, test).*	[FIPS201], Sec. 4.3.2 – Activation by Card Management System

Table 13. Sponsorship Process for PCIs

Identifier	Issuer Control	Source
SP-1	A PIV Card is issued to an individual only after a proper authority has authorized issuance of the card. **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).*	[FIPS201], Sec. 2.1 – Control Objectives
SP-2	The issuing facility collects personal information using only the forms approved by OMB under the Paperwork Reduction Act of 1995. **Assessment** *Determine that*: *(i) The forms used to collect personal information have been approved by OMB (review, observe).*	Paperwork Reduction Act [PAPER-RED]

2322 **Table 14.** Identity Proofing/Registration Process for PCIs

Identifier	Issuer Control	Source
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. Fraudulent identity source documents are not accepted as genuine or unaltered. **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 operators on how to verify the authenticity of source documents (review).* *(iii) The issuing facility performs electronic verification of identity source documents. Cryptographic security features are used to validate evidence, when available (review, observe).*	[FIPS201], Sec. 2.1 – Control Objectives [FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements
EI-2	The applicant appears in person at least once before the issuance of a PIV Card, either at the issuing facility or at a supervised remote identity proofing station. **Assessment** *Determine that:* *(i) The standard operating procedures for identity proofing, registration, and issuance ensure that the applicant appears in person at least once before the issuance of the PIV Card (review).* *(ii) The applicant appears in person at least once before the issuance of a PIV Card (observe).*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements
EI-3 (UPDATED)	Two identity source documents are checked based on those listed in [FIPS201], Sec. 2.7 and are neither expired nor cancelled. **Assessment** *Determine that:* *(i) The requirement to check two identity source documents based on the list provided in* [FIPS201], *Sec. 2.7 of is documented (review).* *(ii) At least one identity source document meets the requirements of strong evidence, as specified in* [SP800-63A] *(review, interview, observe).* *(iii) The identity source documents are not expired or cancelled (interview, observe).* *(iv) Two identity source documents are checked in accordance with* [FIPS201], *Sec. 2.7 of during the identity proofing process (observe).* *(v) If the two identity source documents bear different names, evidence of a formal name change is provided (review, observe).*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements
EI-4	At least 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 at least one of the identity source documents is a valid federal or state government-issued photo ID is documented (review).*	[FIPS201], Sec. 2.1 – Control Objectives [FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements

Identifier	Issuer Control	Source
	(ii) At least 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). *(iii) Driver's licenses and ID cards presented by applicants comply with* [REAL-ID] *when required pursuant to DHS regulations. State-issued driver's licenses and ID cards that are not* [REAL-ID]*-compliant can be used until the full enforcement date under [6 CFR § 37.5] (review, observe).*	
EI-7	The biometric data (e.g., fingerprints, facial image, and optional iris images) used to personalize the PIV Card are captured during the identity proofing and registration process. **Assessment** Determine that: *(i) The requirement to capture biometric data (e.g., fingerprints, facial image, and optional iris images) used to personalize the PIV Card are captured during the identity proofing and registration process and documented as part of standard operating procedures (review).* *(ii) The biometric data (e.g., fingerprints, facial image, and optional iris image) used to personalize the PIV Card are captured during the identity proofing and registration process (observe).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements
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).*	[SP800-76], Sec. 3.2 – Fingerprint Image Acquisition
EI-10	The issuing facility has an in-person or remote operator present at the time of biometric (e.g., fingerprint, facial image, 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 (e.g., fingerprint, facial image, and optional iris images) capture is documented (review).* *(i) The issuing facility has an attending official present at the time of biometric (e.g., fingerprint, facial image, and optional iris images) capture (observe).*	[SP800-76], Sec. 3.2 – Fingerprint Image Acquisition [SP800-76], Sec. 6.6 – Iris image quality control [FIPS201], Sec. 2.7.1 – Supervised Remote Identity Proofing
EI-11	The issuing facility acquires fingerprint images in accordance with Table 3 in [SP800-76]. **Assessment** *Determine that:* *(i) Fingers are inspected to ensure the absence of 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, or rolled ink card are based on procedures in Table 2 of* [SP800-76] *(observe).* *(iv) Multi-finger plain impression images are properly segmented into single finger images (observe).*	[SP800-76], Sec. 3.2 – Fingerprint Image Acquisition

Identifier	Issuer Control	Source
EI-12	A full set of fingerprints is collected from a PIV applicant who lacks an on-record background investigation. If fewer than 10 fingers are available, the missing fingers are labeled before transmitting the fingerprints to the FBI to conduct 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).* *(iii) If no fingers are available to be imaged, guidance is sought from respective investigative service providers for alternative means of performing law enforcement checks (review).*	[FIPS201], Sec. 2.3 –Biometric Data Collection for Background Investigations [SP800-76], Sec. 3.2 – Fingerprint Image Acquisition
EI-13 (UPDATED)	If the identity proofing and enrollment process is performed over multiple visits, an automated biometric verification attempt that compares the applicant's newly captured biometric characteristics against biometric data collected during a previous visit is performed at each visit and results in a positive verification decision. **Assessment** *Determine that:* *(i) If multiple sessions are needed for identity-proofing, registration, and issuance, the applicant is linked through a positive biometric verification decision obtained from an automated comparison of biometric characteristics captured at a previous session to biometric characteristics captured during the current session (review, observe).* *(ii) No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing and whose fingerprints are checked against databases is the person to whom the credential is issued (review, observe).*	[FIPS201], Sec. 2.1 – Control Objectives [FIPS201], Sec. 2.4 – Biometric Data Collection for PIV Card [FIPS201], Sec. 2.5 – Biometric Data Use
EI-14 (NEW)	If supervised remote identity proofing is used, it meets the following requirements at a minimum: (i) the station is maintained in a controlled-access environment; (ii) the station is monitored by staff at the station location while it is being used; (iii) a live operator participates remotely with the applicant for the entirety of the identity proofing session; (iv) operators have undergone a training program to detect potential fraud and to properly perform a supervised remote identity proofing session; (v) the operator monitors the entire identity proofing session with at least one continuous, high-resolution video transmission of the applicant; (vi) the operator requires all actions taken by the applicant during the identity proofing session to be clearly visible to the operator; (vii) the operator validates the physical or cryptographic security features of the primary and secondary identity source documents using scanners and sensors that are integrated into the station; and (viii) all communications occur over a mutually authenticated protected channel. **Assessment** *Determine that:* *(i) The station is maintained in a controlled access environment (observe).* *(ii) The station is monitored by staff at the station location while it is being used (observe).* *(iii) A live operator participates remotely with the applicant for the entirety of the identity proofing session (observe).*	[FIPS201], Sec. 2.7.1 –Supervised Remote Identity Proofing

Identifier	Issuer Control	Source
	(iv) The operator has undergone a training program to detect potential fraud and to properly perform a supervised remote identity proofing session (review). *(v) The operator monitors the entire identity proofing session using at least one continuous, high-resolution video transmission of the applicant (observe).* *(vi) All actions taken by the applicant during the identity proofing session are clearly visible to the operator (observe).* *(vii) The operator validates the physical or cryptographic security features of the primary and secondary identity source documents using scanners and sensors that are integrated into the station (review, observe).* *(viii) All communications from the remote station to the identity management system occur over a mutually authenticated protected channel (review, observe, test).*	
EI-15 (NEW)	If during supervised remote identity proofing, applicant biometric data cannot be collected per the criteria defined in [SP800-76] or if validation of the identity evidence is inadequate, identity proofing and enrollment needs to be halted and performed in-person at the issuer's facility. **Assessment** *Determine that:* *(i) The organization has a formally documented operating procedure on how to perform supervised remote identity proofing (including reasons for termination of the remote identity session, if required) (review).* *(ii) Supervised remote identity proofing is terminated if applicant biometric data cannot be collected per the criteria defined in* [SP800-76] *or if validation of the identity evidence is inadequate (review, observe).*	[FIPS201], Sec. 2.7.1 –Supervised Remote Identity Proofing

2323

2324 **Table 15.** Adjudication Process for PCIs

Identifier	Issuer Control	Source
AP-1 (UPDATED)	Prior to PIV Card issuance, the organization ensures that, at a minimum, (a) a completed and favorably adjudicated Tier 1 investigation — formerly called a National Agency Check with Written Inquiries (NACI) — or (b) the appropriate required investigation is initiated with the authorized federal investigative service provider, and the FBI NCHC portion of the background investigation is completed and favorably adjudicated for individuals for whom no prior investigation exists. **Assessment:** *Determine that:* *(i) The organization references a completed and favorably adjudicated Tier 1 investigation or the appropriate required investigation is initiated with the authorized federal investigative service provider, and the FBI NCHC portion of a background investigation is completed and favorably adjudicated for the applicant prior to PIV Card issuance (review, interview, observe).* *(ii) If the required investigation completes with an unfavorable adjudication after PIV Card issuance, termination procedures are followed, and the PIV identity account is updated with the results of the investigation (review, interview).*	[FIPS201], Sec. 2.7 – PIV Identity Proofing and Registration Requirements OPM Memorandum [CSP]

Identifier	Issuer Control	Source
AP-2	The intent of this control is covered by AP-1.	-
AP-3 (UPDATED)	The organization follows the credentialing eligibility standards issued by the Director of OPM and OMB. **Assessment:** *Determine that:* *(i) The organization has developed and documented a written policy and procedures on credentialing and eligibility standards (review).* *(ii) The organization assigns position designations to determine the investigative requirement (review, interview).* *(iii) Investigative requirements for each position are established by the Suitability and Credentialing Executive Agent and the Security Executive Agent (review, interview).* *(iv) Applicants being processed for a PIV Card receive the required investigation and are subject to any applicable reinvestigation or continuous vetting requirements to maintain their PIV eligibility (review, interview).* *(v) Final eligibility determination is reported to the Central Verification System or, if applicable, to their enrollment in the Continuous Vetting Program (review, interview).* (vi) *Final eligibility determination is recorded in or referenced by the PIV enrollment record to reflect PIV eligibility for the PIV cardholder (review, observe).*	[FIPS201], Sec. 2.2 –Credentialing Requirements OPM Memorandum [CSP]
AP-4	The intent of this control is covered by AP-1.	-
AP-5	The intent of this control is covered by AP-1.	-
AP-6 (NEW)	Only fingerprints are used to link background investigations since fingerprints are the only biometric characteristic used for background investigations. **Assessment:** *Determine that:* *(i) The organization has a formally documented process to link biometric investigations for PIV applicants when required (review).* *(ii) The issuing facility is capable of linking the background investigations of PIV applicants, when required (observe).* (iii) *The issuing facility staff is knowledgeable on how to link the background investigations of PIV applicants (interview).*	[FIPS201], Sec. 2.5 – Biometric Data Use

Table 16. Card Production Process for PCIs

Identifier	Issuer Control	Source
CP-1	To combat counterfeiting and alterations, the PIV Card contains security features outlined in the American Association of Motor Vehicle Administrators (AAMVA) Drivers License/Identification (DL/ID) Card Design Standard. **Assessment** *Determine that:* *(i) The PIV Card contains at least one security feature at inspection level 1 (e.g., an embossed surface pattern; an optically variable device, such as a hologram; color-shifting inks) or inspection level 2*	[FIPS201], Sec. 4.1.2 – Tamper Proofing and Resistance

Identifier	Issuer Control	Source
	(e.g., microtext, UV-fluorescent images, IR-fluorescent ink, nano and micro images, and chemical taggants) (interview, observe). *(ii) The 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).* *(iii) The presence of security features does not prevent the recognition of white as the principal card body color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm. (observe).*	
CP-2	The PIV Card is not embossed other than for security and accessibility features. **Assessment** *Determine that:* *(i) The PIV Card is not embossed other than for security and accessibility features (review, observe).*	[FIPS201], Sec. 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).*	[FIPS201], Sec. 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 that the card's material integrity is not adversely impacted. **Assessment** *Determine that:* *(i) Card body durability requirements and characteristics are not compromised by a punched opening (test).* *(ii) Printed information, including the photograph, are not altered or interfered with (test).* *(iii) Machine-readable technology, such as the embedded antenna, is not interfered with or damaged (test).* *(iv) Documentation shows that card manufacturer warranties or other product claims are not invalidated (review).*	[FIPS201], Sec. 4.1.3 – Physical Characteristics and Durability
CP-5	Requirements for tactilely discernible markers (e.g., edge ridging, notched corner, laser engraving) are covered under of AI-3.	-
CP-6	PIV Cards that contain topographical defects (e.g., scratches, poor color, fading, etc.) or are improperly printed are destroyed. **Assessment** *Determine that:* *(i) The issuing facility has a procedure to destroy PIV Card that contain topographical defects or are improperly printed (review).* *(ii) The issuing facility destroys PIV Cards that contain topographical defects or are improperly printed (observe).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements
CP-7	PIV Cards are printed using the color representation specified in Table 4-2 Color Representation in [FIPS201], Sec. 4.1.5. **Assessment** *Determine that:*	[FIPS201], Sec. 4.1.5 – Color Representation

Identifier	Issuer Control	Source
	(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).*	
CP-8 (NEW)	Card personalization ensures that, at a minimum, (i) the printed material does not rub off, (ii) the printing process does not deposit debris on the printer rollers during printing and laminating, and (iii) printed material does not interfere with the ICCs or related components, nor does it obstruct access to machine-readable information. **Assessment** *Determine that:* *(i) Printed material does not rub off once the PIV Card is personalized (observe, test).* *(ii) PIV Cards function as intended once they are printed and laminated (observe, test).*	[FIPS201], Sec. 4.1.1 – Printed Material

Table 17. Activation/Issuance Process for PCIs

Identifier	Issuer Control	Source
AI-1	The personalized PIV Card complies with all mandatory items on the front of the PIV Card. **Assessment** *Determine that:* *(i) The PIV Card meets the specific requirements in* [FIPS201] *for (i) photograph; (ii) name; (iii) employee affiliation; (iv) agency, department, or organization; (v) card expiration dates (zones 14F and 19F); and (vi) color coding for employee affiliation (zone 15F and 18F) (observe, test).*	[FIPS201], Sec. 4.1.4.1 – Mandatory Items on the Front of the PIV Card
AI-2	The personalized PIV Card complies with all mandatory items on the back of the PIV Card. **Assessment** *Determine that:* *(i) The PIV Card meets the specific requirements in* [FIPS201] *for (i) an agency card serial number and (ii) issuer identification number (observe, test).*	[FIPS201], Sec. 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 the specific requirements in* [FIPS201] *if it includes optional items on the front of the card, such as a (i) signature, (ii) agency-specific text area, (iii) rank, (iv) portable data file (deprecated), (v) header, (vi) agency seal, (vii) footer, (viii) issue date, (ix) photo border, (x) agency-specific data, (xi) organizational affiliation abbreviation, (xii) edge ridging or notched corner tactile marking, and (xiii) laser engraving tactile marker (observe, test).*	[FIPS201], Sec. 4.1.4.3 – Optional Items on the Front of the Card

Identifier	Issuer Control	Source
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 the specific requirements in* [FIPS201] *if it includes optional items on the back of the card, such as (i) a magnetic stripe (deprecated); (ii) a return address (iii) the 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 (deprecated); and (vii) agency-specific text (zones 9B and 10B) (observe, test).*	[FIPS201], Sec. 4.1.4.4 – Optional Items on the Back of the Card
AI-5 (UPDATED)	The PIV Card includes mechanisms to block activation of the card after a number of consecutive failed activation attempts. A maximum of 10 consecutive activation retries for each of the activation methods (i.e., PIN and OCC attempts) are permitted. **Assessment** *Determine that:* *(i) The PIV Card blocks activation after 10 consecutive failed attempts unless a lower limit is imposed by the issuer (observe, test).*	[FIPS201], Sec. 4.3.1 – Activation by Cardholder
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 date 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).*	[FIPS201], Sec. 2.8 – PIV Card Issuance Requirements [FIPS201], Sec. 2.9.1 – PIV Reissuance Requirements
AI-7 (UPDATED)	Before the PIV Card is provided to the applicant, the operator performs a one-to-one comparison of the applicant against the biometric data records available on the PIV Card or in the PIV enrollment record. If the biometric verification decision is negative, or if no biometric data records are available, the cardholder provides two identity source documents (as specified in [FIPS201], Sec 2.7), which are inspected and compared by the operator with the photograph printed on the PIV Card. **Assessment** *Determine that:* *(i) The PIV Card is released to the applicant only after a positive biometric verification decision (review, observe).* *(ii) The issuer has alternate processes in place if biometric matches are not possible (review, observe).*	[FIPS201], Sec. 2.8 – PIV Card Issuance
AI-9	The issuer advises applicants in selecting a strong PIN value. The PIN is (i) a minimum of six digits in length, (ii) not easily guessable, (iii) not individually identifiable (e.g., part of a Social Security Number or phone number), and (iv) not commonly used (e.g., 000000, 123456). **Assessment** *Determine that:* *(i) The issuer has trained operators to advise applicants on PIN selection (review).*	[FIPS201], Sec. 4.3.1 – Activation by Cardholder

Identifier	Issuer Control	Source
	(ii) The operator advises applicants on the selection of a strong PIN (observe). *(iii) The PIN is a minimum of six digits in length (test).*	
AI-10	This control has been withdrawn as the PIV background investigation indicator extension identified by the id-piv-NACI object identifier is deprecated.	-
AI-12	The organization issues electromagnetically opaque holders or other technology to protect against unauthorized contactless access to information stored on a PIV Card. **Assessment** *Determine that:* *(i) Electromagnetically opaque holders or other technology is provided at the time of PIV Card issuance (review, observe).*	[FIPS201], Sec. 2.11 – PIV Privacy Requirements
AI-14	If pseudonyms are required to protect an employee or contractor (e.g., from physical harm, severe distress, or harassment), the issuance of a PIV Card uses agency-approved pseudonyms and follows normal procedures for PIV Card issuance. **Assessment** *Determine that:* *(i) The 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 the employees or contractors authorized to receive such pseudonyms (review).* (iii) *Issuance procedures for pseudonyms are consistent with procedures for issuing regular PIV Cards (review, observe).* *(iv) The use of a pseudonym has been authorized by the organization (review).*	[FIPS201], Sec. 2.8.1 – Special Rule for Pseudonyms

Table 18. Maintenance Process for PCIs

Identifier	Issuer Control	Source
MP-1	A post-issuance update applies to cases where one or more certificates, keys, biometric data records, or signed data objects are updated. Post-issuance updates do not modify the PIV Card expiration date, FASC-N, card UUID, or cardholder UUID. **Assessment** *Determine that:* *(i) Only certificates, keys, biometric data records, or signed data objects are updated during a post-issuance update (review, interview).* *(ii) The PIV Card expiration date, FASC-N, card UUID, or cardholder UUID are not modified post-issuance (review, interview).*	[FIPS201], Sec. 2.9.2 – PIV Card Post Issuance Update Requirements
MP-2	In the case of reissuance 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	[FIPS201], Sec. 2.9.1 – PIV Reissuance Requirements [FIPS201], Sec. 2.9.4 - PIV Card Termination Requirements

Identifier	Issuer Control	Source
	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 that the PIV Card cannot be collected (review, observe).*	
MP-3 (UPDATED)	During PIV Card reissuance and termination, (i) normal revocation procedures are completed within 18 hours of notification if the issued PIV Card cannot be collected and destroyed, and (ii) any databases maintained by the PIV Card issuer that indicate current valid (or invalid) FASC-N or card UUID values are updated to reflect the change in status. **Assessment** *Determine that:* *(i) Documentation includes the requirement that if a PIV Card cannot be collected and destroyed, normal revocation procedures are completed within 18 hours of notification (review).* *(ii) If the PIV Card cannot be collected and destroyed, normal revocation procedures are completed within 18 hours of notification (observe).* *(iii) Databases maintained by the issuer indicate that the FASC-N or card UUID values are updated to reflect the change in status (review, observe).*	[FIPS201], Sec. 2.9.1 – PIV Reissuance Requirements [FIPS201], Sec. 2.9.4 – PIV Card Termination Requirements
MP-4 (UPDATED)	During PIV Card termination, the following actions are taken: (i) the PIV Card is collected and destroyed; (ii) per OPM guidance, the Central Verification System is updated to reflect the change in status; and (iii) card management systems are updated to reflect the PIV Card termination and method of termination (e.g., PIV Card destruction for collected PIV Cards or certificate revocations for uncollected PIV Cards). **Assessment** *Determine that:* *(i) The PIV Card is collected and destroyed, if available (review, observe).* *(ii) The Central Verification System is updated to reflect the change in status (observe).* *(iii) Card management systems are updated to reflect the PIV Card termination and method of termination (review, observe).*	[FIPS201], Sec. 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 the PIV Card status. This information is distributed effectively throughout the systems used for physical and logical access to organizational facilities and resources. **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).*	Commonly accepted security readiness measures

Identifier	Issuer Control	Source
	(iii) The PIV Card termination status is distributed to all logical and physical access points, as applicable (test).	
MP-7	The organization has completed a life cycle 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 life cycle walkthrough to cover sponsorship, identity proofing, card production, activation/issuance, and maintenance processes (interview).* *(ii) Life cycle walkthroughs have been completed at one year intervals since the last authorization date (interview).* *(iii) The results of the issuer life cycle walkthrough have been documented and reviewed by the DAO (review, interview).*	SP 800-79, Sec. 5.4 – Monitoring Phase
MP-8	The intent of this control is covered by controls MP-18 and MP-19.	-
MP-9 (UPDATED)	The entire identity proofing, registration, and issuance process is repeated if the issuer does not maintain a PIV enrollment record that includes biometric data records for the cardholder. **Assessment** *Determine that:* *(i) The issuing facility completes the entire identity proofing, registration, and issuance process if they do not maintain a PIV enrollment record that includes biometric data records for the cardholder (review, observe).*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements
MP-10	Previously collected biometric data is not reused with the new PIV Card if the expiration date of the new PIV Card is more 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).*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements
MP-11	Post-issuance updates are performed (either with the issuer in physical custody of the PIV Card or remotely) 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 only occurs 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 endpoint entity other than the PIV Card issuer during the remote post-issuance update. **Assessment** *Determine that:* *(i) Post-issuance updates require all security controls to be implemented by the issuer and the issuer's information systems (review).*	[FIPS201], Sec. 2.9.2 – PIV Card Post Issuance Update Requirements
MP-12 (UPDATED)	When a PIN reset is performed in person at the issuing facility, the issuer performs a biometric verification before giving the reset PIV Card back to the cardholder to ensure that the cardholder's biometric characteristics elicit a positive biometric verification decision when compared to biometric data	[FIPS201], Sec. 2.9.3.1 – PIN Reset

Identifier	Issuer Control	Source
	records stored in the PIV enrollment record or when compared to the biometric data records on the PIV Card using the BIO-A or OCC-AUTH authentication mechanisms. If the biometric verification decision is negative or the cardholder's biometric characteristics are not successfully acquired, the cardholder provides another identity source document, and an attending operator inspects it and compares the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the card. **Assessment** *Determine that:* *(i) The reset PIV Card is released to the cardholder only after a positive biometric verification decision (review, observe).* *(ii) If the biometric verification decision is negative, the cardholder provides a primary identity source document that is compared to the electronic facial image retrieved from the enrollment data record and the photograph printed on the card (interview, observe).*	
MP-13 (UPDATED)	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 characteristics elicit a positive biometric verification decision when compared to biometric data records stored in the PIV enrollment record or when compared to the biometric data records on the PIV Card using the OCC-AUTH authentication mechanism. If the biometric verification decision is negative or the cardholder's biometric characteristics are not successfully acquired, the session is terminated, and the kiosk does not reset the PIV Card. **Assessment** *Determine that:* *(i) The reset PIV Card is only released to the cardholder after a positive biometric verification decision (review, observe).*	[FIPS201], Sec. 2.9.3.1 – PIN Reset
MP-14	Remote PIN reset on a general computing platform (e.g., desktop, laptop) is only performed 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 independent procedure (e.g., authenticating the cardholder with an associated derived PIV credential or by confirming reset via email to the on-record government-issued email address), and (iii) the cardholder's biometric characteristics elicit a positive biometric verification decision when compared to the stored biometric data records on the PIV Card through the OCC-AUTH authentication mechanism. **Assessment** *Determine that:* *(i) The PIV Card PIN is only reset after a positive biometric verification decision (observe).* *(ii) Remote PIN resets meet all security requirements to be implemented by the issuer and the issuer information systems (review, observe, test).*	[FIPS201], Sec. 2.9.3.1 – PIN Reset
MP-15	The intent of this control is covered by MP-21, MP-22, and MP-23.	-
MP-16 (NEW)	The issuer ensures that an adjudicative entity has authorized the issuance of the new PIV Card if the expiration date of the new PIV Card is later than the expiration date of the old card or if any data about the cardholder is being changed.	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements

Identifier	Issuer Control	Source
	Assessment *Determine that:* *(i) The issuance of the new PIV Card has been authorized (review).* *(ii) The issuer ensures that the adjudicative entity has verified that there is a PIV eligibility determination in an authoritative record in the IDMS or the Central Verification System (review).*	
MP-17 (NEW)	During reissuance, the issuer only releases the new PIV card to the applicant after a positive biometric verification decision using the BIO-A or OCC-AUTH authentication mechanisms. If the biometric verification decision is negative or if no biometric data records are available, the cardholder provides two identity source documents, and an attending operator inspects them and compares the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the new PIV Card. **Assessment** *Determine that:* *(i) The new PIV Card is only released to the applicant after a positive biometric verification decision (review, observe).* *(ii) If the biometric verification decision is negative or if no biometric data records are available, the cardholder provides two identity source documents that are compared to the electronic facial image retrieved from the enrollment data record and the photograph printed on the new PIV Card (interview, observe).*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements
MP-18 (NEW)	During reissuance of a PIV Card, the following actions are taken: (i) a new PIV authentication certificate and a new card authentication certificate are generated, (ii) the corresponding certificates are populated with the new FASC-N and card UUID, and (iii) a new digital signature key and associated certificate are generated for government-issued email accounts, while key management keys and associated certificates may be imported to the new PIV Card. **Assessment** *Determine that:* *(i) A new PIV authentication key and certificate and card authentication key and certificate are generated (review).* *(ii) A new FASC-N and card UUID are generated to be populated on the newly issued certificates (review).* *(iii) A new digital signature key and certificate are issued (to be used for government-issued email accounts) (review).* *(iv) A new key management key and certificate are issued, or old key management keys and certificates are imported on to the new PIV Card (review, observe).*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements
MP-19 (NEW)	In the event of a name change, the following actions are taken prior to the card issuer issuing a new PIV Card: (i) the cardholder notifies the issuer that their name has changed and presents the card issuer with evidence of a formal name change, and (ii) the card issuer notifies the respective adjudicative entity of the name change to ensure that appropriate records are updated unless the expiration date of the new card is no later than the expiration of the old card and no data other that the cardholder's name is being changed. **Assessment** *Determine that:* *(i) The cardholder presents the issuer with evidence of a formal name change (e.g., marriage certificate, divorce decree, judicial*	[FIPS201], Sec. 2.9.1 – PIV Card Reissuance Requirements

Identifier	Issuer Control	Source
	recognition of a name change, or any other mechanism permitted by state law or regulation) (review, observe). *(ii) The card issuer notifies the respective adjudicative entity of the name change to ensure that appropriate records are updated, if required (review).*	
MP-20 (NEW)	During a PIV Card activation reset, no more than 10 consecutive activation retries for each of the activation methods (i.e., PIN and OCC attempts) are permitted. **Assessment** *Determine that:* *(i) The issuer does not permit more than 10 consecutive activation retries when attempting to reset the PIN or OCC (review, observe).*	[FIPS201], Sec. 2.9.3 – PIV Card Activation Reset
MP-21 (NEW)	When a PIN reset is performed at a supervised remote identity proofing station, the issuer initiates a biometric verification to ensure that the cardholder's biometric characteristics captured at the station elicit a positive biometric verification decision when compared to biometric data records stored in the PIV enrollment record or when compared to the biometric data records on the PIV Card using the OCCAUTH authentication mechanism. If the biometric verification decision is negative or the cardholder's biometric characteristics are not successfully acquired, the cardholder provides another primary identity source document via the scanners and sensors integrated into the station. The remote operator inspects the document and compares the video feed of the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card. **Assessment** *Determine that:* *(i) All protections and requirements of* [FIPS201], *Sec. 2.7.1 are observed during the procedure (review, observe).* *(ii) The PIV Card PIN is only reset after a positive biometric verification decision (review, observe).* *(iii) If the biometric verification decision is negative, the cardholder provides another primary identity source document via the scanners and sensors integrated into the station. The remote operator inspects the document and compares the video feed of the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card (interview, observe).*	[FIPS201], Sec. 2.9.3 – PIV Card Activation Reset
MP-22 (NEW)	When an OCC reset is performed in person at the issuing facility, the issuer performs a biometric verification of the cardholder to the biometric data records in the PIV enrollment record before the reset. If the biometric verification decision is negative or no alternative biometric data records are available, the cardholder provides another primary identity source document, which is inspected and compared to the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card. **Assessment** *Determine that:* *(i) Both fingerprints used for OCC are replaced during an OCC reset (observe, test).* *(ii) The reset PIV Card is only released to the cardholder after a positive biometric verification decision (review, observe).*	[FIPS201], Sec. 2.9.3 – OCC Reset

Identifier	Issuer Control	Source
	(iii) If the biometric verification decision is negative or no alternative biometric data records are available, the cardholder provides another primary identity source document, which is inspected and compared to the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card (review, observe).	
MP-23 (NEW)	When an OCC reset is performed at a supervised remote identity proofing station, the operator initiates a biometric verification to ensure that the cardholder's biometric characteristics captured at the station elicit a positive biometric verification decision when compared to biometric data records stored in the PIV enrollment record or when compared to the biometric data records on the PIV Card using the BIO-A authentication mechanism. If the biometric verification decision is negative or the cardholder's biometric characteristics are not successfully acquired, the cardholder provides another primary identity source document via the scanners and sensors integrated into the station. The remote operator inspects the document and compares the video feed of the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card. **Assessment** *Determine that:* *(i) Both fingerprints used for OCC are replaced during an OCC reset (observe, test).* *(ii) All protections and requirements of* [FIPS201], *Sec. 2.7.1 are observed during the procedure (review, observe).* *(iii) The PIV Card OCC is only reset after a positive biometric verification decision (review, observe).* *(iv) If the biometric verification decision is negative, the cardholder provides another primary identity source document via the scanners and sensors integrated into the station. The remote operator inspects the document and compares the video feed of the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the PIV Card (interview, observe).*	[FIPS201], Sec. 2.9.3 – OCC Reset

G.2. Controls and Assessment Procedures for DPCIs

The following tables specify the controls and assessment procedures for derived PIV credential issuance. Unlike for a PIV Card issuer, not all controls are applicable to a derived PIV credential issuer as the issuance of a derived PIV credential is an instance of post-enrollment binding, which leverages the identity proofing and vetting associated with an existing PIV identity account. Certain issuer controls are only applicable to AAL2 or AAL3 derived PIV credentials and must therefore be implemented by the issuer only if they are issuing that level of a derived PIV credential. Similarly, certain issuer controls are applicable to PKI-based derived PIV credentials, while some are applicable to non-PKI-based derived PIV credentials. This is represented via the "applicability" columns, which identify whether the issuer control needs to be met by a PKI-based or non-PKI, AAL2, or AAL3 derived PIV credential issuer. If the "applicability" column states "DPCI," then the issuer control is applicable to all derived credential issuers, regardless of what type of derived PIV credential is issued by the issuer.

Table 19. Preparation and Maintenance of Documentation for DPCIs

Identifier	Issuer Control	Applicability	Source
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 (i) the list of issuer controls from* Appendix G.2, *(ii) the owner for each owner, (iii) a description of how the control is implemented, and (iv) whether the control is organization or facility-specific (review).* *(iii) Relevant operating procedures and associated documentation are referenced accurately (review).* *(iv) The operations plan has been reviewed and approved by the DAO within the organization (review, interview).*	DPCI	SP 800-79, Sec. 2.12 – Authorization Submission 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 (to include in-person, remote, or both) (review).* *(ii) The policy is consistent with the organization's mission and functions,* [FIPS201], [SP800-157], *and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The policy and procedures are approved by the federal department or agency (review).* *(iv) The organization periodically reviews and updates the policy and procedures as required (review, interview).*	DPCI	[SP800-157], Sec. 2 – Life Cycle Activities and Related Requirements [SP800-157], Sec. 2.2 – Initial Issuance

Identifier	Issuer Control	Applicability	Source
DO(DC)-5	The organization has a written policy and procedures that describe 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,* [FIPS201], [SP800-157]*, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The organization periodically reviews and updates the policy as required (review, interview).*	DPCI	[SP800-157], Sec. 2 – Life Cycle Activities and Related Requirements
DO(DC)-6	The organization has a written policy and procedures that describe the conditions for derived PIV credential maintenance. Maintenance activities include rekeying, the modification of certificates (if the authenticator is PKI-based), and the replacement of an activation factor (e.g., biometric or memorized secret), as appropriate. **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,* [FIPS201], [SP800-157]*, and applicable laws, directives, policies, regulations, standards, and guidance (review).* *(iii) The organization periodically reviews and updates the policy and procedures as required (review, interview).*	DPCI	[SP800-157], Sec. 2 –Life Cycle Activities and Related Requirements [SP800-157], Sec. 2.3 – Maintenance

2346

2347 **Table 20.** Assignment of Roles and Responsibilities for DPCIs

Identifier	Issuer Control	Applicability	Source
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 (review).* *(ii) The organization has assigned the role of senior authorizing official (review).*	DPCI	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities
RR(DC)-2	The organization has appointed the role of designated authorizing official (DAO). **Assessment** *Determine that*:	DPCI	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities

Identifier	Issuer Control	Applicability	Source
	(i) The organization has defined the role of designated authorizing official and its responsibilities according to the requirements of SP 800-79 (review). *(ii) The organization has assigned the role of designated authorizing official (review, interview).*		
RR(DC)-3	The organization has appointed the role of enterprise identity management official (EIMO). **Assessment** *Determine that*: *(i) the organization has defined the role of enterprise identity management official and its responsibilities according to the requirements of SP 800-79 (interview).* *(ii) The organization has assigned the role of enterprise identity management official (review, interview).*	DPCI	SP 800-79, Sec. 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 (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 offices directly responsible for the day-to-day operation of the organization (review, interview).*	DPCI	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities
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 (review).* *(ii) The organization has assigned the role of the privacy official (review).* *(iii) The privacy official does not have any other roles in the organization (review, interview).*	DPCI	[FIPS201], Sec. 2.11 – PIV Privacy Requirements SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities

Table 21. Facility and Personnel Readiness for DPCIs

Identifier	Issuer Control	Applicability	Source
FP(DC)-1	For hardware-based tokens issued in person, minimum physical controls at the issuing facility are implemented. These include (i) door locks and restricted access (e.g., use of locked rooms, safes, and lockable cabinets, as appropriate), (ii) secure issuance stations to ensure that no malicious code is introduced to compromise or otherwise impair the station and the derived PIV credential, (iii) security monitoring and automated alarms, (iv) emergency power and lighting, and (v) fire prevention and protection mechanisms.	DPCI	Commonly accepted security readiness measures

Identifier	Issuer Control	Applicability	Source
	Assessment *Determine that:* *(i) The EIMO and issuing facility managers are aware of the minimum set of physical controls that need to be in place at the facility (interview).* *(ii) The minimum physical security controls are implemented by the issuing facility (observe).* *(iii) The facility has a process to report any problems with the station to the issuer (review).*		
FP(DC)-2	Issuer documentation (e.g., operations plan, standard operating procedures, contracts, etc.) are maintained for issuing facilities. **Assessment** *Determine that:* *(i) The most current versions of issuer documentation are available for reference as needed (review, interview).*	DPCI	Commonly accepted security readiness measures
FP(DC)-3	The issuer develops, maintains, and securely stores a contingency/disaster recovery plan for information systems. **Assessment** *Determine that*: *(i) The contingency/disaster recovery plan is stored securely at the facility (interview, observe).* *(ii) The operations staff are knowledgeable about how to restore/reconstitute information systems in case of system failures (interview).*	DPCI	Commonly accepted security readiness measures
FP(DC)-4	The intent of this control is covered by DP(DC)-1.	-	-
FP(DC)-5	For in-person authenticator issuance and maintenance using stations, ensure that the stations are situated in an enclosed area (e.g., wall or partition) to provide privacy for the applicant and the operator. **Assessment** *Determine that*: *(i) Issuing facility stations are situated in an enclosed area (e.g., wall or partition) such that unauthorized individuals cannot see applicant information (observe).*	DPCI	Commonly accepted security readiness measures
FP(DC)-6	This control is withdrawn since M-11-11 has been rescinded.	-	-
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 (review, interview).*	DPCI	SP 800-79, Sec. 2.6 – Issuer Roles and Responsibilities Commonly accepted security readiness measures

Identifier	Issuer Control	Applicability	Source
	(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).		
FP(DC)-8	All pre-personalized, unissued physical authenticators from vendors are only received by authorized personnel who ensure that these authenticators are stored, handled, and disposed of securely at the issuing facility. **Assessment** *Determine that*: *(i) The issuing facility has an authorized list of personnel who are responsible for ensuring that authenticator stock is received and stored securely (interview).* *(ii) The procedures for receiving, storing, and destroying authenticators are documented in the issuing facility's standard operating procedures (review).* *(iii) Authorized personnel are knowledgeable about the procedures on how to receive, store, and destroy the authenticators (interview).*	DPCI	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 (i.e., physical authenticators) 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, interview).*	DPCI	Commonly accepted security readiness measures

Table 22. Protection of Stored and Transmitted Data for DPCIs

Identifier	Issuer Control	Applicability	Source
ST(DC)-1 (UPDATED)	The issuer PIV information systems are implemented in accordance with the spirit and letter of all federal privacy laws and policies, including the E-Government Act of 2002 [E-GOV], the Privacy Act of 1974 [PRIVACY], and OMB [M-03-22], as applicable. **Assessment** *Determine that*: *(i) PIV information systems are operated and managed in accordance with federal privacy laws and applicable organizational policies (review).* *(ii) The organization does not disclose any record that 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 or one of the exceptions for disclosure in the Privacy Act are met (review, interview).*	DPCI	[FIPS201], Sec. 2.11 – PIV Privacy Requirements E-Government Act [E-GOV] Privacy Act [PRIVACY] OMB Memorandum [M-03-22]

Identifier	Issuer Control	Applicability	Source
	(iii) Individuals are permitted to gain access to their personal record (i.e., in the PIV identity account), and the information is provided in a form that is comprehensible to them (review, interview). *(iv) 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).* *(v) 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).*		
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	[FIPS201], Sec. 2.11 – PIV Privacy Requirements [SP800-157], Sec. 2.2 – Initial Issuance

Table 23. Enforcement of Privacy Requirements for DPCIs

Identifier	Issuer Control	Applicability	Source
PR(DC)-1	Privacy act statements/notices, complaint procedures, appeals procedures for those denied derived PIV credentials or whose credentials are revoked, and sanctions for employees who violate 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*: *(iii) The issuing facility posts privacy act statements/notices, complaint procedures, appeals procedures for those denied a token or whose token is revoked, and sanctions for employees who violate privacy policies (interview, review).* *(iv) The organization maintains appeal procedures for those who are denied a derived PIV credential or whose credentials are revoked (review).*	DPCI	OMB Memorandum [M-05-24]
PR(DC)-2 (UPDATED)	The organization conducts a comprehensive privacy impact assessment (PIA) and a periodic review and update of the assessment on systems that contain PII for the purpose of implementing derived PIV credentials in a manner consistent with the methodology of [E-GOV] and the requirements of [M-03-22]. **Assessment** *Determine that:*	DPCI	[FIPS201], Sec. 2.11 – PIV Privacy Requirements E-Government Act [E-GOV] OMB Memorandum [M-03-22]

Identifier	Issuer Control	Applicability	Source
	(i) The organization conducts a privacy impact assessment of their issuer information systems based on guidance found in [E-GOV] *and* [M-03-22] *(review).* *(ii) The organization submits the privacy impact assessment of their issuer information systems to OMB (interview, review).*		
PR(DC)-3	The organization's employee and contractor identification SORNs 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 [PRIVACY] and OMB Circular [A-130], Appendix 1. **Assessment** *Determine that:* *(i) The organization updates SORNs to reflect changes in the disclosure of information (review, interview).*	DPCI	Privacy Act [PRIVACY] OMB Memorandum [M-05-24]
PR(DC)-4 (UPDATED)	The organization writes, publishes, and maintains a clear and comprehensive list of the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the derived PIV credential, how the information will be protected, and the complete set of uses of the derived PIV credential and related information. **Assessment** *Determine that:* *(i) Before receiving the derived PIV credential, the issuer requires the applicant to be notified of the PII 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 the information (review, observe).* *(ii) The applicant is informed of what PII 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	[FIPS201], Sec. 2.11 – PIV Privacy Requirements
PR(DC)-5	The issuer employs technologies that allow for the 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 PII (interview, test).*	DPCI	[FIPS201], Sec. 2.11 – PIV Privacy Requirements

2355 **Table 24.** Deployed Products and Information Systems for DPCIs

Identifier	Issuer Control	Applicability	Source
DP(DC)-1	Issuer PIV information systems are authorized to operate in accordance with [SP800-37] in order to be compliant with the provisions of OMB Circular [A-130], App III. The controls described in [SP800-53] are used to accomplish security and privacy goals, where applicable. **Assessment** *Determine that:* *(i) The organization has a letter showing the current authorization decision for each information system used to support the issuer (review).*	DPCI	[FIPS201], Appendix A.2 – Application of Risk Management Framework to IT System(s) Supporting PCI [FIPS201], Sec. 2.11 – PIV Privacy Requirements
DP(DC)-2	Products and services utilized by an issuing facility to issue derived PIV credentials are listed on the GSA FIPS 201 Evaluation Program's Approved Products List (APL), where applicable.[11] **Assessment** *Determine that:* *(i) The presence (i.e., make, model, versions) of each product or service that falls within one of the categories in the FIPS 201 Evaluation Program is checked on the APL (review).* *(ii) There is no product in operation that has been moved to the GSA FIPS 201 Evaluation Program Removed Products List (RPL).*	DPCI	OMB Memorandum [M-05-24] Federal Acquisition Regulation (FAR), Sec. 4.1302 – Acquisition of Approved Products and Services for Personal Identity Verification
DP(DC)-3	This control has been withdrawn as OMB Memorandum M-07-06 has been rescinded.	-	-
DP(DC)-4 (NEW)	PKI-based derived PIV credentials issued at AAL2 meet the requirements for phishing resistance defined in [SP800-63B], Sec. 5.2.5. **Assessment** *Determine that:* *(i) The organization establishes blanket approvals for particular device types that meet AAL2 requirements (interview).* *(ii) Either a multi-factor cryptographic device authenticator or a multi-factor cryptographic software authenticator as specified in* [SP800-63B]*, Sec. 5.1.8.1 is used for derived PIV authentication at AAL2 (review, interview).* *(iii) For a specific devices or authenticators issued to a cardholder, the organization has a documented policy and procedure for approval and issuance (review, interview).*	PKI-AAL2	[SP800-157], Sec. 2.2 – Initial Issuance [SP800-157], Sec. 3.1.3 – Allowable Authenticator Types
DP(DC)-5 (NEW)	Non-PKI based derived PIV credentials issued at AAL2 meet the requirements for phishing resistance defined in [SP800-63B], Sec. 5.2.5. **Assessment** *Determine that:* *(i) The organization establishes blanket approvals for particular device types that meet AAL2 requirements (interview).*	Non-PKI-AAL2	[SP800-157], Sec. 2.2 – Initial Issuance [SP800-157], Sec. 3.2.1 – Allowable Authenticator Types

[11] This control will be applicable when the test requirements and tools for testing and approving derived PIV credentials are available through the GSA FIPS 201 Evaluation Program.

Identifier	Issuer Control	Applicability	Source
	(ii) A cryptographic device authenticator or a multi-factor cryptographic software authenticator as specified in [SP800-63B], *Sec. 5.1.8.1, or a single-factor cryptographic software authenticator as specified in* [SP800-63B], *Sec. 5.1.6.1 is used for derived PIV authentication at AAL2 (review, interview).* *(iii) For specific devices or authenticators issued to a cardholder, the organization has a documented policy and procedure for approval and issuance (review, interview).*		
DP(DC)-6 (NEW)	PKI-based derived PIV credentials issued at AAL3 meet the requirements for phishing resistance defined in [SP800-63B], Sec. 5.2.5. **Assessment** *Determine that:* *(i) The organization establishes blanket approvals for particular device types that meet AAL3 requirements (interview).* *(ii) A multi-factor cryptographic device authenticator as specified in* [SP800-63B], *Sec. 5.1.9.1 is used for derived PIV authentication at AAL3 (review, interview).* *(iii) For specific devices or authenticators issued to a cardholder, the organization has a documented policy and procedure for approval and issuance (review, interview).*	PKI-AAL3	[SP800-157], Sec. 2.2 – Initial Issuance [SP800-157], Sec. 3.1.3 – Allowable Authenticator Types
DP (DC)-7 (NEW)	Non-PKI-based derived PIV credentials issued at AAL3 meet the requirements for phishing resistance defined in [SP800-63B], Sec. 5.2.5. **Assessment** *Determine that:* *(i) The organization establishes blanket approvals for particular device types that meet AAL3 requirements (interview).* *(ii) Either a multi-factor cryptographic device authenticator as specified in* [SP800-63B], *Sec. 5.1.9.1 or a single-factor cryptographic device authenticator as specified in* [SP800-63B], *Sec. 5.1.7.1 is used for derived PIV authentication at AAL3 (review, interview).* *(iii) For specific devices or authenticators issued to a cardholder, the organization has a documented policy and procedure for approval and issuance (review, interview).*	Non-PKI-AAL3	[SP800-157], Sec. 2.2 – Initial Issuance [SP800-157], Sec. 3.2.1 – Allowable Authenticator Types
DP (DC)-8 (NEW)	The applicant is provided with or needs to supply an approved physical authenticator for the highest AAL that the derived PIV credential will be used to authenticate. If the authenticator is not directly provided by the issuer, the issuer verifies that the authenticator's characteristics (e.g., single-factor or multi-factor) meet the requirements of [SP800-63B] for the highest authentication assurance level at which it will be used (AAL2 or AAL3), including [FIPS140] requirements. **Assessment** *Determine that:* *(i) The organization establishes approved authenticator characteristics (review, interview).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 2.2.2 – Non-PKI-based Derived PIV Credential Issuance

Identifier	Issuer Control	Applicability	Source
	(ii) Authenticator characteristics meet the requirements of [SP800-63B] *and* [FIPS140] *for the highest authentication level at which it will be used (review).*		

2356

2357 **Table 25.** Implementation of Credentialing Infrastructures for DPCIs

Identifier	Issuer Control	Applicability	Source
CI(DC)-2 (UPDATED)	Derived PIV authentication certificates are issued under the id-fpki-common-derived-pivAuth-hardware 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 at AAL3 (review).* *(ii) Derived PIV authentication certificates comply with the derived PIV authentication certificate profile (review).* *(iii) Cryptographic algorithms and key sizes are based on* [SP800-78] *(review).*	PKI-AAL3	[SP800-157], Sec. 3.1.1 – Certificate Policies for Derived PIV Credentials [SP800-157], Sec. 3.1.2 – Cryptographic Specifications
CI(DC)-11	For derived PIV authentication certificates issued under id-fpki-common-derived-pivAuth-hardware, the derived PIV authentication key pair is generated within a hardware cryptographic module that meets the requirements of [SP800-63B], Sec. 4.2.2, including being validated to [FIPS140] Level 2 or higher, providing Level 3 physical security to protect the derived PIV authentication private key while in storage, and not permitting the private key to be exported. **Assessment** *Determine that:* *(i) The organization ensures that derived PIV authentication certificates issued under id-fpki-common-derived-pivAuth-hardware certificate policy are generated on cryptographic modules the meet the requirements of* [SP800-63B], *Sec. 4.2.2 and validated against* [FIPS140] *at Level 2 or higher with Level 3 physical security (review).* *(ii) The keypair is generated in the device (authenticator or endpoint) that will house the derived PIV credential (interview, test).*	PKI-AAL3	[SP800-157], Sec. 2.2.1 – PKI-Based Derived Credential Issuance [SP800-157], Sec. 3.1.2 – Cryptographic Specifications
CI(DC)-12	For derived PIV authentication certificates issued under id-fpki-common-derived-pivAuth, the derived PIV authentication key pair is generated within a cryptographic module that has been validated to [FIPS140] Level 1 or higher. **Assessment** *Determine that:* *(i) The organization ensures that derived PIV authentication certificates issued under id-fpki-common-derived-pivAuth certificate policy are generated on* [FIPS140]*-validated cryptographic modules or higher (review).* *(ii) If the key pair is generated outside of the authenticator itself, the private key is transferred via an authenticated*	PKI-AAL2	[SP800-157], Sec. 3.1.2 – Cryptographic Specifications

Identifier	Issuer Control	Applicability	Source
	protected channel as defined in [SP800-63B]*, and the authenticator meets the requirements of* [SP800-63B], *Sec. 4.2.2, including being validated to* [FIPS140] *Level 1 or higher (review).*		
CI(DC)-13 (UPDATED)	Binding a derived PIV credential to a PIV identity account is accomplished through a connection to a PIV-authenticated endpoint, a direct connection to the PIV Card, or the use of the external authenticator binding procedure, as described in [SP800-63B], Sec. 6.1.2.4. In all cases, binding SHALL require the use of the PIV-AUTH authentication mechanism specified in [FIPS201]. **Assessment** *Determine that:* *(i) The organization has implemented a method to bind the derived PIV credential to the PIV identity account (review).* *(ii) Binding of the derived PIV credential to the PIV identity account uses the PIV-AUTH mechanism (observe).*	DPCI	[SP800-157], Sec. 3.3 – Binding Derived PIV Credentials
CI(DC)-14	The issuer retains the biometric sample used to verify the applicant for future reference. **Assessment** *Determine that:* *(i) The issuer has implemented a process/system to retain the applicant's biometric data for maintenance of the derived PIV Credential (review).*	DPCI	[SP800-157], Sec. 2.2 – Initial Issuance
CI(DC)-18 (NEW)	Derived PIV authentication certificates are issued under the id-fpki-common-derived-pivAuth 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).* *(ii) Derived PIV authentication certificates comply with the derived PIV authentication certificate profile (review).* *(iii) Cryptographic algorithms and key sizes are based on* [SP800-78] *(review).*	PKI-AAL2	[SP800-157], Sec. 3.1.1 – Certificate Policies for Derived PIV Credentials [SP800-157], Sec. 3.1.2 – Cryptographic Specifications
CI(DC)-19 (NEW)	Once the applicant is authenticated and the derived PIV credential is issued, it is represented in the cardholder's PIV identity account. **Assessment** *Determine that:* *(i) The issuance of a derived PIV credential is recorded in the PIV identity account for the cardholder (review, observe, test).*	DPCI	[SP800-157], Sec. 2.2 – Initial Issuance

Identifier	Issuer Control	Applicability	Source
CI(DC)-20 (NEW)	Authenticators used as non-PKI-based derived PIV credentials meet the cryptographic requirements specified in [SP800-63B], Sec. 5.1 for the corresponding authenticator type. **Assessment** *Determine that:* *(i) The authenticator used for non-PKI-based derived PIV credentials meet the cryptographic requirements in* [SP800-63B]*, Sec. 5.1 (review, test).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 3.2.2 – Cryptographic Specifications

2358

2359 **Table 26.** Sponsorship Process for DPCIs

Identifier	Issuer Control	Applicability	Source
SP(DC)-1	A derived PIV credential is issued only upon request by a proper authority. **Assessment** *Determine that:* *(i) The process for making a request is documented (review).* *(ii) A derived PIV credential is issued only by the home agency of the associated PIV identity account (review, interview).* *(iii) A request from a valid authority is made in order to issue a derived PIV credential (observe).*	DPCI	[FIPS201], Sec. 2.1 –Control Objectives [SP800-157], Sec. 2.2 – Initial Issuance
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) The forms used to collect personal information have been approved by OMB (review, observe).*	DPCI	Paperwork Reduction Act [PAPER-RED]

2360

2361 **Table 27.** Identity Proofing/Registration Process for DPCIs

Identifier	Issuer Control	Applicability	Source
EI(DC)-1	This control is withdrawn as there are no identity-proofing requirements for issuing derived PIV credentials.	-	-

2362

2363 **Table 28.** Activation/Issuance Process for DPCIs

Identifier	Issuer Control	Applicability	Source
AI(DC)-5 (UPDATED)	A mechanism to block use of the derived PIV credential after a number of consecutive failed authentication attempts using the memorized secret is implemented. **Assessment** *Determine that:* *(i) The implementation can block use of the derived PIV credential if the number of consecutive failed*	DPCI	[SP800-157], Sec. 3.1.4 – Activation Data [SP800-157], Sec. 3.2.3 – Activation Data

Identifier	Issuer Control	Applicability	Source
	attempts to activate the memorized secret has exceeded that set by the issuer (test, observe).		
AI(DC)-16	This control is withdrawn. Requirements for issuance over multiple transactions is covered by AI(DC)-18.	-	-
AI(DC)-17 (UPDATED)	A derived PIV credential at AAL3 is issued after verifying that the applicant is currently eligible to possess a PIV Card by (i) performing the PKI-AUTH authentication mechanism described in Sec. 6.2.3.1 of [FIPS201] and (ii) identifying themselves using a biometric sample that can be verified against their PIV Card or the biometric information in their enrollment record. **Assessment** *Determine that:* *(i) The issuer has a documented process in place to verify the identity of the applicant (review).* *(ii) Derived PIV credentials at AAL3 are issued in accordance with* [SP800-63B]. *Sec. 6.1.2.1 (review, interview, observe).*	PKI-AAL3, Non-PKI-AAL3	[SP800-157], Sec. 2.2 – Initial Issuance
AI(DC)-18 (UPDATED)	If the issuance of a derived PIV credential at AAL3 consists of two or more transactions, the applicant identifies themselves using a biometric sample that can be verified against either their PIV Card or a biometric sample that was recorded in a previous transaction. **Assessment** *Determine that:* *(i) The issuer retains the biometric sample for future reference. The retained biometric is used to verify the applicant (review, interview, observe).* *(ii) The issuing facility verifies the identity of the applicant by using a biometric sample that can be verified against their PIV Card or a biometric that was recorded in a previous transaction (review, observe).*	PKI-AAL3, Non-PKI-AAL3	[SP800-157], Sec. 2.2 – Initial Issuance
AI(DC)-19 (NEW)	The issuer notifies the PIV cardholder of the binding of a derived PIV credential through independent means that would not afford an attacker the opportunity to interfere with the notification. **Assessment** *Determine that:* *(i) The issuer has a process to notify the PIV cardholder of the binding of a derived PIV credential (review).* *(ii) The method of notification does not provide an attacker with an opportunity to interfere with the notification (review, observe).*	DPCI	[SP800-157], Sec. 2.2 – Initial Issuance
AI(DC)-20 (NEW)	Activation using a biometric characteristic meets the requirements of [SP800-63B], Sec. 5.2.3. **Assessment** *Determine that:* *(i) Activation of the biometric characteristic meets the requirements of* [SP800-63B], *Sec. 5.2.3 (review, interview).*	DPCI	[SP800-157], Sec. 3.1.4 – Activation Data [SP800-157], Sec. 3.2.3 – Activation Data

Identifier	Issuer Control	Applicability	Source
	(ii) The applicant is able to successfully activate the derived PIV authenticator using the biometric characteristic (observe, test).		
AI(DC)-21 (NEW)	Unlocking the device that houses a derived PIV authenticator (e.g., mobile phone) is not considered activation of the authenticator. A separate entry of the activation secret or presentation of a biometric factor is performed to use the authenticator. **Assessment** *Determine that:* *(i) A separate entry of the activation secret or presentation of a biometric factor is performed to use the authenticator (observe, test).*	DPCI	[SP800-157], Sec. 3.1.4 – Activation Data [SP800-157], Sec. 3.2.3 – Activation Data
AI(DC)-22 (NEW)	A derived PIV credential at AAL2 is issued after verifying that the applicant is currently eligible to possess a PIV Card by performing the PKI-AUTH authentication mechanism described in Sec. 6.2.3.1 of [FIPS201]. **Assessment** *Determine that:* *(i) The issuer has a documented process in place to verify the identity of the applicant (review).* *(ii) Derived PIV credentials are issued in accordance with* [SP800-63B]*, Sec. 6.1.2.1 (review, interview, observe).*	PKI- AAL2, Non-PKI-AAL2	[SP800-157], Sec. 2.2 – Initial Issuance
AI(DC)-23 (NEW)	Activation of the derived PIV authenticator using a memorized secret meets the requirements of [SP800-63B], Sec. 5.2.11. **Assessment** *Determine that:* *(i) Activation of the memorized secret meets the requirements of* [SP800-63B]*, Sec. 5.2.11 (review, interview).* *(ii) The applicant is able to successfully activate the derived PIV authenticator using the established memorized secret (observe, test).*	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 3.1.4 – Activation Data
AI(DC)-24 (NEW)	The applicant is prompted to establish a memorized secret or biometric activation factor (or both) for a multi-factor authenticator and successfully authenticate using the authenticator. **Assessment** *Determine that:* *(i) A process to authenticate to a multi-factor authenticator is established (review, interview).* *(ii) The applicant is able to establish a memorized secret, a biometric activation factor, or both and successfully authenticate to the authenticator (observe, test).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 2.2.2 – Non-PKI-Based Derived PIV Credential Issuance
AI(DC)-25 (NEW)	The applicant is prompted to register a memorized secret that meets the requirements of [SP800-63B], Sec. 5.1.1 for a single-factor authenticator that will be verified along with the physical authenticator during the authentication process. **Assessment**	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 2.2.2 – Non-PKI-Based Derived PIV Credential Issuance

Identifier	Issuer Control	Applicability	Source
	Determine that: *(i) A process to register a memorized secret that meets the requirements of* [SP800-63B]*, Sec. 5.1.1 is established (review, interview).* *(ii) The applicant is able to register a memorized secret that meets the requirements of* [SP800-63B]*, Sec. 5.1.1 and successfully authenticate to the authenticator (observe, test).*		
AI(DC)-26 (NEW)	Activation of a multi-factor authenticator being used as a derived PIV credential using a memorized secret SHALL meet the requirements of [SP800-63B], Sec. 5.2.11. **Assessment** *Determine that:* *(i) Activation of the multi-factor authenticator meets the requirements of* [SP800-63B]*, Sec. 5.2.11 (review, interview).* *(ii) The applicant is able to successfully activate the multi-factor authenticator using the established memorized secret (observe, test).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 3.2.3 – Activation Data

Table 29. Maintenance Process for DPCIs

Identifier	Issuer Control	Applicability	Source
MP(DC)-2 (UPDATED)	When an authenticator that contains the private key corresponding to a PKI-based derived PIV credential is lost, stolen, or damaged, the issuer prevents further use of the affected credential by either collecting and destroying the associated private key or by revoking the associated certificate. **Assessment** *Determine that:* *(i) In the case of lost, stolen, damaged, or compromised credentials, the issuer has processes in place to collect the authenticator and destroy the private key or revoke the associated authentication certificate (review, observe, test).*	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 2.1 – Derived PIV Credential Life Cycle Activities [SP800-157], Sec. 2.4.1 – PKI-Based Derived PIV Credential Invalidation
MP(DC)-3 (NEW)	When a non-PKI-based derived PIV credential is lost, stolen, or damaged, the issuer invalidates the credential to prevent its further use. **Assessment** *Determine that:* *(i) In the case of lost, stolen, damaged, or compromised credentials, the issuer has processes in place to invalidate the use of the credential so that it cannot be used to authenticate (review, observe, test).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 2.1 – Derived PIV Credential Life Cycle Activities [SP800-157], Sec. 2.4.2 – Non-PKI-Based Derived PIV Credential Invalidation

Identifier	Issuer Control	Applicability	Source
MP(DC)-5	Upon derived PIV credential invalidation, the organization enforces a standard methodology for updating the PIV identity account to indicate the derived PIV credential status. **Assessment** *Determine that:* *(i) The issuer has procedures to update the PIV identity account to indicate derived PIV credential invalidation (review).*	DPCI	[SP800-157], Sec. 2.4 – Invalidation
MP(DC)-7	The organization has completed a life cycle 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 life cycle walkthrough to cover initial issuance, maintenance, and termination processes (interview).* *(ii) A life cycle walkthrough has been completed at one year intervals since the last authorization date (interview).* *(iii) The results of the issuer life cycle walkthrough have been documented and reviewed by the DAO (review, interview).*	DPCI	SP 800-79, Sec. 5.4 – Monitoring Phase
MP(DC)-11	When certificate rekeying or modification is performed remotely for a derived PIV credential, communication between the issuer and the cryptographic module in which the derived PIV authentication private key is stored occurs only over mutually authenticated secure sessions between tested and validated cryptographic modules. **Assessment** *Determine that:* *(i) Remote updates for certificate rekeying and the modification of a derived PIV authentication certificate meet all required security controls to be implemented by the issuer and the issuer information systems (review).*	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 2.3.1 - PKI-Based Derived PIV Credential Maintenance
MP(DC)-12	The intent of this control is covered by MP(DC)-22 and MP(DC)-23.	-	-
MP(DC)-13	The intent of this control is covered by MP(DC)-22 and MP(DC)-23.	-	-
MP(DC)-16	Reissuance of derived PIV credentials in cases of expiration, loss, damage, or compromise is performed in accordance with the initial issuance process. **Assessment** *Determine that:* *(i) The issuer follows the initial issuance process while reissuing a derived PIV credential in cases of expiration, loss, damage, or compromise (review, observe).*	DPCI	[SP800-157], Sec. 2.3 – Maintenance
MP(DC)-17	If the derived PIV authentication private key was created and stored on a hardware cryptographic token that permits export of the private key, then the derived PIV authentication certificate is revoked upon termination, even if the token is collected and either zeroized or destroyed.	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 2.4.1 – PKI-Based Derived PIV Credential Invalidation

Identifier	Issuer Control	Applicability	Source
	Assessment *Determine that:* *(i) The issuer has developed and follows compliant processes to terminate derived PIV credentials (review, observe).*		
MP(DC)-18 (UPDATED)	All derived PIV credentials associated with a given PIV Card are invalidated when the associated PIV identity account is terminated. **Assessment** *Determine that:* *(i) The issuer has implemented a process to invalidate all issued derived PIV credentials when the PIV identity account is terminated (review, test).* *(ii) The issuer continuously monitors the associated PIV identity account to determine its termination status (review).*	DPCI	[SP800-157], Sec. 2.4 – Invalidation
MP(DC)-19 (NEW)	If the subscriber's PIV Card is reissued as a result of a change in the subscriber's name and the subscriber's name appears in the derived PIV authentication certificate, a new derived PIV authentication certificate is issued with the new name, and the previous certificate is invalidated. **Assessment** *Determine that:* *(i) The issuer has procedures for updating a derived PIV authentication certificate as part of a reissuance of a subscriber's PIV Card (review, observe).* *(ii) The existing derived PIV authentication certificate is revoked (review, observe, test).*	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 2.3.1 – PKI-Based Derived PIV Credential Maintenance
MP(DC)-22 (NEW)	If the activation secret is forgotten or the permitted number of consecutive wrong attempts is reached, the organization is required to input the PIN unblocking key (PUK). If the PUK is not implemented by the authenticator or cannot be provided, the authenticator certificates are revoked, or the associated private keys are destroyed or zeroized. **Assessment** *Determine that:* *(i) The PIN unblocking key is entered if the maximum number of consecutive wrong attempts is reached prior to resetting the memorized secret or the biometric activation factor (review, observe, test).* *(ii) If the PIN unblocking key cannot be entered, the authentication certificates are revoked, or the private keys are zeroized or destroyed (observe, test).*	PKI-AAL2, PKI-AAL3	[SP800-157], Sec. 3.1.4 – Activation Data
MP(DC)-24 (NEW)	If the memorized secret used for activation or the biometric activation factor needs to be changed, entry of the current memorized secret is required to change the value. **Assessment** *Determine that:* *(i) Entry of the current activation secret is required prior to changing the memorized secret or the biometric activation factor (review, observe, test);*	DPCI	[SP800-157], Sec. 3.1.4 – Activation Data [SP800-157], Sec. 3.2.3 – Activation Data

Identifier	Issuer Control	Applicability	Source
MP(DC)-25 (NEW)	Invalidation of a derived PIV credential is accomplished by invalidating the reference to the associated authenticator in the PIV identity account so that the authenticator cannot be used any longer. **Assessment** *Determine that:* *(i) The issuer has developed and follows compliant processes to terminate derived PIV credentials (review, observe).* *(ii) Hardware-based authenticators (if used) are collected from the subscriber (observe).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 2.4.2 – Non-PKI-Based Derived PIV Credential Invalidation
MP(DC)-26 (NEW)	If the activation secret is forgotten or the permitted number of consecutive wrong attempts is reached, the activation secret and attempt counter can be reset by centralized management at the home agency. If centralized reset is not available, the authenticator is reset and will require rebinding to the PIV identity account. **Assessment** *Determine that:* *(i) The organization has a method to reset the activation secret and the attempt counter (review, observe, test).* *(ii) If the activation secret and the attempt counter cannot be reset, the authenticator is reset and bound to the PIV identity account (observe, test).*	Non-PKI-AAL2, Non-PKI-AAL3	[SP800-157], Sec. 3.2.3 – Activation Data

2366

Appendix H. Assessment and Authorization Tasks

Table 30. Initiation Phase, Task 1: Preparation

Subtask	Role(s) Responsible
Subtask 1.1: Confirm that the operations of the issuer is fully described and documented in an operations plan.	EIMO
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.	EIMO, Issuing Facility Manager

Table 31. Initiation Phase, Task 2: Resource identification

Subtask	Role(s) Responsible
Subtask 2.1: Identify the SAO, DAO, PO, issuing facility managers, assessor, and other key personnel at the facility level who are performing functions, such as identity proofing/registration, card/token production, and activation/issuance (of the PIV Card or derived PIV credential). Maintenance personnel also need to be contacted to provide requested assessment information to the assessor.	EIMO
Subtask 2.2: Determine the authorization boundary for the issuer.	EIMO, DAO
Subtask 2.3: Determine the resources and the time needed for the assessment of the issuer, and prepare a plan to execute the assessment.	EIMO, Assessor, DAO

Table 32. Initiation Phase, Task 3: Operations plan analysis and acceptance

Subtask	Role(s) Responsible
Subtask 3.1: Review the list of required issuer controls documented in the organization's issuer operations plan, and confirm that they have been implemented properly.	DAO, EIMO
Subtask 3.2: Analyze the operations plan to determine whether there are deficiencies in satisfying all of the policies, procedures, and other requirements in [FIPS201] that could result in a DATO being issued. After discussing the discovered deficiencies in the documentation and operations plan with the EIMO, 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 either authorizes continuation of the assessment or terminates the assessment effort, depending on the evaluation of the issuer's ability to address the deficiencies.	DAO, EIMO
Subtask 3.3: Verify that the operations plan is acceptable	DAO

2371 **Table 33.** Assessment Phase, Task 4: Issuer control assessment

Subtask	Role(s) Responsible
Subtask 4.1: Review the suggested and selected assessment methods for each issuer control in preparation for the assessment.	Assessor
Subtask 4.2: Assemble all documentation and the supporting materials necessary for the assessment of the issuer. If these documents include previous assessments, review the findings, and determine whether they are applicable to the current assessment.	EIMO, Assessor
Subtask 4.3: Assess the required issuer controls using the prescribed assessment procedures found in Appendices G.1 and G.2 based on the scope of the issuance functions.	Assessor
Subtask 4.4: Prepare the assessment report.	Assessor

2372 **Table 34.** Assessment Phase, Task 5: Assessment documentation

Subtask	Role(s) Responsible
Subtask 5.1: Provide the EIMO with the assessment report.	Assessor
Subtask 5.2: Revise the operations plan (if necessary), and implement its new provisions.	EIMO
Subtask 5.3: Prepare the CAP	EIMO
Subtask 5.4: Assemble the authorization submission package, and submit it to the DAO.	EIMO

2373 **Table 35.** Authorization Phase, Task 6: Authorization decision

Subtask	Role(s) Responsible
Subtask 6.1: Review the authorization decision package to see if it is complete and if all applicable issuer controls are fully assessed using the designated assessment procedures.	DAO
Subtask 6.2: Determine whether the risk to the organization's operations, assets, or potentially affected individuals is acceptable.	DAO
Subtask 5.3: Share the authorization package with an independent party for review, and arrive at an authorization decision	DAO

2374 **Table 36.** Authorization Phase, Task 7: Authorization documentation

Subtask	Role(s) Responsible
Subtask 7.1: Provide copies of the authorization decision package in either paper or electronic form to the EIMO and any other organization officials who have interests, roles, or responsibilities in the issuer's operations.	DAO

Subtask	Role(s) Responsible
Subtask 7.2: Update the operations plan.	EIMO

Table 37. Monitoring Phase, Task 8: Operations plan update

Subtask	Role(s) Responsible
Subtask 8.1: Document all relevant changes in the issuance processes within the operations plan.	EIMO
Subtask 8.2: Analyze the proposed or actual changes to the issuer, and determine the impacts of such changes.	EIMO

Table 38. Monitoring Phase, Task 9: Annual life cycle walkthrough

Subtask	Role(s) Responsible
Subtask 9.1: Observe all of 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 needs to be repeated using randomly selected issuing facilities.	EIMO (or designated appointee)
Subtask 9.2: The results of the life cycle walkthrough are summarized in a report to the DAO. The report highlights any deficiencies and the corrective actions that need to be implemented to correct those deficiencies.	EIMO, DAO

Appendix I. Revision History

Version	Release Date	Updates
SP 800-79	July 2005	Initial Release
SP 800-79-1	June 2008	The major changes for this revision include: • Removal of attributes as the basis of reliability assessment, and replacing them with PCI controls, traceable to specific requirements from FIPS 201-1 and related documents; • Additional guidelines on how to determine the accreditation boundaries of a PCI; • Discussion of the risk involved in authorizing the operation of a PCI; • Removal of "Section 4.0 - PCI Functions and Operations" and "Section 5.0 - PIV Services and Operations," which were narrative discussions of FIPS 201-1 requirements; • Clarification of the similarities and differences between the accreditation of computer systems for secure operation as specified in SP 800-37 and the accreditation of the reliability of an organization as specified in SP 800-79-1; • Changing the term "certification" to "assessment"; and • Use of "organization" instead of "department" or "agency.
SP 800-79-2		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; • Provided detailed controls to address post-issuance updates for PIV Cards; • Updated references to more recent credentialing guidance issued by Office of Personnel Management (OPM); • Addition of issuer controls with respect to the chain-of-trust records maintained by a PIV Card issuer; and

Version	Release Date	Updates
		• Modified process to include an independent review prior to authorization of issuer.

SP 800-79-3	[Insert Date]	The major changes for this revision include additions and updates to issuer controls in response to new or changed requirements in [FIPS201] and [SP800-157]:
		
		• Updates to issuer controls based on revisions to [FIPS201], which include:
		  o Supervised remote identity-proofing
		  o Inclusion of the concept of a PIV identity account
		• Inclusion of additional issuer controls for derived PIV credentials based on updates to [SP800-157], which include:
		  o PKI and non-PKI-based credentials issued at authentication assurance level (AAL) 2 or 3
		• Updates to issuer controls based on updated adjudicative guidelines for PIV credential eligibility issued by the Office of Personnel Management (OPM)

2378