NIST Special Publication 800-79

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

Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

Dennis Branstad
Alicia Clay
Joan Hash

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

PUBLIC DRAFT
Version 1.1

June ***2005***

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Michelle O'Neill, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Hratch G. Semerjian, Acting Director

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.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.
NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION,
INFORMATION TECHNOLOGY LABORATORY, NIST, VIA ELECTRONIC MAIL AT PIVACCREDITATION@NIST.GOV
OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors wish to thank their colleagues who reviewed drafts of this document and contributed to its development. We would especially like to thank Mr. Arnold Johnson, Ms. Judith Spencer and Dr. Richard Wilsher for their contributions. The authors also gratefully acknowledge and appreciate the many contributions made by others in supporting the development of this draft.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Homeland Security Presidential Directive 12 (HSPD 12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," established a Federal policy to create and use a government-wide secure and reliable form of identification for Federal employees and contractors. It further specified that this secure and reliable form of identification be issued only by providers whose reliability has been established by an official accreditation process. Federal Information Processing Standard 201, entitled "Personal Identity Verification of Federal Employees and Contractors," and NIST Special Publications 800-73, *Integrated Circuit Card for Personal Identity Verification,* 800-76, *Biometric Data Specification for Person Identity Verification* and 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* (hereafter collectively called FIPS 201) specify the requirements for an Integrated Circuit Card ("Smart Card") to be used as the secure and reliable form (hereafter called a PIV Card) of identification.

NIST Special Publication 800-79, ***Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*** should be used by any Federal agency issuing or planning to issue Personal Identity Verification (PIV) Cards that satisfy FIPS 201 to their Federal employees or Federal contractor employees. These guidelines describe a set of attributes that should be exhibited by a PIV issuer in order to be accredited. They are to be used by an organization to assess its reliability for providing PIV Card issuing services.

These guidelines are patterned closely after those in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. Instead of providing guidance for certifying and accrediting the security of information systems, these guidelines have been tailored to provide guidance for certifying and accrediting the reliability of a PIV Card issuing organization. Specifically, these guidelines are intended to help Federal agency officials:

- Satisfy the requirement in HSPD 12 that all identity cards be issued by providers whose reliability has been established by an official accreditation process;
- Help answer several questions about the PIV Card Issuer including: Does the issuer understand the requirements? Can the issuer reliably provide the required services?
- Assure more consistent, comparable, and repeatable assessments of the required attributes, of PIV Card issuers;
- Assure more complete, reliable, and trusted identification of individuals for controlling the access of Federal employees and contractors to Federal physical facilities and information systems; and
- Facilitate informed PIV Card issuer accreditation decisions without significant delay or use of resources.

Accreditation of a PIV Card Issuer is the official management decision of the Designated Accreditation Authority to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily being established through appropriate assessment and certification processes. Accreditation provides one form of quality control and urges managers and technical staffs at all levels of a PIV Card issuing organization to implement procedures compliant with FIPS 201.

It is essential that agency officials have the most complete, accurate and trustworthy information possible on the status of their PIV Card issuer in order to make timely, credible, risk-based decisions on whether to authorize its operation. ***Certification*** in this context means a formal process of assessing the attributes (i.e., reliability, availability, capabilities, and adequately supported facilities, personnel, equipment, finances and support infrastructures) of a PIV Card Issuer using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion a PIV Card issuing organization is reliable and capable of enrolling approved applicants and issuing PIV Cards in accordance with FIPS 201.Certification directly supports accreditation by providing authorizing officials with important information necessary to make credible decisions on whether initially to authorize an organization to issue PIV Cards or subsequently to continue its PIV Card issuing operations.

The certification and accreditation processes consist of four distinct phases:

- Initiation Phase;
- Certification Phase;
- Accreditation Phase; and
- Monitoring Phase.

Each phase in the certification and accreditation processes consists of a set of tasks and that are to be carried out by responsible agency officials (e.g. an agency's Designated Accreditation Authority, PIV Card Issuer Manager) and their designated and authorized support personnel. These are outlined in detail in this document.

Accreditation should be conducted in a manner that assures: (i) continued reliability of the PIV issuer and its offered services; (ii) ongoing monitoring of management and quality assurance controls; and, (iii) that re-accreditation occurs periodically in accordance with Federal or agency policy and whenever a significant change is made to the system or its operational environment.

CHAPTER ONE

1. INTRODUCTION

Homeland Security Presidential Directive 12 (HSPD 12), ***Policy for a Common Identification Standard for Federal Employees and Contractor***s, established a Federal policy to create and use a government-wide secure and reliable form of identification for Federal employees and contractors. It further ***specified secure and reliable identification that****:*

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

From the HSPD 12 objectives, ***Federal Information Processing Standard (FIPS) 201***, entitled "Personal Identity Verification of Federal Employees and Contractors*," **derived more specific objectives** of PIV Card issuing organizations (Issuers) assuring that:

- A PIV Card is issued only: 1) to an individual whose true identity has been verified, and 2) after a proper authority has authorized issuance of the Card.
- Only an individual with an acceptable, appropriate background investigation is issued a Card;
- An individual is issued a Card only after presenting two acceptable, authentic "identity source documents", at least one of which is a valid Federal or State government issued picture ID;
- Fraudulent or altered identity source documents are not accepted as being authentic;
- Any person suspected by, or known to, the government as being a terrorist is not issued a Card;
- No substitution of one person for another can occur in the identity proofing and PIV Card issuing processes. Specifically, the individual who applies for a PIV Card, who submits identity source documents, who appears for identity proofing, whose fingerprints are checked against applicable databases, and who appears to obtain an issued PIV card shall be the same person as the one to whom the PIV Card is issued;
- No PIV Card is issued unless requested by the proper authority;
- No single individual in the PIV Card Issuing Organization acting alone can issue a Card or cause one to be issued.

The objectives of these Guidelines include:

- establishing the attributes required of organizations in order to reliably perform appropriate identity "proofing" and issuing of PIV Cards to Federal and contractor employees;

- describing the methods needed to determine if a PIV issuer exhibits the required attributes; and

- providing guidance to Federal agencies in establishing, or obtaining the services of, a PIV Card Issuing Organization whose reliability is certified and accredited.

Certification of PIV Card issuing organizations is a formal process of assessing the attributes (i.e., reliability, availability, capabilities, and adequately supported facilities, personnel, equipment, finances and support infrastructures) of a PIV Card Issuer using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion a PIV Card issuing organization is reliable and capable of enrolling approved applicants and issuing PIV Cards in accordance with FIPS 201. ***Accreditation*** of a PIV Card Issuer is the official management decision of the Designated Accreditation Authority to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily being established through appropriate assessment and certification processes. ***These guidelines do not cover specifically certifying and accrediting the security of computer systems, PIV system components, access control systems utilizing PIV services, or the network comprising the PIV card management system.***

1.1 INTENDED AUDIENCE

These guidelines are intended for any Federal agency issuing or planning to issue Personal Identity Verification (PIV) Cards to Federal employees or Federal contractor employees. Homeland Security Presidential Directive (HSPD) 12 requires that all PIV Cards be issued by providers whose reliability has been established by an official accreditation process.

These guidelines describe a set of attributes that should[1] be exhibited by a PIV issuer in order to be accredited. They are intended to be used initially by an organization to assess its own capabilities and reliability to perform the required functions described in the Standard for Personal Identity Verification of Federal Employees and Contractors (Federal Information Processing Standard 201).

1.2 KEY RELATED NIST PUBLICATIONS

- NIST SP 800-73, *Integrated Circuit Card for Personal Identity Verification*
- NIST SP 800-76, *Biometric Data Specification for Person Identity Verification*
- NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*

These publications are integral parts of FIPS 201 and must[2] be considered as included whenever FIPS 201 is referenced in this publication.

1 "should" is used to denote a recommended but not mandatory action]

2 "must" is used to denote a mandatory action based on a regulation or standard].

1.3 AVAILABLE ASSISTANCE

These guidelines describe the processes of planning, certification, accreditation, and monitoring required for PIV Card issuers and provide references to documents that should be used when performing them. The PIV Card Issuer Manager responsible for establishing the needed services should be familiar with the list of documents included in Appendix A. These provide the technical specifications that must be exhibited by PIV Cards, the identity verification processes required to establish the legal identity of the PIV Card applicant, and the facility security systems and that information access control systems that use the PIV System. The references also provide guidance for assessing the security of the automated PIV Card issuing system.

Information will be posted as it becomes available at the URL http://www.csrc.nist.gov/piv-project. Questions regarding accreditation should be E-mailed to: PIVACCREDITATION@NIST.GOV..

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter 2** describes the fundamentals of PIV Card Issuer certification and accreditation. It also includes discussions of the: (i) roles and responsibilities of key participants in the PIV Card issuing organization and the agency or agencies that it supports; (ii) types of accreditation decisions; (iii) requirements for supporting documentation; and (iv) the need for monitoring of the PIV Card issuer.
- **Chapter 3** provides overviews of the required and desired attributes of a PIV Card Issuer and the methods suggested for assessing the presence of the attributes in the context of performing required PIV Card issuing services,
- **Chapter 4** discusses the major functions and operations of PIV Card Issuers, including planning, documentation, implementation, certification and accreditation, operations and maintenance. It then addresses the two primary services of Issuers: Applicant Identity Proofing and Registration; and PIV Card Issuance and Management and methods to assess organizational reliability.
- **Chapter 5** discusses PIV Card Issuing services and operations including design and development plans, reviews, validation testing, acquisition of services and applicant identity proofing and registration.
- **Chapter 6** uses the four phases of the certification and accreditation (C & A) processes specified in NIST SP 800-37, applies them to the new C and A application of accrediting PIV Card Issuers. The chapter includes: (i) a description of the tasks and subtasks in each phase; (ii) the responsibilities of various participants in each subtask; and (iii) guidance to help explain how to execute each subtask.
- **Supporting Appendices** provide more detailed PIV Card issuer certification and accreditation-related information and include: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) summary of tasks and subtasks; and (v) sample accreditation transmittal and decision letters.

CHAPTER TWO

2.0 THE FUNDAMENTALS

This chapter will review basic fundamentals of certification and accreditation since these are important concepts which must be understood by readers of this publication in terms of their application to PIV Issuing organizations.

2.1 CERTIFICATION AND ACCREDITATION

Certification and accreditation are required for PIV Card Issuers and will serve their best interests as well as those the entire Federal government if performed appropriately. Accreditation will not only satisfy the requirement of HSPD 12 but will also aid in establishing a common level of trust within each agency for the PIV Cards issued by other agencies. Good security begins with establishing the correct identity of a person and then subsequently verifying that it is still the same person to whom specific credentials (e.g. the physical PIV Card, the Applicant-unique data stored in and on the card) and authorizations (e.g. security clearance, access privileges, procurement authority) have been issued.

Certification directly supports accreditation by providing authorizing officials with important information necessary to make credible decisions on whether initially to authorize an organization to issue PIV Cards or subsequently to continue its PIV Card issuing operations. This information is produced by assessing various attributes and operations of the organization to determine if the issuer is reliable, that is that the required services are implemented correctly, operating as intended, and producing the desired outcomes. The certification and accreditation processes consist of four distinct phases:

- Initiation Phase;
- Certification Phase;
- Accreditation Phase; and
- Monitoring Phase.

Each phase in the certification and accreditation processes consists of a set of tasks and that are to be carried out by responsible agency officials (e.g. an agency's Designated Accreditation Authority, PIV Card Issuer Manager) and their designated and authorized support personnel.

The **Initiation Phase** consists of three tasks: (i) preparation; (ii) resource identification; and (iii) plan preparation, analysis, and acceptance. The purpose of this phase is to ensure that the appropriate agency officials participate in the preparation and design of a new PIV Card issuing system or review of an existing PIV Card issuing system..

The **Certification Phase** consists of two tasks: (i) FIPS 201 requirements analysis and assessments of the processes planned to satisfy the requirements; and (ii) certification documentation. The goal of this phase is to determine the extent to which the requirements can be achieved using the selected processes if they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the objectives and requirements of HSPD 12 and FIPS 201. This phase includes actions to be taken to correct deficiencies and discrepancies found during the assessment. Upon successful completion of this phase, the authorizing official will have the information needed to determine the risk associated with the agency's PIV card issuing process/system.

The **Accreditation Phase** consists of two steps: (i) making an accreditation decision; and (ii) preparing accreditation documentation. This phase specifies if the PIV Card issuer will have: (i) full authorization to enroll PIV Applicants and issue PIV Cards; (ii) an interim authorization to perform these services under specific terms and conditions; or (iii) denial of authorization to perform the services.

The **Monitoring Phase** consists of two tasks: (i) periodic PIV Card Issuer management and control review; and (ii) status reporting and documentation. This phase assures that continued oversight and monitoring of the operations specified in FIPS 201 are being conducted appropriately and informs the appropriate agency officials when changes will occur or have occurred that may impact the capability and reliability of the PIV Card issuer. The activities in this phase should be performed ongoing as long as the PIV Card issuing process is in place.

Certification and accreditation should be an integral part of a dynamic, ongoing management process. A PIV Card issuer is authorized to operate for a specific time depending on its accreditation status. The inevitable changes to any organization (including policy, procedures, equipment, and people) and the potential impact those changes may require structured monitoring of the organization on an ongoing basis. Thus, the initial accreditation needs to be followed by monitoring that: (i) tracks changes to the PIV Issuer; (ii) analyzes the impact of those changes; and (iii) reports the status of the PIV Card Issuer resulting from the changes to appropriate agency officials.

The following questions should be answered during the monitoring phase:

- Have there been any changes made to or proposed changes submitted for the PIV Card issuing system or its environment?
- Could any of the proposed changes affect the approved and accredited status quo?
- If so, would the resulting operational environment or status be unacceptable?
- When will re-accreditation be required?

Since the cost of certification and accreditation can be substantial, it is important to leverage the results of previous assessments that have been conducted.

2.2 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities of key participants involved in a PIV Card Issuer's certification and accreditation process.[3] Recognizing that agencies have widely varying missions and organizational structures, there may be differences in naming conventions for certification and accreditation-related roles and how the associated responsibilities are allocated among agency personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles[4]). However, the basic functions remain the same. The certification and accreditation processes described in these Guidelines are flexible and allow agencies to achieve the goals of specific tasks within their organizational structures in a way that best support their access control systems.

[3] Agencies may define other significant roles (e.g., government-wide PIV System liaisons, facilities managers, and operations managers) to support the PIV Card issuing organization certification and accreditation processes.

[4] No one individual should perform multiple roles in performing the certification and accreditation processes.

Authorizing Official

The *authorizing official* (or designated accrediting authority -DAA) is a senior management official or executive with the authority to formally accredit the reliability of PIV Card issuers in accordance with HSPD 12. The authorizing official should have the authority to oversee and assure the budget and operations of the PIV Card issuer. The authorizing official must be a government employee.

PIV Card Issuer Manager

The PIV Card Issuer Manager is responsible for ensuring that PIV Cards are produced in accordance with the requirements in FIPS 201 and the agencies using the Issuer' services.

Certification Agent

The *certification agent* is an individual, group, or organization responsible for conducting certifications (i.e. comprehensive assessments) of a PIV Card Issuer. The certification agent also provides recommended corrective actions to reduce or eliminate discrepancies between the current status of the Issuer and the requirements of FIPS 201. Prior to initiating the activities of the certification process, the certification agent provides a plan to ensure that a realistic snapshot of the current reliability of the Issuer will be obtained.

To preserve the impartial and unbiased nature of certifications, the certification agent should be independent from the persons directly responsible for the PIV Card Issuer and its day-to-day operation. The certification agent should also be independent of those individuals responsible for correcting deficiencies and discrepancies identified during the certification phase. The independence of the certification agent is an important factor in assessing the credibility of the assessment results and ensuring that the authorizing official receives objective information in order to make an informed accreditation decision.

PIV Card Applicant Representatives

PIV Card Applicant *representatives* are individuals that represent the interests of Federal employees and their contractors who are the Applicants for PIV Cards. These representatives should be interviewed during the certification and accreditation processes to ensure that the rights of Applicants are being protected.

Delegation of Roles

At the discretion of senior agency officials, certain certification and accreditation responsibilities may be delegated and if so, appropriately documented. Agency officials may appoint qualified individuals, including contractors, to perform C and A roles with the exception of the authorizing official. ***Only Government personnel should perform the role of authorizing official***. Table 1 below summarizes roles described.

Certification and Accreditation Roles	**PIV Role-Based Model Roles (See FIPS 201 Appendix A)**	**System-Based Model Roles (See FIPS 201 Appendix A)**
Designated Accreditation Authority Certification Agent PIV Card Issuer Manager PIV Card Applicant Representative	PIV Card Applicant PIV Applicant Sponsor PIV Registrar PIV Card Issuer PIV Digital Signatory PIV Authentication Certification Authority	Applicant Employer/Sponsor Enrollment Official Issuing Authority Approving Authority

Table 1: "Roles" in PIV Context

2.3 ACCREDITATION DECISIONS

Accreditation recommendations resulting from certification processes should be conveyed to the agency's authorizing official. To ensure the agency's business and operational needs are fully considered, the authorizing official should meet with the certification agent and the PIV Card Issuer Manager prior to issuing the accreditation decision to discuss the certification findings and the terms and conditions of the authorization. There are three types of accreditation decisions that can be rendered by authorizing officials:

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

Authorization to Operate

If, after reviewing the results of the certification phase assessments, the authorizing official deems that PIV Card issuer exhibits all the required attributes to an acceptable degree, an *authorization to operate* is issued. The issuer is authorized to perform all FIPS 201 complying PIV Card issuing services without restrictions or limitations. Although not affecting the accreditation decision, the authorizing official should require that the PIV Card Issuer's Manager reduce identified vulnerabilities where it is cost-effective to do so. Re-accreditation should occur at the discretion of the authorizing official when significant changes have occurred in the issuer's status or when a specified time period has elapsed.

Interim Authorization to Operate

If, after reviewing the results of the certification phase assessments, the authorizing official deems that the discrepancies are significant but there is an overarching mission necessity to allow the PIV issuer to operate, an *interim authorization to operate* may be issued. An interim authorization to operate is rendered when the identified deficiencies in the planned or implemented PIV Card issuing procedures are significant but can be addressed in a timely manner. An interim authorization is an authorization to operate under specific terms and conditions.

A PIV Card issuer is *not considered* accredited during the period of limited authorization to operate. The duration established for an interim authorization to operate should be commensurate with operational requirements. When the deficiencies have been adequately addressed and corrected, the interim authorization should be lifted and the PIV Card issuer should be accredited. Monitoring phase activities should focus on the identified deficiencies. Significant changes in the status of the PIV Card Issuer that occur during the period of limited authorization to operate should be reported immediately to the authorizing official.

Denial of Authorization to Operate

If, after reviewing the results of the certification phase assessments, the authorizing official deems operation of the PIV Card issuer to be unacceptable, the authorization to operate is denied. The PIV Card issuer is not accredited and PIV Cards should not be issued. If the PIV Card Issuer is currently in operation, all issuance of PIV Cards should be halted. Failure to receive authorization to operate indicates that there are major deficiencies in the required attributes of the PIV Card Issuer. The authorizing official or designated representative should work with the PIV Card issuer manager to ensure that proactive measures are taken to correct the deficiencies.

2.4 ACCREDITATION PACKAGE AND SUPPORTING DOCUMENTATION

The *accreditation package* documents the results of the certification phase and provides the authorizing official with the essential information needed to make a credible, risk-based decision on

whether to authorize operation of the PIV Card Issuer. Unless specifically designated otherwise by the authorizing official, the PIV Card Issuer Manager is responsible for the assembly, compilation, and submission of the accreditation package. The accreditation package contains the following documents:

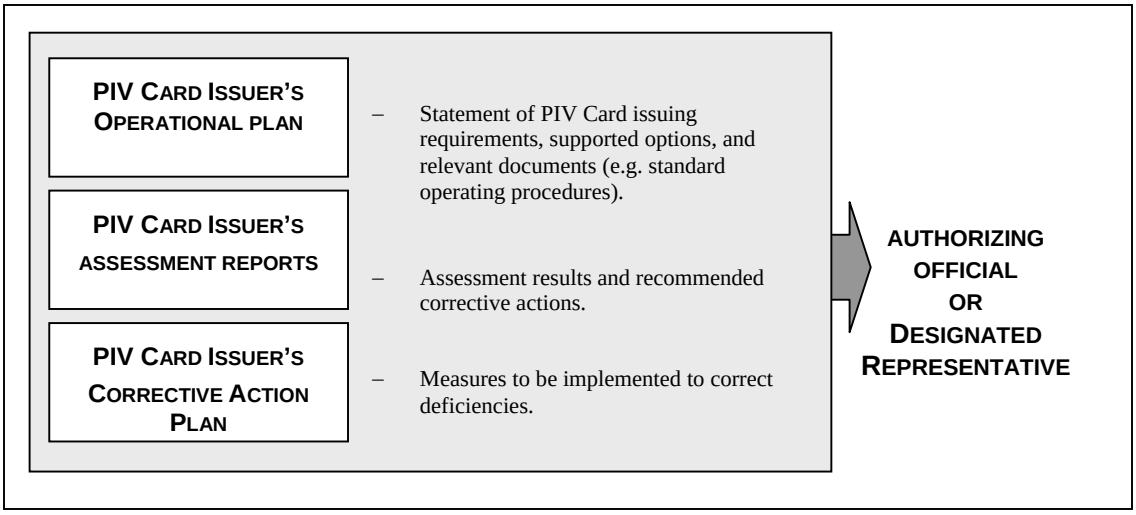
- PIV Card Issuer's operational plan;
- PIV Card Issuer's assessment reports; and
- PIV Card Issuer's corrective action plan.

The PIV Card Issuer's ***operational plan*** that is prepared by the PIV Card Issuer's Manager and previously approved by the authorizing official should specify all the requirements for issuing PIV Cards and describes the processes in place or planned for meeting those requirements. The plan should also contain supporting material and identity management related documents such as the Issuer's privacy policy for Applicants, descriptions of management procedures for assuring continued reliable operations, and all agreements with agencies regarding using the services of the Issuer.

The Issuer's attribute ***assessment reports***, prepared by the certification agent, provides the results of assessing the required attributes of the PIV Card Issuer to determine the extent to which the attributes are exhibited now and expected to continue during future operations. The assessment report should also contain recommended corrective actions if deficiencies or discrepancies are found.

The corrective action plan, which is prepared by the PIV Card Issuer's Manager, describes the measures that are being implemented: (i) to correct deficiencies noted during the assessment; and (ii) to reduce or eliminate discovered vulnerabilities to the secure creation and issuance of PIV Cards. The Manager submits the accreditation package to the authorizing official.[5] Figure 1 illustrates the primary sections of the accreditation package.

FIGURE 1 ACCREDITATION PACKAGE



The accreditation decision letter transmits the accreditation decision from the authorizing official to the PIV Card Issuer Manager. The accreditation decision letter contains the following information:

[5] Accreditation packages may be submitted in either paper or electronic format. Appropriate measures should be employed to protect the information contained in accreditation packages (electronic or paper format) in accordance with agency policy.

- Accreditation decision;
- Supporting rationale for the decision; and
- Terms and conditions for the authorization.

The accreditation decision letter (see Appendix E for examples) indicates to the PIV Card Issuer Manager whether the PIV card issuing system is: (i) authorized to operate; (ii) authorized to operate on an interim basis; or (iii) not authorized to operate. The supporting rationale includes the justification for the authorizing official's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the PIV Card issuer. The accreditation decision letter is attached to the original accreditation package and provided to the PIV Card issuer.

Upon receipt of the accreditation decision letter and accreditation package, the PIV Issuer manager reviews the terms and conditions of the authorization. The authorizing official also retains a copy of the accreditation decision letter and accreditation package. The certification and accreditation-related documentation (especially information dealing with vulnerabilities) should be: (i) marked and protected appropriately in accordance with agency policy; and (ii) retained in accordance with the agency's record retention policy.

CHAPTER THREE

3.0 ATTRIBUTES OF PIV CARD ISSUERS AND ASSESSMENT METHODS

This chapter discusses the attributes that are applicable to assessing an organization's ability to successfully demonstrate the ability to comply with the requirements of FIPS 201 related to the PIV card issuing process and it also identifies various assessment methods that can be applied to derive an opinion on an organization's reliability posture.

3.1 ATTRIBUTES

HSPD 12 requires, that all PIV Cards be issued by providers, whose reliability has been established, through an official accreditation process. ***One can determine an organization's reliability by assessing the following attributes:***

- **Knowledgeable**: understanding all the management, documentation, document control, work flow, privacy, security, technical foundation, data, devices, communications, and electronic processing requirements in FIPS 201;

- **Capable**: possessing the management, personnel, facilities, equipment, funding, and technical abilities of performing the required services of FIPS 201 including development of a plan, initiation of required acquisitions and initiation of corrective actions as appropriate.

- **Available**: the characteristic that required functions and services will be performed, by the Issuer, whenever desired by the consumer or customer.

- **Legal**: operating within all the applicable laws.

- **Compliant**: operating consistent with, and utilizing as required, all applicable policies, standards, rules, and regulations.

- **Adequately supported**: Having the personnel, facilities, equipment, finances, and support infrastructures needed to perform assigned duties and fulfill responsibilities.

The following desired attributes are similarly described:

- **Prepared/responsive/efficient**: exhibiting proper planning to be able to perform a service, in response to normal or expedited requests, and able to perform it without undue expenditure of time or resources.

- **Cost effective**: characteristic of a product, service, person, or organization that the cost for obtaining a product or service or using a person or organization to perform a service is proportional to the value of the product or service.

- **Adaptable**: Able to change to exhibit new characteristics, perform new services, use new technology, and operate in new environments as requirements change.

These attributes or organizational characteristics are not independent. They are defined to provide a broad foundation of attributes of a PIV Card Issuer that would meet the requirements of most agencies and satisfy the consumers of the offered services.

Accreditation based on assessment of these attributes is intended to assist an agency determine that the PIV Card Issuer services and operations will be conducted in an acceptable, consistent and predictable manner. The certification and accreditation processes to be performed initially and periodically thereafter should use one or more methods of assessing these attributes, determine if they are presently in, and adequately exhibited by, the Issuer now and will be reasonably expected to continue in the future. If the results of these processes are positive, an approval to operate should be issued by the Designated Accreditation Authority and the accreditation requirement of HSPD 12 should be considered satisfied.

3.2 ASSESSMENT METHODS

The following methods of assessment are described in the context of being applied to determine if the required attributes of a PIV Card Issuer are adequately exhibited in order to achieve successful accreditation. They are common methods of assessing the attributes of an organization or comparing one organization with others seeking to provide products or services to consumers and customers. The following overviews may be used by a DAA in selecting appropriate methods for establishing that the required attributes of the PIV Card Issuer are present.

- **Review and analysis**: broad methods of assessment that may be applied to most attributes but are best applied to reviewing documents (plans, policies, rules) and analyzing them in accordance with applicable standards.

- **Interview**: direct conversation with an assessment subject in which both pre-established and follow-on questions are asked, responses documented, discussion encouraged, and conclusions reached.

- **Demonstration/Direct Observation**: a producer or provider actively showing an assessor how a product works or a service is performed to a passive observer.

- **Sampling/statistics**: actively selecting relevant process information in accordance with a statistical sampling plan in order to verify that the functions or services produced on an on-going basis also satisfy the initial requirements.

- **Evaluation/Measurement**: analyzing an attribute using a metric that is selected to produce a result useful for assessing a quality of the attribute.

- **Compliance/conformance with standards**: analyzing an attribute to determine if the specified standards are being followed appropriately.

- **Precedence/Accepted Practice**: assessing an attribute and deeming it acceptable because it has been successfully used previously by others or has been used so frequently as to have become a deFacto standard.

- **Experience**: assessing organizational attributes of and deeming it acceptable because the organization has previously provided products or services similar or identical to those required by FIPS 201 while exhibiting said attributes.
- **Testing/validation**: actively testing attributes of an Issuer against a set of specifications using applicable test methods and metrics; validation is testing against a standard.

The methods of assessment described above may be used to verify that a PIV Card Issuer exhibits the required attributes. They should be applied when assessing PIV card Issuer functions, operations and services.

CHAPTER FOUR

4.0 PIV CARD ISSUER FUNCTIONS AND OPERATIONS

The attributes and methods of assessment described in chapter three may be used to verify the reliability of PIV Card Issuer functions and operations. The primary PIV Card Issuer functions are overviewed in this document to give the DAA information about the expected operations needed to support services provided by a PIV Card Issuer. Certification and accreditation processes should look to determine the reliability of these functions and operations. Detailed technical specifications and service descriptions required of a PIV Card Issuer are provided in FIPS 201 and the FICC Identity Management Handbook and are not repeated in this document. Criteria for a detailed assessment of PIV-I are being developed for inclusion in that Handbook and may be used in assessing the capability attribute of the Issuer using the compliance with standards method of assessment.

4.1 PLANNING

A PIV Card Issuer Manager plays a significant role and has major responsibilities in planning, initiating, operating, and managing a PIV Card issuing organization to service one or more agencies. The Manager must have a plan for: the design, implementation and operation of the PIV Card issuing system, the performance of the required PIV Card Issuing services, and the management of all required support activities of the organization including certification and accreditation requirements. In addition, the Manager must have a corrective actions plan to correct any deficiencies discovered in the organization during the certification phase. The Manager must be knowledgeable about the requirements of HSPD 12 and FIPS 201, be organized in having the needed documents, and be qualified to carry out all responsibilities of the position. The manager should be interviewed to assess his knowledge and skills, and the documentation of the organization should be reviewed and analyzed. Upon re-accreditation, the reliability of the organization should also be evaluated by statistical sampling of the products and services of the organization, and by direct observation.

4.2 DOCUMENTATION

A PIV Card Issuing organization is required to collect, organize, store, and disseminate many documents important to its operations. Five types are given here. The Manager and staff must be knowledgeable of the documentation requirements, including protection of the privacy of the Card Applicants and proper handling of the identity source documents. These documents should be reviewed and analyzed to assure that the organization is operating in accordance with legal and standards requirements. All of the documentation should be kept current. Document management may be patterned after other experienced PIV Card Issuers to show adherence to precedence.

- **Plans**: includes PIV Card Issuer's operational plan and the corrective action plan resulting from certification activities.

- **Policies**: includes the PIV Privacy requirements as specified in section 2.4 of FIPS 201 and information security policies relevant to the organization.

- **Standards and Guidelines**: includes all FIPS and NIST Guidelines relevant to the organization as well as international, national, and industry standards applicable to the services and operations of the organization, especially those related to PIV Cards as specified in FIPS 201 and NIST SP 800-73, biometric characteristics of people as specified in NISTG SP 800-76, and cryptography as specified in NIST SP 800-78.

- **Identity source documents**: PIV Card Applicants must supply identity source documents as specified in FIPS 201 in order to prove that their identity is authentic and can be verified by the originators of the documents. These documents must be stored in a manner that assures their contents are protected, used only for authorized purposes, and be able to be retrieved at some later time for re-verification if needed. FIPS 201 places requirements on the handling of these documents.

- **Forms/Reports**: Various forms will be used to obtain information and reports will be produced to provide information as specified in FIPS 201. Agency officials may obtain or provide required information in various ways without resorting to developing new forms whose formats may require prior approval. Document control is an important aspect of this element.

The most appropriate assessment methods include review and analysis of said documentation.

4.3 IMPLEMENTATION

Subsequent to planning and documenting the services and operations of a PIV Card Issuer, the PIV Card Issuer Manager needs to implement the operations plan.

Personnel

Obtaining knowledgeable, qualified, trustworthy, honest, and reliable personnel for the PIV Card Issuing organization is the first task of the PIV Card Issuer Manager. These people may already be operating the existing agency identity badge management system. They may need to be trained in the requirements of FIPS 201 and indoctrinated in the new policy of HSPD 12 in order to perform reliably in the new PIV Card issuing organization. They will need to be organized in a structure that will support the requirements of FIPS 201 and to be assigned the roles and responsibilities specified in that standard. Assessments of the required attributes of the Issuer organization may include: interviews, direct observation, and testing for knowledge of FIPS 201 and organizational policy requirements.

Facilities

Obtaining adequate facilities to support:
- Personnel,
- Storage of vital and sensitive records,
- Test systems and associated components (Hardware/software/firmware), and
- Other operational components.

The most appropriate assessment methods include review and analysis of plans for facilities.

Equipment

Obtaining adequate and reliable equipment to support the services provided by the PIV Card Issuer is fundamental to success of its operations. Demonstration and testing equipment will be needed to assure that PIV Card stock meets FIPS 201 specifications when obtained from the supplier; that PIV Card Readers/Writers are able to initialize the supplied cards; that the biometric data can be captured from the Applicant and entered into the Integrated Circuit "Chip" memory in the PIV Cards; that required software, credentials, and data can be loaded securely; and that completed PIV Cards will operate properly when issued. Assessments of the required attributes include review and analysis of plans for equipment to meet FIPS requirements.

Procurement

If adequate personnel, facilities, or equipment are not available, they must be procured, by the PIV Card Issuer. Procurement includes personnel transfers, acquiring additional staff if needed, establishment of support contracts, and purchasing or leasing of equipment. Procurement must be conducted in a manner that assures that reliable personnel services are obtained and that reliable and conformant equipment is obtained. These attributes may be assessed through interviews, demonstrations, direct observations and evaluations. Precedence of demonstrated capability and reliability of service providers and successful previous audits attesting to these attributes may be used to assess the success of procurement.

Monitoring

A critical aspect of the certification and accreditation processes is the post-accreditation period involving the monitoring of the operations and status of the PIV Card Issuer. An effective monitoring program requires:

- Configuration management processes;
- Review and analysis of changes to the PIV Card issuer's procedures and practices; and
- Assessment and reporting of status changes to appropriate agency officials.

It is important to document proposed or actual changes to the overall operation of the PIV Card Issuer and to determine the impact of those changes to its reliability. The PIV System will typically be in a state of migration due to changes in technology and modifications to the surrounding environment. Documenting PIV System and PIV Card Issuer changes and assessing their potential impact is an essential aspect of monitoring and maintaining accreditation.

CHAPTER FIVE

5.0 PIV CARD ISSUING SERVICES AND OPERATIONS

The attributes and methods of assessment described in chapter three may be used to verify the reliability of the following elements of PIV Card Issuing Services and Operations.

The PIV Card Issuer Manager is responsible for ensuring that PIV Cards are designed and produced in accordance with the requirements in FIPS 201 and the agencies using the Issuer' services. During the design and production planning, the card issuer must establish the responsibilities and authorities for design and production. Inputs to establishing the complete set of Card requirements include physical, electrical, functional, and interface requirements as specified in FIPS 201; performance requirements as specified by the using agencies; and applicable statutory and regulatory requirements as stated in HSPD 12 and FIPS 201 and those established by the departments or agencies using the services, and overseeing the operations, of the PIV Card Issuer. Specifications defined in these documents include: secure and reliable forms of identification; Identify Proofing; PIV Card Applicant privacy assurance; capture/acquisition and encoding of biometrics; collecting, processing, and protecting personally identifiable information; and maintaining a complete production record of PIV Cards from procurement of the blank cards through issuance of a completed PIV Card. The most appropriate Issuer assessment methods include sampling and statistics of organizational adherence to established standards and standard operating procedures (SOPs).

Design and development plans and specifications should be documented in a form that enables verification against the design and operation requirements. The documents should provide appropriate information for creating, establishing, or acquiring the needed facilities, automated support equipment, operations staff, conformance tests, PIV Card Issuer System components, PIV Card Readers/Writers, and other materials needed to operate a competent and reliable PIV Card issuing organization and set of services. The most appropriate Issuer assessment methods include review and analysis of plans.

Periodic reviews of plans, processes and services should be performed in order to evaluate the continued ability of the Issuer to produce conformant and reliable PIV Cards and identify any problems and propose corrective actions. Records of the results of the reviews and any necessary actions shall be maintained and protected. The most appropriate Issuer assessment methods include review and analysis of plans.

Validation testing should be performed on the first PIV Cards produced by a PIV Card Issuer to ensure they meet the stated requirements and periodically thereafter on a statistical sample of production Cards to ensure that the production processes are operating properly. Initial validation shall be performed prior to deeming that the PIV Card production process is operational. Records of the results of validation and any necessary corrective actions must be maintained and made available during subsequent certification phases.

The PIV Card Issuer is responsible for ensuring that purchased, leased, or created PIV System services comply with FIPS 201 specifications and that similarly acquired PIV Card stock, integrated circuit chips, applications software, communications services and software, and biometric marker (fingerprint and facial images) acquisition equipment conform to relevant standard's requirements. The type and extent of control that should be applied to the

supplier and the purchased elements is dependent on the overall effect of the purchased items on the availability, capability, and reliability of subsequently issued PIV Cards. The most appropriate Issuer assessment methods include review and analysis of supplier contracts.

The PIV Card Issuer should evaluate and select suppliers based on their ability to supply validated, FIPS 201 conformant card components or related services in accordance with organizational and regulatory requirements. Criteria for selection, evaluation and re-evaluation should be established by the PIV Card Issuer Manager and documented for later assessment. The appropriate Issuer assessment methods include review and analysis of supplier contracts, experience, precedence or accepted practices, sampling and testing.

Acquisition documentation should specify the requirements of card components or related services including: requirements for delivery and acceptance; requirements for supplier's procedures, processes and equipment in order to demonstrate reliability, requirements for supplier's personnel; protection of personally identifiable information of PIV Card Applicants if applicable; and the overall organizational security posture of supplier. The PIV Card Issuer Manager or staff should ensure that all procurement documents, actions, and controls satisfy the attributes of compliant, legal, organized, and adequately supported. These attributes should be assessed using the methods of review and analysis, direct observation, interviews, statistical sampling, evaluation/measurement, compliance, conformance, and prior experience.

The card issuer shall exercise due diligence and care with an individual's personally identifiable information while it is under the card issuer's control or being used by the card issuer in accordance with regulations and organizational requirements. The card issuer shall identify, verify, protect and safeguard identity credentials and other personally identifiable information provided for use in initializing or incorporation into the card. If any individual's personally identifiable information is lost, damaged or found to be unsuitable for use, this should be reported to the individual and the affected record should be changed. The PIV Card Issuer must have the capability and procedures for de-enrolling employees, revoking and destroying cards, and reissuing cards, all in compliance with FIPS 201. The most appropriate Issuer assessment method may be review and analysis of plans and sampling and statistics of organizational adherence to established standards and SOPs.

The PIV Card Issuer Manager is responsible for assuring that the monitoring phase of the certification and accreditation processes is undertaken and resources provided to collect and assess relevant evidence of continued reliability of the PIV Card Issuer. The attributes that should be exhibited include that the managers and operational personnel remain knowledgeable, capable, well managed, available, and adequately supported throughout the life cycle of every issued PIV Card. The Issuer organization personnel should undergo assessment for continued organizational reliability through review and analysis of required documentation, direct observation of day- to- day operations, and continued compliance with standards.

Commitment of the PIV Card Issuer to the implementation and operation of a secure and reliable PIV System can be demonstrated by: ***documenting and communicating*** to the organization the importance of meeting the requirements stated in HSPD 12, FIPS 201 and the FICC Identity Management Handbook; conducting reviews and analysis of the PIV Issuer's documentation; and ensuring the availability of appropriate resources for the Issuer.

The PIV Card Issuer Manager should inform all managers and operational personnel of this commitment and assure that all required policies, procedures, and operational requirements are communicated throughout the organization.

The PIV Card Issuer Manager has the responsibility for reporting to agency management on the performance of the PIV System and any need for improvement; The Manager is responsible for reviewing the status of the PIV System on a periodic basis to ensure its continuing reliability. The appropriate Issuer assessment methods include review and analysis of reports and other documentation.

PIV Card Issuer vital records should include: PIV Applicant Enrollment/Registration performance; status of recommended corrective actions; changes to the PIV Issuer's operations that may affect the overall PIV System; recommendations for improvements or modifications needed to adapt to changing agency requirements, and changing resource needs along with a plan for acquiring the needed resources. The appropriate Issuer assessment methods include review and analysis of plans and other records.

PIV Card Issuing personnel must be deemed reliable as determined by testing and adherence to requirements in standards such as FIPS 201 and HSPD-12. The PIV Issuer's Manager should satisfy this requirement by determining the necessary education, experience, and areas of competence needed by employees and contractors. The Certification agent should assess if the management and training of employees is being appropriately performed.

The PIV Card Issuer Manager must obtain and maintain the infrastructure needed to support performing the services required of FIPS 201. Support infrastructure includes: buildings, utilities, secure transportation and storage of sensitive records and secure communications among system components. The appropriate Issuer assessment method is direct observation.

5.1 APPLICANT IDENTITY PROOFING AND REGISTRATION

FIPS 201, Appendix A, specifies two models approved for PIV Identity Proofing and Registration. The Role Based Model defines the roles that must be played by various individuals in order to prove and register the identity of an Applicant and issue the Applicant a PIV Card. The roles in this model are: Applicant; PIV Sponsor; PIV Registrar; PIV Issuer; PIV Digital Signatory; PIV Authentication Certification Authority. ***The roles, of Applicant, Sponsor, Registrar, and Issuer must be played by different people when issuing a PIV Card***. The System-Based Model uses slightly different terminology and processes to accomplish equivalent results. The roles in this model are: Applicant; Employer/Sponsor; Enrollment Official; Approval Authority; Issuing Authority (Issuer). This model calls for using best practices and procedures for assuring separation of roles and performing responsibilities according to risk. This model further stipulates that ***all roles and processes must be provided by accredited service providers compliant with this standard.*** A PIV Card Issuer should be knowledgeable of the two approved models, the differences between the roles defined in the models, and the requirement for operating only an approved model to issue PIV Cards. A PIV Card Issuer needs to implement and support only one approved model.

5.2 APPLICANT INTERACTIONS

Both approved models are designed to serve PIV Card Applicants by processing their identity source documents and issuing a PIV Card only to approved applicants in accordance with FIPS 201. A PIV Card Issuer must interact with the applicant at various times under various circumstances. An Applicant should be notified of his/her responsibilities regarding identity proofing, registration/enrollment, and successful issuance of a PIV Card and all rights of an Applicant if the Card is not approved. Applicant interactions, described below must be able to be supported by a PIV Card Issuer. These include: assuring appropriate privacy to the Applicant and his/her Personally Identifiable Information; fairness and consistency in processing PIV Card Applications; and protection of the Integrity and Confidentiality of the PIV System. The PIV Card Issuer should exhibit the attributes of being reliable in all dealings with an Applicant. These attributes should be assessed using document review and analysis, direct observation, sampling, and evaluation.

Notification of Responsibilities and Rights

The Applicant should be notified of the responsibilities of holding a PIV Card and requested to agree to protect it in accordance with agency and PIV Card Issuer's policies and rules. Such rules/agreements may include that the Applicant will not attempt to clone, modify, or obtain data from any PIV Card; will not assist others in gaining unauthorized access to Federal facilities or information; and will report the loss or theft of an issued PIV card within 24 hours of noting its disappearance. The Applicant should be notified of what information will be required to obtain a PIV Card; what documents will be required in either original or paper copy form; what use will be made of the Personally Identifiable Information; what protection it will be provided; what will be required if the Application is approved; and what can be done by the Applicant if the Application is denied. The Application should include the printed name and signature of the PIV Card Applicant, the name and signature of the PIV Card Sponsor/Employer and the name of the PIV Card Issuer.

The Applicant should be notified of his/her rights under all applicable law, rules, regulations, directives, and policies. These include all privacy rights of the Applicant, including notification how the Personally Identifiable Information requested from the Applicant will be protected while stored or being processed, both manually and electronically. The rights of the Applicant to reapply for the current position or for other Federal or contractor positions if the Applicant is not accepted should be disclosed to the Applicant. The procedures for correcting incorrect information in the Identity Source Documents and all documentation and decisions based on them should be disclosed. The PIV Card Issuer Manager should document how various outcomes of Identity Proofing will be handled prior to the outcome arising and obtain agency approval for the planned responses to the Applicant. The most appropriate Issuer assessment method may be review and analysis of plans and documentation and sampling and statistics of organizational adherence to established standards and SOPs.

Application for a PIV Card

The following information may be included or solicited in a PIV Card Application that is used by an Agency. Only items applicable to the Applicant and required by the Agency for the position should be used. They include: (Applicant's current full name); maiden name or prior aliases; date and place of birth (using a birth certificate or other legal identity

establishment document); driver's license number and State and date of issuance; Social Security number and date of issuance; Military ID number and date of issuance; Passport number and country and date of issuance; Identity Source Documents as specified in FIPS 201; and other relevant information useful for proving the claimed identity. The most appropriate Issuer assessment method may be review and analysis of application forms.

Authorization to Conduct Identity Proofing

The Applicant should be requested to authorize the agency and the PIV Card Issuer to process the Application in accordance with the requirements of FIPS 201 and to conduct any and all Identity Proofing needed to verify the authenticity of the Identity Source Documents and otherwise prove the claimed Identity is valid for the Applicant. The authorization should include the printed name and signature of the PIV Card Applicant and the name of the PIV Card Issuer. The most appropriate Issuer assessment method may be review of documentation kept by Issuer during the application process.

Notification of Identity Proofing Results

The Applicant should be notified in writing of the results of Identity Proofing. The notification should be originated by the PIV Card Issuer and submitted to the PIV Card Sponsor/Employer for notification of the Applicant. The notification should include additional rights of the Applicant if the application is denied and instructions for proceeding to PIV Card Issuance if the application is approved. The Applicant should be notified that a PIV Applicant Representative is available to assist in removing any incorrect information that adversely affected the Identity Proofing process. The agency and PIV Card Issuer should have a policy for how, when, and how often an Applicant may reapply if an Application is denied. The appropriate Issuer assessment methods include review of documentation kept by Issuer during the application process and interviews with a random sample of Applicants who have gone through the Identity Proofing and registration/enrollment processes.

5.3 AGENCY INTERACTIONS[6]

A PIV Card Issuer should be explicitly authorized by an agency to issue PIV Cards for its employee's, its contractors, and other parties as defined in FIPS 201. One or more agencies may use the same PIV Card Issuer and one agency may utilize more than one authorized PIV Card Issuer. There will be numerous interactions between an agency and its PIV Card Issuer(s).

The certification and accreditation processes, specified in this document include initial and periodic interactions between the agency authorizing official (i.e. Designated Accredited Authority) and the PIV Card Issuer Manager, often through a Certification agent that is an employee of the agency but not connected with the PIV Card Issuer. A primary goal of the PIV Card Issuer Manager and the Issuer's personnel should be maintaining capable and available PIV Card Issuing services in support of the agency, its employees and contract personnel to meet the reliability objective. These attributes may be assessed through review and analysis of documented interactions, direct observation of teams and committees

6 One or more agencies may use the same PIV Card Issuer. In this case, only one accreditation is needed but should be viewed by all agencies that use the Issuer's services.

established to optimize PIV Card adoption and utilization, and interviews of agency officials and PIV Card Issuer Management.

Request for Identity Proofing

An agency PIV Employer/Sponsor issues a request for identity proofing to the PIV Registrar who is responsible for identity proofing of the Applicant and ensuring successful completion of the required background checks. The most appropriate Issuer assessment method may be review of documentation kept by the Issuer during the application process.

Enrollment/Registration of Applicant

Subsequent to satisfactory of Identity Proofing of the Applicant, the PIV Registrar registers or enrolls the Applicant in the PIV System's database and approves issuing of a PIV Card to the Applicant. The most appropriate Issuer assessment method may be review of documentation kept by the Issuer during the application process.

Notification of Identity Proofing Results

The PIV Registrar notifies the Applicant's Employer/Sponsor that the identity proofing has been completed and if the applicant has been approved. The Employer/Sponsor notifies the Applicant. The most appropriate Issuer assessment method may be review of documentation kept by the Issuer during the application process.

CHAPTER SIX

6.0 CERTIFICATION AND ACCREDITATION PROCESSES

The certification and accreditation processes consist of four phases: (i) Initiation; (ii) Certification; (iii) Accreditation; and (iv) Monitoring. Each phase consists of tasks and subtasks that are to be carried out by responsible officials (e.g. authorizing official, certification agent, PIV Card Issuer Manager,). Figure 2 provides a view of the certification and accreditation processes including the tasks associated with each phase. A table of certification and accreditation tasks and subtasks and the official responsible is provided in Appendix D.

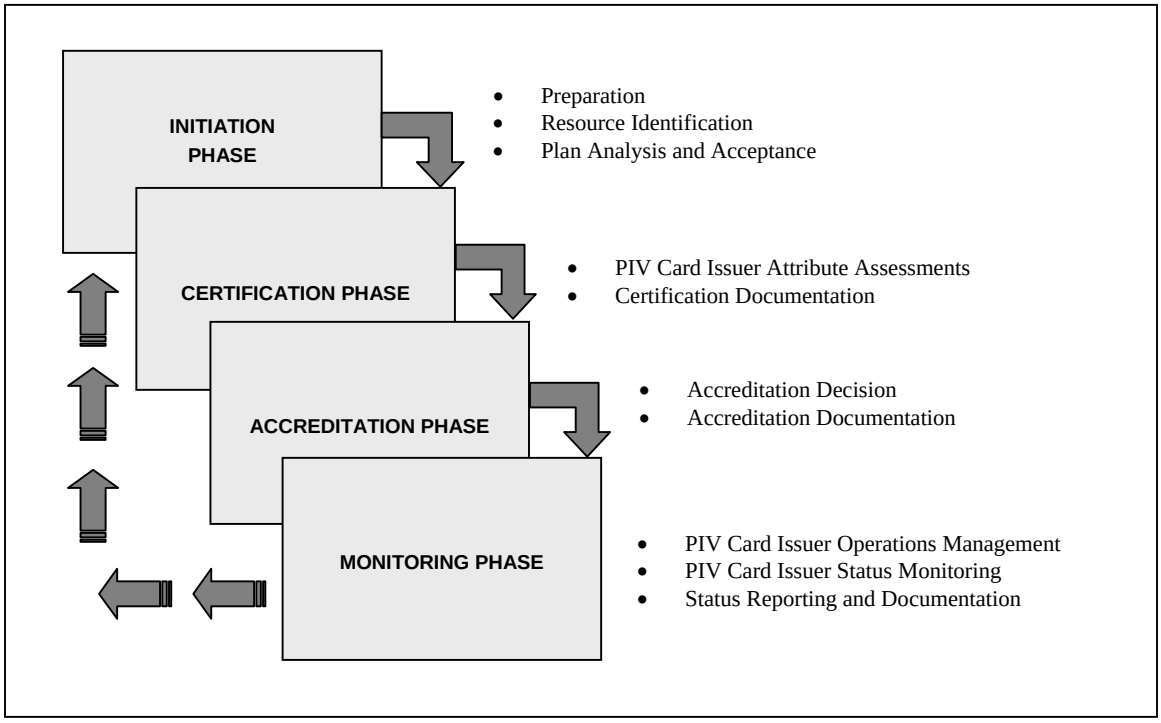


FIGURE 2 CERTIFICATION AND ACCREDITATION PROCESSES

6.1 INITIATION PHASE

The Initiation Phase consists of three tasks: (i) preparation; (ii) resource identification; and (iii) plan, analysis, and acceptance. The purpose of this phase is to ensure that the authorizing official has identified the attributes of the PIV Card Issuer that should be exhibited before the certification agent begins the assessment tasks. The early involvement of the authorizing official with key participants helps assure the success of the certification and accreditation.

TASK 1: PREPARATION

The objective of this task is to prepare for certification and accreditation by reviewing the PIV Card Issuing operations plan and confirming that the plan is consistent with FIPS 201 and the provided services and operations comply with it.

SUBTASK 1.1: Confirm that the PIV Card Issuer system has been fully described and documented in the PIV Card Issuer's plan.

RESPONSIBILITY: PIV Card Issuer Manager

GUIDANCE: A PIV Card Issuer description includes: (i) the names of the agencies sponsoring and using the PIV Card Issuer; (ii) a unique identifier for the Issuer; (iii) the status of the Issuer with respect to the operations plan; (iv) the name of the approving authority; (v) contact information for the PIV Card Issuer Manager; (vi) the applicable laws, directives, policies, regulations, and standards affecting the operations of the PIV Issuer (vii) the PIV Card Issuer's organization chart; (viii) a description of the automated system(s) used by the PIV Card issuer in performing the required services; (ix) a description of the network used for communicating with information systems and other parts of the PIV System; (x) encryption algorithms and cryptographic key types and sizes used for protecting information processing, transmission, and storage; (xi) public key infrastructures, certificate authorities, and certificate practice statements; (xii) the physical environment in which the PIV Card Issuer and supporting automated systems operate; and (xiii) the distributed, collaborative computing environments comprising the PIV System. The level of detail provided in the PIV Card Issuer's operations plan would depend on the history of the PIV Card issuing organization.

SUBTASK 1.2: Confirm that the applicability of the PIV Card issuer's services and supporting automated system has been determined and documented in the PIV Card issuer's plan and that it is not related to, or supporting, National Security.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: Consult NIST Special Publication 800-59 to confirm that the applicability of the PIV Card issuer's services is other than a national security system

SUBTASK 1.3: Confirm that the PIV Card Issuer has adopted and will use approved identity proofing and registration processes as required in FIPS 201 Appendix A and that all required roles, responsibilities, activities, and actions specified in the approved model (Role Based and System Based Models are pre-approved) are adequately documented in the PIV Card Issuer services operations plan and are used for performing the required services according to FIPS 201.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: FIPS PUB 201, Sections 2.2 and 5.2, require the adoption and use an approved identity proofing and registration process. All identity proofing and registration systems must satisfy the PIV objectives and requirements stated in Sections 2.2 and 5.2 in order to be approved. Two models (Role Based and System Based) are approved in FIPS 201 as satisfying the requirements. Agencies presently using the System Based model may continue to use it for issuing PIV Cards. Agencies not having a current program in the use of Integrated Circuit Cards for personal identity verification should design their PIV Card issuing service using the Role Based model.

SUBTASK 1.4: Confirm that the PIV Card Issuer has adopted and will use approved PIV Card Issuance and Life Cycle maintenance procedures.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: Section 2.3 of FIPS 201 requires the adoption and use of an approved issuance and maintenance process. All PIV issuance and maintenance systems must satisfy the PIV-I objectives and requirements stated in Section 2.3 in order to be approved. Two examples of PIV issuance process sets that satisfy the requisite PIV-II objectives and requirements are provided in Appendix A, Section A.1.2 and Appendix A Sections A.2.2 through A.2.4. The heads of Federal departments and agencies may approve other identity issuance process sets that are accredited as satisfying the requisite PIV-I objectives and requirements. Departments and agencies may enhance their issuance process to meet their local constraints and requirements.

TASK 2: RESOURCE IDENTIFICATION

The objective of the resource identification task is to: (i) identify and document the resources needed to provide all required services of FIPS 201 in accordance with its specifications; and (ii) prepare a plan of execution for the certification and accreditation activities indicating the proposed schedule and key milestones.

SUBTASK 2.1: Identify the senior agency authorizing official, certification agent, PIV Applicant representative, and other interested agency officials that are involved with agency personal identity verification, identity badge management, physical and information system access control, and information security that will be providing certification and accreditation support.

RESPONSIBILITY: PIV Card Issuer Manager

GUIDANCE: Identification of key agency officials is an important activity to establish that certification and accreditation processes are an integral part of the PIV Card Issuer system development life cycle and to verify that they will be participating in the processes. Identification and coordination also serve as a notification that they will be participants in the upcoming tasks necessary to plan, organize, and conduct the certification and accreditation.

SUBTASK 2.2: Determine the level of effort and resources required for the certification and accreditation of the PIV Card Issuer services and supporting automated system (including organizations involved) and prepare a plan of execution.

RESPONSIBILITY: PIV Card Issuer Manager; Authorizing Official.

GUIDANCE: The level of effort required for certification depends on: (i) the size the PIV Card issuing organization; (ii) its location and proximity to the agency personnel being served; (iii) the history and status of the PIV Card issuing organization; and (iv) the specific methods and procedures used to assess the management and technical controls being used to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. Identifying appropriate resources (e.g., supporting organizations, funding, and individuals with critical skills) needed for the certification effort is an essential aspect of preparation and is typically integrated within development life cycle and capital planning and budgeting processes. Once a certification agent is selected (or certification services procured), an execution plan for conducting the certification and accreditation is prepared by the certification agent in conjunction with the PIV Card Issuer Manager and authorizing official. The execution plan contains specific tasks, milestones, and delivery schedule. This information can be included in a system development/change plan and need not be in a separate plan of execution.

TASK 3: PIV CARD ISSUER'S OPERATIONS PLAN ANALYSIS AND ACCEPTANCE

The objectives of the PIV Card Issuer plan analysis and acceptance task are to: (i) perform an analysis of the PIV Card Issuer attributes required and desired by the senior agency officials (ii) obtain an independent analysis of the PIV Card issuing plan and revise as needed; and (iii) obtain acceptance of

the plan by the authorizing official prior to conducting an assessment of the attributes of the organization. The completion of this task concludes the Initiation Phase of the certification and accreditation processes.

SUBTASK 3.1: Review the list of desired attributes of a PIV Card Issuer described in these guidelines and document those that should be exhibited by the Issuer in addition to the required attributes in order to satisfy agency requirements.

RESPONSIBILITY: Authorizing Official; Certification Agent.

GUIDANCE: HSPD 12 specified that the reliability of a PIV Card Issuer be officially accredited before it could issue PIV Cards. This required attribute is one of several that are required in order to meet the goals of a personal identity management system as specified in FIPS 201. The attributes to be exhibited by an accredited PIV Card Issuer must be specified by the agency issuing the Issuer's services and then assessed to determine the extent to which the attributes are now being, or reasonably will be expected to be, exhibited.

Subtask 3.2 Select appropriate methods to assess the required and desired attributes of the PIV Card Issuer.

Responsibility: Certification Agent

Guidance: Certification agent should review the FIPS 201 and these guidelines to select methods and procedures for assessing the required attributes of the PIV Card Issuer. The certification agent, as directed by the authorizing official, may supplement these assessment methods and procedures as desired by the agency using the services of the PIV Card Issuer. Assessment methods and procedures may need to be created or tailored for assessing additional attributes of, or services provided by a PIV Card Issuer.

SUBTASK 3.3: Analyze the PIV Card Issuer plan to determine if there are vulnerabilities in plan that would result in not satisfying all the policies, procedures, and required in FIPS 201 and by the agency being serviced by the PIV Card Issuer if the plan was implemented properly and the specified operations performed as planned.

RESPONSIBILITY: Authorizing Official; Certification Agent.

GUIDANCE: The PIV Card Issuer plan provides an overview of the PIV Applicant vetting; identity source document proofing; PIV Card creation, issuance, and life-cycle management services and procedures of the PIV Card Issuer. The independent analysis of the plan by the certification agent and review by the authorizing official determine if the plan is complete and consistent with the requirements of FIPS 201. The certification agent and authorizing official can then determine if potential risks vulnerabilities in the provided services and automated support system appear to be adequately assessed, countered, and any residual risks are reasonable. Based on the results of the analysis by the certification agent and review by the authorizing official, changes to the plan should be recommended to the PIV Card Issuer Manager.

SUBTASK 3.4: Accept the PIV Card Issuer plan as acceptable.

RESPONSIBILITY: Authorizing Official.

GUIDANCE: If the PIV Card Issuer plan and the residual risks are deemed acceptable, the authorizing official accepts the plan. Acceptance allows the certification and accreditation processes to advance to the next phase (i.e. assessment of attributes of the PIV Card Issuer). Acceptance of the PIV Card Issuer plan also approves the resources required to initiate and complete the certification and accreditation activities.

6.2 CERTIFICATION PHASE

The Certification Phase consists of two tasks: (i) PIV Card Issuer service and attribute assessments; and (ii) certification documentation. The purpose of this phase is to determine the extent to which the services and specifications of FIPS 201 are provided and implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements of the agency

using the services of the PIV Card Issuer. This phase also specifies actions to be taken to correct deficiencies in the operations of the PIV Card Issuer and to minimize risks and mitigate vulnerabilities. Upon successful completion of this phase, the authorizing official will have the information needed from the certification activities to recommend the appropriate security accreditation decision in order to authorize operation of the PIV Card Issuer.

TASK 4: PIV CARD ISSUER ATTRIBUTE ASSESSMENT

The objective of this task is to: (i) initiate assessment of the required and desired attributes of the PIV Card Issuer; (ii) conduct the assessments; and (iii) document the results of the assessments. Initiation of attribute assessments involves gathering appropriate PIV policies, standards, guidelines, service requirements, attribute evidence, and results from previous assessments or audits. Initiation includes specifying the methods to be used to assess the attributes. The certification agent should determine that the specified attributes of the PIV Card Issuer are exhibited in such a manner that any Federal agency will accept the personal identity verification procedures performed by, and PIV Cards produced, by the Issuer. The certification agent will also be in a position to make recommendations on corrective actions for discovered deficiencies and offer advice to the PIV Card Issuer Manager and authorizing official on how to proceed with the certification.

SUBTASK 4.1: Assemble all documentation and supporting materials necessary for the assessment of the PIV Card Issuer; if these documents include previous assessments, then review the findings, results, and evidence.

RESPONSIBILITY: PIV Card Issuer Manager; Certification Agent.

GUIDANCE: The PIV Card Issuer Manager should assist the certification agent in gathering all relevant documents and supporting materials from the agency that will be required during the assessment of the required and desired attributes of the PIV Card Issuer. Supporting materials include PIV Issuer policies, the approved PIV Card Issuer service description and operations plan, relevant standards, guidelines, identity management handbooks, documentation available from other previously accredited PIV Card Issuers, and any records showing evidence of the required and desired attributes of the PIV Card Issuer. Assessment results from validation programs that test and evaluate features of commercial PIV components and products are especially important. If assessment results from the developer of similar PIV Card Issuer support systems are available, the certification agent may incorporate those results into the security certification with permission of the developer. Certification agents should maximize the use of previous assessment results.

REFERENCES: Documents and supporting materials included or referenced in the PIV Card Issuer plan; NIST Special Publication 800-37; audits; certifications; self-assessments; PIV product and component test, evaluation, and validation reports; privacy impact assessments; FIPS 140-2 and FIPS 201 validations.

SUBTASK 4.2: Assess the required and desired attributes of the PIV Card Issuer using methods and procedures selected or developed.

RESPONSIBILITY: Certification Agent.

GUIDANCE: Security assessment determines the extent to which the attributes are inherent in, or exhibited by, the PIV Card Issuer The results of the security assessment, including recommendations for correcting any deficiencies in the attributes of the organization, PIV Card services offered, or procedures used should be documented in the assessment report.

SUBTASK 4.3: Prepare the assessment report.

RESPONSIBILITY: Certification Agent.

GUIDANCE: The assessment report contains: (i) the results of assessments; and (ii) recommendations for correcting deficiencies in the organization, its services, its procedures, and its results. The assessment report is part of the final accreditation package along with the revised PIV Card Issuer plan and plan of action. The assessment report is the certification agent's statement regarding the capabilities and reliability, among other required and desirable attributes, of the PIV Card Issuer.

TASK 5: CERTIFICATION DOCUMENTATION

The security certification documentation task: (i) provides the certification findings and recommendations to the PIV Card Issuer Manager; (ii) revises the PIV Card Issuer's plan as needed; (iii) prepares the plan of action (including milestones); and (iv) assembles the accreditation package. The PIV Card Issuer Manager has an opportunity to reduce or eliminate vulnerabilities in the PIV Card plan and issuing services prior to the assembly of the accreditation package and submission to the authorizing official. This is accomplished by implementing corrective actions recommended by the certification agent. The certification agent should assess any plan or service modification or enhancement added during this process. The completion of this task concludes the Certification Phase.

SUBTASK 5.1: Provide the PIV Card Issuer Manager with the certification report.

RESPONSIBILITY: Certification Agent.

GUIDANCE: The PIV Card Issuer Manager relies on the expertise, experience and judgment of the certification agent to: (i) assess the required and desired attributes exhibited by the PIV Card Issuer; and (ii) provide recommendations on how to correct deficiencies in the planned or performed operations. The PIV Card Issuer Manager may choose to act on selected recommendations of the certification agent before the accreditation package is finalized. To optimize utilization of resources agency-wide, any actions taken by the PIV Card Issuer Manager prior to the final accreditation decision should be coordinated with the authorizing official. The certification agent assesses any changes made in response to the corrective actions and revises the assessment report as appropriate.

SUBTASK 5.2: Revise the PIV Card Issuer operations plan.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The PIV Card Issuer plan should reflect changes made in response to recommendations for corrective actions from the certification agent. At the completion of the Certification Phase, the plan should accurately describe what PIV services are to be offered, how they will be performed, how all the managerial and technical requirements specified in FIPS 201 shall be satisfied, how the required services are to be offered and to whom, and how the attributes of the PIV Card Issuer considered to be required or desirable will be continued throughout the life cycle of the organization.

SUBTASK 5.3: Prepare the corrective action plan.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The plan of action, one of the three primary documents in the accreditation package, describes actions taken by the PIV Card Issuer Manager to correct deficiencies identified in the Certification phase. The plan of action document identifies: (i) the tasks to be accomplished; (ii) the resources required to accomplish the tasks; and, (iii) scheduled completion dates for the tasks.

SUBTASK 5.4: Assemble the accreditation package and submit to authorizing official.

RESPONSIBILITY: PIV Card Issuer Manager; Certification Agent.

GUIDANCE: The PIV Card Issuer Manager is responsible for the assembly and compilation of the accreditation package with inputs from the certification agent. The accreditation package contains: (i) the assessment report from the certification agent

providing the results of the assessment of the attributes of the PIV Card Issuer and recommendations for corrective actions if needed; (ii) the plan of action from the PIV Card Issuer Manager indicating actions taken to correct deficiencies; and (iii) the revised PIV Card Issuer plan. Certification agent input to the accreditation package provides an independent view of the capabilities and reliability, along with the other required and desired attributes, of the PIV Card Issuer in fulfilling all FIPS 201 requirements. The PIV Card Issuer Manager may also wish to consult with other key agency participants (e.g., the PIV Applicant's representative) prior to submitting the final accreditation package to the authorizing official. The authorizing official will use this information during the Accreditation Phase to determine if the PIV Card Issuing procedures and operations should be accredited and authorized to operate. The accreditation package can be submitted in either paper or electronic form. The contents of the accreditation package should be protected appropriately in accordance with agency policy.

6.3 ACCREDITATION PHASE

The Accreditation Phase consists of two tasks: (i) making an appropriate accreditation decision; and (ii) completing the accreditation documentation. Upon successful completion of this phase, the PIV Card Issuer Manager will have: (i) authorization to operate the PIV Card Issuing services defined in the Issuer's plan; (ii) an interim authorization to operate under specific terms and conditions; or (iii) a denial of authorization.

TASK 6: ACCREDITATION DECISION

The accreditation decision task: (i) determines if the certification phase results in a recommendation to authorize operation of the PIV Card Issuer in accordance with the Issuer's plan for offering PIV Applicant vetting and PIV System enrollment services; and (ii) determines that the PIV Card Issuer may offer and provide the services and that the required and desired attributes of the Issuer have been deemed acceptable. The authorizing official, working with the, and certification agent produced during the previous phase, has independent confirmation of the identified vulnerabilities in the information system and a list of planned or completed corrective actions to reduce or eliminate those vulnerabilities. It is this information that is used to determine the final risk to the agency and the acceptability of that risk.

SUBTASK 6.1: Determine the risk to agency operations, agency assets, or individuals based on the vulnerabilities in PIV Card issuer system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

RESPONSIBILITY: Authorizing Official.

GUIDANCE: The authorizing official receives the final accreditation package from the PIV Card Issuer system owner. The vulnerabilities in the PIV Card Issuer system confirmed by the certification agent should be assessed to determine how those particular vulnerabilities translate into risk to agency operations, agency assets, or individuals. The authorizing official or designated representative should judge which PIV Card Issuer system vulnerabilities are of greatest concern to the agency and which vulnerabilities can be tolerated without creating unreasonable agency-level risk. The plan of action and milestones (i.e., actions taken or planned to correct deficiencies and reduce or eliminate vulnerabilities) submitted by the PIV Card Issuer system owner should also be considered in determining the risk to the agency. The authorizing official may consult the PIV Card Issuer system owner, certification agent, or other agency officials before making the final risk determination.

SUBTASK 6.2: Determine if the risk to agency operations, agency assets, or individuals is acceptable and prepare the final accreditation decision letter.

RESPONSIBILITY: Authorizing Official.

GUIDANCE: The authorizing official should consider many factors when deciding if the risk to agency operations, agency assets, or individuals is acceptable. Balancing risk considerations with mission and operational needs is paramount to achieving an acceptable accreditation decision. The authorizing official renders an accreditation decision after reviewing all of the relevant information and, where appropriate, consulting with key agency officials.

If, after assessing the results of the certification, the authorizing official deems that the agency-level risk is acceptable, an authorization to operate is issued. The PIV Card Issuer is accredited without any restrictions or limitations on its operation.

If, after assessing the results of certification, the authorizing official deems that the agency-level risk is unacceptable, but there is an important mission-related need to place the PIV Card Issuing System into operation, an interim authorization to operate may be issued. The interim authorization to operate is a limited authorization under specific terms and conditions including corrective actions to be taken by the PIV Card Issuer Manager and a required timeframe for completion of those actions. A detailed plan of action should be submitted by the PIV Card Issuer Manager and approved by the authorizing official prior to the interim authorization to operate taking effect. The PIV Card Issuer is *not* accredited during the period of limited authorization to operate. The PIV Card Issuer Manager is responsible for completing the corrective actions identified in the plan of action and resubmitting an updated accreditation package upon completion of those actions.

If, after assessing the results of the certification, the authorizing official deems that the agency-level risk is unacceptable, the Issuer is not authorized for operation and not accredited.

The authorizing official's designated representative or administrative staff prepares the final accreditation decision letter. The letter includes the accreditation decision, the rationale for the decision, the terms and conditions for the PIV Card Issuer's operation, and required corrective actions, if appropriate. The accreditation decision letter states whether the system is: (i) authorized to operate; (ii) authorized to operate on an interim basis under strict terms and conditions; or (iii) not authorized to operate. The supporting rationale provides the rationale for the authorizing official's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions that must be followed. The accreditation letter is included in the final accreditation package. The contents of the accreditation package should be protected appropriately in accordance with agency policy.

TASK 7: ACCREDITATION DOCUMENTATION

The objective of the accreditation documentation task is to: (i) transmit the final accreditation package to the appropriate individuals and organizations; and (ii) update the PIV Card Issuer's operations plan with the latest information from the accreditation decision. The completion of this task concludes the Accreditation Phase.

SUBTASK 7.1: Provide copies of the final accreditation package including the accreditation decision letter (in either paper or electronic form), to the PIV Card Issuer Manager and any other agency officials having interests, roles, or responsibilities in the PIV System

RESPONSIBILITY: Authorizing Official.

GUIDANCE: The accreditation package including the accreditation decision letter is returned to the PIV Card Issuer system manager. Upon receipt of the security accreditation decision letter and accreditation package, the PIV Card system manager accepts the terms and conditions of the authorization. The original accreditation package is kept on file by the PIV Card system manager. The authorizing official retains copies of

the decision letter and accreditation package. The accreditation package contains important documents and as such, should be appropriately safeguarded and stored, whenever possible, in a centralized agency filing system to ensure accessibility. The accreditation package should also be readily available to auditors and oversight agencies upon request. The accreditation package including all supporting documents, should be retained in accordance with the agency's records retention policy.

SUBTASK 7.2: Update the PIV Card Issuer's operations plan.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The operations plan should be updated to reflect any changes in the operations plan. Any conditions set forth in the accreditation decision should also be noted in the plan.

6.4 MONITORING PHASE

The Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) operations monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the day-to-day operations of the PIV Card Issuer on an ongoing basis and to inform the authorizing official when changes occur that may impact the reliability of the PIV System or any of its components. The activities in this phase are performed continually throughout the life cycle of the PIV System. Re-accreditation may be required because of changes in operation, management, technology, or support systems or because Federal or agency policies require periodic re-accreditation or independent accreditation of the PIV system or its components.

TASK 8: MANAGEMENT AND CONTROL

The objective of the management and control task is to: (i) document proposed or actual changes to the PIV system; and (ii) determine the impact of proposed or actual changes on the reliability of the system. Any organization or automated system will undergo changes in personnel, facilities, environments, hardware, software, or firmware. Documenting changes and assessing their potential impacts on an ongoing basis is an essential aspect of maintaining accreditation.

SUBTASK 8.1: Using established management and control procedures, document any changes that may be significant with respect to service offerings, PIV Card operations, or the PIV support automated system (including hardware, software, firmware, and surrounding environment).

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: An orderly and disciplined approach to managing, controlling, and documenting changes to PIV Card Issuer policies, procedures, services, and support systems is critical to the assessment of the PIV Card life cycle management of the Issuer. It is important to record all relevant information about changes to procedures, hardware, firmware, or software and modified features or capabilities. It is also important to record any changes to the working environment such as modifications to the physical facilities, management, and key personnel. The PIV Card Issuer Manager should use this documentation in assessing the potential impact of changes to the required and desired attributes of the Issuer. Significant changes should not be undertaken without assessing impact of such changes.

SUBTASK 8.2: Analyze the proposed or actual changes to the PIV System (including hardware, software, firmware, and surrounding environment) to determine the impact of such changes.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: Changes in the PIV System may affect the operations of the PIV Card Issuer, produce new vulnerabilities in the system, or generate requirements for new procedures.

If the results of the impact analysis indicate that changes to the PIV System could affect the PIV Card Issuer's operations, corrective actions should be initiated and the corrective action plan updated. The authorizing official or the PIV Card Issuer Manager may wish to consult with other agency officials prior to making the changes.

TASK 9: ATTRIBUTE MONITORING

The objective of the attribute monitoring task is to: (i) select an appropriate set of attributes to be monitored; and (ii) assess the attributes using methods and procedures selected by PIV Card Issuer Manager. The monitoring phase helps to identify potential problems during operations that are not identified during the certification phase.

SUBTASK 9.1: SELECT THE ATTRIBUTES OF THE PIV CARD ISSUER TO BE MONITORED

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The attributes of the PIV Card Issuer established by the PIV Card Issuer Manager to be monitored should reflect the agency's priorities and importance of the PIV services to the agency. For example, certain attributes may be considered more critical than others because of the potential impact on the operations if those attributes were reduced or circumvented. The attributes being monitored should be reviewed over time to ensure that a representative sample is included in the ongoing assessments. The authorizing official and PIV Card Issuer Manager should agree on the attributes that should be monitored as well as the frequency of such monitoring activity. The level of effort applied to the assessment should be commensurate with the FIPS 201 requirements, the sensitivity of the assets being protected by PIV Cards, and the risks remaining in the PIV Card Issuing system (i.e., the level of effort may increase corresponding to increases in the potential impact on agency operations, agency assets, or individuals increases.

SUBTASK 9.2: Assess an agreed-upon set of required and desired attributes to determine the extent to which they are exhibited by the PIV Card Issuer in all aspects of providing services to the agency and producing the desired outcome with respect to meeting the requirements specified in FIPS 201.

RESPONSIBILITY: Authorizing official with the PIV Card Issuer Manager.

GUIDANCE: The assessing of the attributes of an organization can be accomplished in a variety of ways. The methods and procedures employed to assess the Issuer's attributes during the monitoring process are at the discretion of the authorizing official coordinating with the PIV Card Issuer Manager. The monitoring process should be documented and available for review by the authorizing official, external auditor, or accreditation organization (if applicable) upon request. If the results of the attribute assessment indicate that processes are less than effective and are affecting reliability of the operations of the PIV Card Issuer, corrective actions should be initiated and the corrective action plan updated. The level of effort applied to the assessment should be commensurate with the FIPS 201 requirements, the sensitivity of the assets being protected by PIV Cards, and the risks remaining in the PIV Card Issuing system (i.e., the level of effort may increase corresponding to increases in the potential impact on agency operations, agency assets, or individuals increases).

TASK 10: STATUS REPORTING AND DOCUMENTATION

Status reporting and documentation includes: (i) revising the PIV Card Issuer's operations plan to reflect changes that could affect the reliability of the PIV System and the required attributes of the PIV Card Issuer; (ii) revising the plan of action based on the results of assessments conducted during the monitoring phase; and (iii) reporting the status of the PIV Card Issuer's attributes and experiences (problems and successes) to the authorizing official. The information in the status reports should be

used as part of the determination of the need for re-accreditation and to satisfy agency policy and additional requirements.

SUBTASK 10.1: Update the PIV Card Issuer's plan based on documented changes to the PIV operational requirements, personnel, facilities, equipment, and technology available to implement PIV systems and components and the results of the monitoring process.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The PIV Card Issuer's plan should contain the most up-to-date information about the services being offered, the technology being used, the statistics on false acceptance and false rejection rates of the Cards it issues, and the changes being planned. The frequency of plan updates is at the discretion of the PIV Card Issuer Manager. The updates should occur at appropriate intervals to capture significant changes to the operations, but not so frequently as to generate unnecessary work. The authorizing official, PIV Card Issuer Manager and certification agent will be using the plan to guide any future certification and accreditation activities.

.

SUBTASK 10.2: Update the plan of action based on the documented changes to the plan and the results of the monitoring process.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The plan of action is used by the authorizing official to monitor progress in correcting deficiencies noted during certification. The plan of action and should: (i) report progress in correcting deficiencies noted in the plan; (ii) address vulnerabilities in the PIV System operation discovered during monitoring; and (iii) describe how the deficiencies will be corrected and the vulnerabilities eliminated or minimized. The frequency of revising the corrective actions plan is at the discretion of the PIV Card Issuer Manager. The updates should occur at appropriate intervals to capture significant changes to the PIV system, but not so frequently as to generate unnecessary work. The authorizing official, PIV Card Issuer Manager, and certification agent will be using the plan of action to guide future certification and accreditation activities.

.

SUBTASK 10.3: Report the status of the PIV Card Issuer to the authorizing official.

RESPONSIBILITY: PIV Card Issuer Manager.

GUIDANCE: The status report should describe the PIV Card Issuer monitoring activities and report the results of monitoring. The status report should include descriptions of changes to the PIV Issuer's services, management, key personnel, PIV Card issuing support automated systems, and deficiencies. The frequency of status reports should be responsive re-accreditation is necessary. The status report should be handled and protected in accordance with agency policy.

APPENDIX A: REFERENCES

LAWS, DIRECTIVES, POLICIES, STANDARDS, AND GUIDELINES

1. Privacy Act of 1974 (Public Law 93-579), September 1975.

2. Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002.

3. OMB Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

4. Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

5. Federal Information Processing Standards Publication 200, *Security Controls for Federal Information Systems* (projected for publication December 2005).

6. Committee for National Security Systems Instruction 4009, *National Information Assurance Glossary*, revised May 2003.

7. 7. Federal Information Processing Standard (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors, February, 2005.

8. 8. NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

9. 9. NIST Special Publication 800-37, Guide for Security Certification and Accreditation of Information Systems, NIST, May 2004

10. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, NIST, February 2005.

11. NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

12. NIST Special Publication 800-73, Integrated Circuit Card for Personal Identity Verification, NIST, February 2005.

13. NIST Special Publication 800-76 (Draft), Biometric Data Specification for Person Identity Verification, NIST, February 2005

14. NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, NIST, March 2005

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

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

17. *Federal Identity Management Handbook (Draft Version 0.2),* Federal Identity Credentialing Committee, March, 2005.

APPENDIX B: GLOSSARY

COMMON TERMS AND DEFINITIONS

Terminology as used in these Guidelines	Definition or explanation of term.
Accreditation	The official management decision of the Designated Accreditation Authority to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily being established through appropriate assessment and certification processes.
Accreditation Package	The evidence provided to the Designated Accreditation Authority to be used in the accreditation 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); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a PIV Card issuer.
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which the reliability and supporting required attributes of a PIV Card Issuer are exhibited.
Authorizing Official	See Designated Accreditation Authority
Authorization to Operate	One of the three possible decisions of a Designated Accreditation Authority that is provided to a PIV Card Issuer after all certification activities have been performed and the reliability of the Issuer has been verified.
Certification Agent	The individual, group, or organization responsible for conducting certification activities under the guidance and direction of a Designated Accreditation Authority.
Certification (as applied to PIV Card Issuing organizations)	Certification in this context means a formal process of assessing the attributes (i.e., reliability, availability, capabilities, and adequately supported facilities, personnel, equipment, finances and support infrastructures) of a PIV Card Issuer using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion a PIV Card issuing organization is reliable and capable of enrolling approved applicants and issuing PIV Cards in accordance with FIPS 201.
Corrective Action Plan	The document that identifies corrective action tasks that need to be performed in order to obtain subsequent accreditation.
Designated Accreditation Authority	A senior agency official that has been given the authorization to accredit the reliability of a PIV Card Issuer.
FIPS	Federal Information Processing Standard

FISMA	Federal Information Security Management Act
National Security System	Any information system used or operated by an agency or its contractor: (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
NIST	National institute of Standards and Technology
OMB	Office of Management and Budget
PIV Card Applicant Identity Proofing	The processes of analyzing the identity source documents provided by a PIV Card Applicant to determine if they are authentic, to contact the sources of the documents to verify that they were issued to the Applicant, and to perform background checks of the Applicant to determine if the claim of identity is correct.
PIV Card Applicant Representative	An individual that represents the interests of all PIV Card Applicants using the services of a PIV Card issuer.
PIV Card Issuer	The organization that is authorized by one or more agencies to perform PIV Card Applicant Identity Proofing and has been accredited as being reliable for issuing PIV Cards.
PIV Card Issuer support automated system	The automated (computer-based) system used by a PIV Card Issuer to capture (acquire) the biometric characteristics (i.e. fingerprints, facial image) of a PIV Card Applicant, create the PIV credentials needed by the Applicant to access Federal facilities and information systems, and create a PIV Card for the Applicant by printing the required information on the Card and writing the required data into the memory of the Card.
PIV Subscriber	A person who had been a PIV Card Applicant and was approved to be issued a PIV Card.
PIV System	The automated (computer-based) system used by PIV Card Issuers to store the data about PIV Subscribers that is needed by agency automated access control systems utilizing the services of the PIV System to control access to Federal facilities and information systems.
Risk	The level of potential impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals of a threat or a given likelihood of that threat occurring.

APPENDIX C: CERTIFICATION AND ACCREDITATION TASK LIST FOR PIV CARD ISSUING FUNCTIONS

PHASES, TASKS, SUBTASKS AND RESPONSIBILITIES

PHASES, TASKS, AND SUBTASKS (VERIFY THE TASK NAMES)	RESPONSIBILITY (VERIFY THESE ROLES)
Initiation Phase	
Task 1: Preparation	
Subtask 1.1: PIV Card Issuer Service and Operational Plan Review	PIV Card Issuer Manager
Subtask 1.2: Agency and PIV Card Issuer National Security Categorization	PIV Card Issuer Manager
Subtask 1.3: Identity proofing and registration Processes Review	PIV Card Issuer Manager
Subtask 1.4: PIV Card Issuer Life Cycle Identification Review	PIV Card Issuer Manager
Task 2: Resource Identification	
Subtask 2.1: C & A Personnel Identification	PIV Card Issuer Manager
Subtask 2.2: C & A Level of Effort Required	PIV Card Issuer Manager, Authorizing Official
Task 3: Plan Analysis and Acceptance	
Subtask 3.1: PIV Card Issuer Desired Attributes Selection	PIV Card Issuer Manager Certification Agent
Subtask 3.2: Assessment Methods and Procedures	Certification Agent
Subtask 3.3: PIV Card Issuer Operations Plan Analysis	Authorizing Official, Certification Agent
Subtask 3.4: PIV Issuer Operations Plan Acceptance	Authorizing Official
Certification Phase	
Task 4: PIV Card Issuer Attribute Assessment	
Subtask 4.1: Documentation and Supporting Materials	PIV Card Issuer Manager Certification Agent
Subtask 4.2: Attribute Assessment	Certification Agent
Subtask 4.3: Attribute Assessment Report	Certification Agent
Task 5: Certification Documentation	
Subtask 5.1: Findings and Recommendations	Certification Agent
Subtask 5.2: PIV Card Issuer Operational Plan Update	PIV Card Issuer Manager
Subtask 5.3: Corrective Action Plan Preparation	PIV Card Issuer Manager
Subtask 5.4: Accreditation Package Assembly	PIV Card Issuer Manager Certification Agent

PHASES, TASKS, AND SUBTASKS	RESPONSIBILITY
Accreditation Phase	
Task 6: Accreditation Decision	
Subtask 6.1: Final Certification Review and Accreditation Determination	Authorizing Official
Subtask 6.2: Evaluation of Attribute (Reliability) Acceptability	Authorizing Official
Task 7: Accreditation Documentation	
Subtask 7.1: Accreditation Package Transmission	Authorizing Official
Subtask 7.2: PIV Card Issuer Plan Update	PIV Card Issuer Manager
Monitoring Phase	
Task 8: PIV Card Issuer Operations Management	
Subtask 8.1: Documentation of PIV Card Issuer Operations Plan Changes	PIV Card Issuer Manager
Subtask 8.2: Services and Operations Analysis	PIV Card Issuer Manager
Task 9: PIV Card Issuer Status Monitoring	
Subtask 9.1: Attribute Selection	PIV Card Issuer Manager
Subtask 9.2: Selected Attribute Assessment	Authorizing Official with PIV Card Issuer Manager
Task 10: Status Reporting and Documentation	
Subtask 10.1: Update PIV Card Issuer's Plan	PIV Card Issuer Manager
Subtask 10.2: Update Plan of Action	PIV Card Issuer Manager
Subtask 10.3: Status Report	PIV Card Issuer Manager

APPENDIX D: SAMPLE TRANSMITTAL AND DECISION LETTERS

AUTHORIZATION, INTERIM AUTHORIZATION, AND DENIAL OF AUTHORIZATION

Sample Security Accreditation Package Transmittal Letter

From: PIV Card issuer manager Date:

To: Authorizing Official

Subject: PIV Card Issuer Accreditation Package for [PIV CARD ISSUER]

A certification of the [PIV Card Issuer Name] located at [LOCATION] has been conducted in accordance NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations* and the [AGENCY] policy on PIV Card Issuer accreditation. The attached accreditation package contains: (i) the PIV Card Issuer operations plan; (ii) the assessment report; and (iii) corrective action plan.

The PIV Card issuer plan has been assessed by [CERTIFICATION AGENT] using the assessment methods and procedures described in the security assessment report to determine the extent to which the attributes are exhibited adequately, that the PIV Card issuing procedures are operating as intended, and producing the desired outcome. The plan of action describes the corrective measures that are planned to address any deficiencies in the PIV Card issuer's procedures.

Signature

Title

Enclosures

Sample Security Accreditation Decision Letter (Authorization to Operate)

From: Authorizing Official Date:

To: PIV Card Issuer Manager

Subject: Accreditation Decision for [PIV CARD ISSUER MANAGER]

After reviewing the results of the certification of the [PIV CARD ISSUER] and its supporting automated system-level components located at [LOCATION] and the supporting evidence provided in the associated accreditation package, I have determined that the plan and procedures are in compliance with FIPS 201 and are acceptable. Accordingly, I am issuing an *authorization to operate* the PIV Card Issuer's services in its existing operating environment. The PIV Card Issuer is accredited without any significant restrictions or limitations. This accreditation is my formal declaration that adequate attributes have been exhibited by the PIV Card Issuer and that a satisfactory level of capability and reliability is present.

The security accreditation of the information system will remain in effect as long as: (i) the required status reports for the PIV Card issuer are submitted to this office every [TIME PERIOD]; (ii) the problems reported during the monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the PIV Issuer operations have not exceeded the maximum allowable time period between accreditations in accordance with Federal or agency policy.

A copy of this letter with all supporting certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Signature

Title

Enclosures

Sample Security Accreditation Decision Letter (Interim Authorization to Operate)

From: Authorizing Official Date:

To: Information System Owner

Subject: Accreditation Decision for [PIV CARD ISSUER]

After reviewing the results of the certification of the [PIV CARD ISSUER] and its supporting automated system-level components located at [LOCATION] and the supporting evidence provided in the associated accreditation package, I have determined that the required attributes exhibited by the Issuer are *not* acceptable. However, I have also determined that there is an overarching need for the PIV Card Issuer to provide the needed services or to continue providing the services due to mission necessity. Accordingly, I am issuing an *interim authorization to operate* the PIV Card Issuer services in its existing operating environment. An interim authorization is a limited authorization to operate under specific terms and conditions and acknowledges greater risk for a limited period of time. The PIV Card Issuer is *not* considered accredited during the period of limited authorization to operate. The terms and conditions of this limited authorization are described in Attachment A.

A process must be established immediately to monitor the reliability of the PIV Card Issuer during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the certification. Significant changes in the status of the operations during the period of limited authorization should be reported immediately.

This interim authorization to operate is valid for [TIME PERIOD]. The limited authorization will remain in effect during that time period as long as: (i) the required status reports for the system are submitted to this office every [TIME PERIOD]; (ii) the problems or deficiencies reported during the monitoring process do not result in additional risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating the deficiencies in accordance with the plan of action. At the end of the period of limited authorization, the PIV Card issuer must be either authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this interim authorization to operate will be granted only under the most extenuating of circumstances. This office will monitor the plan of action submitted with the accreditation package during the period of limited authorization.

A copy of this letter with all supporting certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Signature

Title

Enclosures

Sample Security Accreditation Decision Letter (Denial of Authorization to Operate)

From: Authorizing Official Date:

To: PIV Card Issuer Manager

Subject: Accreditation Decision for [PIV Card Issuer Manager]

After reviewing the results of the certification of the [PIV CARD ISSUER] located at [LOCATION] and the supporting evidence provided in the associated security accreditation package, I have determined that the attributes exhibited by the PIV Card Issuer are unacceptable. Accordingly, I am issuing a denial of authorization to operate in its existing operating environment. The information system is *not* accredited and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED]. Failure to receive an authorization to operate indicates that there are major deficiencies.

The plan of action should be established or revised immediately to ensure that proactive measures are taken to correct the deficiencies found during the assessment. Certification should be repeated at the earliest opportunity to determine the effectiveness of correcting the deficiencies.

A copy of this letter with all supporting certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Signature

Title

Enclosures