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

July 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
William A. Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) stimulates U.S. economic growth and industrial competitiveness through technical leadership and collaborative research in critical infrastructure technology, including tests, test methods, reference data, and forward-looking standards, to advance the development and productive use of information technology. To overcome barriers to usability, scalability, interoperability, and security in information systems and networks, ITL programs focus on a broad range of networking, security, and advanced information technologies, as well as the mathematical, statistical, and computational sciences. 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, Usage, and Revisions

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 of 2002 (FISMA), 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.)

These guidelines will be reviewed within a year of initial issuance and will be revised based on additional information and experience obtained in implementing FIPS 201, creating and operating PCIs, and certifying and accrediting the reliability of PCIs.

Nothing in this document should be taken to contradict standards 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 this document and contributed to its development. We would especially like to thank Tanya Brewer, Arnold Johnson, Judith Spencer, and Richard Wilsher for their assistance and suggestions. The authors also gratefully acknowledge and appreciate the many comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

TABLE OF CONTENTS

Tables and Figures

EXECUTIVE SUMMARY

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

The guidelines in this document should be used by Federal agencies issuing, or preparing to issue, Personal Identity Verification (PIV) Cards that comply with FIPS 201 to their Federal employees and/or Federal contractor employees. These guidelines describe a set of attributes that should be exhibited by a PIV Card Issuer (hereafter called a PCI) in order to be accredited. They should be used by each agency for assessing the reliability of any organization providing its PCI services.

These guidelines are patterned closely after those in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. SP 800-37 provides guidance for certifying and accrediting the security of information systems. This document, SP 800-79, provides guidance for certifying and accrediting the reliability of a PCI. Note that use of SP 800-79 for accrediting the reliability of a PCI must be done in addition to accrediting the security of computer systems used by the PCI by using SP 800-37 and SP 800-53 as guidance.

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;

- Answer several questions about the PCI including— Does the PCI Manager and staff understand the requirements specified in FIPS 201? Can the PCI reliably provide the required services? Are the PCI processes implemented as designed and are they adequately documented in the PCI operations plan? Is there credible evidence to believe that the operations plan will be implemented as designed?

- Ensure more consistent, comparable, and repeatable assessments of the required attributes of PCI's;

- Ensure 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 PCI accreditation decisions without significant delay or use of resources.

It is essential that agency officials have complete, accurate and trustworthy information about their PCI 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 of a PCI using various methods of assessment that verify that a PCI is reliable and capable of enrolling approved applicants and issuing PIV Cards.

Accreditation of a PCI is the official management decision of a Designated Accreditation Authority (DAA) to authorize operation of a PCI after determining that the PCI's reliability has satisfactorily been established through appropriate assessment and certification processes. Accreditation provides one form of quality control and helps to assure that managers and the technical staff of a PCI will implement procedures compliant with FIPS 201 and assure that all its provisions are satisfied on a continuing basis. Certification directly supports accreditation by providing the DAA with important information necessary to make credible decisions on whether to authorize an organization to issue PIV Cards or to continue its PIV Card issuing operations.

The certification and accreditation processes consist of four phases: Initiation Phase, Certification Phase, Accreditation Phase, and Monitoring Phase. Each phase consists of a set of tasks that are to be carried out by specified agency officials (e.g., DAA, PCI Manager) and their authorized support personnel.

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

Several models of a PIV Card issuing organization are possible. A centralized model and distributed model are described. The primary responsibilities of a PCI include identity proofing and registration, PIV Card Creation and Issuance, and PIV Card Life Cycle Management. The certification and accreditation activities specified in this document cover all these operations whether they are in a single organization or distributed across several organizations.

If one agency would like to use the services of a PCI of a second agency, the first agency should review the second agency's PIV policies and the PCI's operations plan, accreditation package, and Authorization to Operate. If acceptable the client agency may utilize the services of the server agency's PCI without re-accreditation.

Certain roles and responsibilities may be delegated and/or contracted. Specific time periods are specified for re-accreditation and providing PIV services under an Interim Authorization to Operate. These are specified in appropriate sections of the Guidelines. Some services of a PCI may be accredited and provided without requiring that all potential services be accredited and provided. In particular, PIV-I services should be accredited for a PCI when they are available but before they are provided. PIV-II services should be accredited for a PCI as they become available and added to PIV-I service offerings. Appropriate PCI attribute and assessment methods should be selected by the SAO and the DAA and used for partial service accreditations.

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, *Personal Identity Verification of Federal Employees and Contractors*, derived more specific objectives of Personal Identity Verification (PIV) Card issuing organizations (hereafter called a PCI or Issuer) including that—

- A PIV Card is issued only— (i) to an individual whose true identity has been verified; (ii) subsequent to a request to process an Applicant for a PIV Card by an authorized authority (e.g., employer, sponsor); and (iii) after an authorized authority (e.g., registrar) has authorized issuance of the Card;
- Only an individual with an acceptable background check which satisfies the requirements of FIPS 201 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 single individual in a PCI *acting alone* is authorized or technically capable of issuing a PIV Card or is able to cause one to be issued.

The objectives of the guidelines in this document include—

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

- Describing methods for determining if a PIV issuer exhibits the required attributes; and

- Providing guidance to Federal agencies in establishing or obtaining the services of a PCI whose reliability is accredited.

These guidelines describe a set of attributes required to be exhibited by a PIV issuer in order to be accredited as well as other attributes that are considered highly desirable. They are intended to be used by an agency to assess a PCI's capabilities and reliability to perform the required services described in FIPS 201.

Certification of a PIV Card issuing organization is a formal process of assessing the attributes (availability, capability, and possessing adequately supported facilities, personnel, equipment, finances and support infrastructures) of a PCI using various methods of assessment (e.g., interviews, document reviews, laboratory test results, procedure evaluations, component validation reports) that support the assertion that 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 PCI is the official management decision of the Designated Accreditation Authority (DAA) to authorize operation of a PCI after determining that the PCI's reliability has satisfactorily been *established through appropriate assessment and certification processes. These guidelines do not specifically cover 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. These activities should be performed in accordance with NIST SP 800-37 in addition to those specified in this document.*

1.1 Intended Audience

These guidelines are intended for any Federal agency issuing or preparing to issue PIV Cards to Federal employees and/or Federal contractor employees. HSPD-12 requires that all PIV Cards be issued by providers whose reliability has been established by an official accreditation process.

1.2 Key Related NIST Publications

The following NIST publications establish requirements of a PCI. These publications are integral parts of FIPS 201 and must[1] be considered as included whenever FIPS 201 is referenced in this publication.

- Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*

- NIST Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification*

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

- NIST SP 800-76 (Draft), *Biometric Data Specification for Personal Identity Verification*
- NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*

1.3 Available Assistance

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

Information will be posted as it becomes available at 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 publication is organized as follows:

- **Chapter 2** describes the fundamentals of PCI certification and accreditation. It also includes discussions of the— (i) roles and responsibilities of key participants in the PCI and the agency or agencies that it supports; (ii) types of accreditation decisions; and (iii) requirements for supporting documentation.
- **Chapter 3** provides overviews of the required and desired attributes of a PCI and the methods suggested for assessing the presence of the attributes.
- **Chapter 4** discusses the major functions and operations of PCIs, including planning, documentation, implementation, operations, and maintenance.
- **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, and applies them to the C&A of PCIs. 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.
- **Appendices** include— (i) references; (ii) definitions and acronyms; (iii) summary of tasks and subtasks; and (iv) sample accreditation transmittal and decision letters.

2.0 THE FUNDAMENTALS

This chapter reviews fundamentals of certification and accreditation of PIV Issuing organizations.

Accreditation is a term that is used in various contexts with somewhat different meanings. University departments are often accredited to provide assurance that graduates have capabilities equivalent with those of similarly accredited departments. Testing laboratories may be accredited to demonstrate that their results are equivalent with others similarly accredited. One goal of PCI accreditation is to demonstrate that the capability and reliability of PCIs are appropriate and adequate. Another goal of PCI accreditation is to authorize a PCI to create and issue PIV Cards whose security is equivalent with those issued by other PCIs. Finally, PIV Cards created by an accredited PCI should be trusted and acceptable to other organizations so that access control decisions can be made relying on the accuracy of the information on the PIV Card.

2.1 Certification and Accreditation

Accreditation is required for PCIs by HSPD-12, and will serve the interests of the entire Federal government if performed appropriately. Accreditation can assist in establishing a common level of trust among agencies for PIV Cards. Good physical and logical access control begin 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, Applicant-unique data stored in and on the Card) and authorizations (e.g., access privileges) have been issued.

Certification provides the DAA with important information necessary to make credible decisions on whether to authorize an organization to issue PIV Cards or 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 and that the required services are implemented correctly, operating as intended, and producing the desired outcomes.

The certification and accreditation (including re-accreditation) processes consist of four phases:

- Initiation Phase
- Certification Phase
- Accreditation Phase
- Monitoring Phase

Each phase consists of tasks that should be carried out by responsible agency officials (e.g., an agency's DAA, PCI Manager) and their designated and authorized support personnel.

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 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) performing assessments of the attributes of the PCI; and (ii) preparing certification documentation. This phase is to determine the extent to which the requirements of FIPS 201 are being achieved using the selected assessment methods and verifying that they are implemented correctly, operating as intended, and producing the desired outcomes. This phase includes recommending actions to be taken to correct deficiencies and discrepancies found during the assessment. Upon successful completion of this phase, the risk associated with the agency's PCI operations should have been determined, documented, and a recommendation made to the DAA regarding accrediting the capability and reliability of the PCI.

The **Accreditation Phase** consists of two tasks: (i) making an accreditation decision; and (ii) preparing accreditation documentation. The DAA should review the certification documentation and the recommendation prepared by the certification agent(s). Following the review, the DAA should prepare a letter (see Appendix D for examples) regarding operation of the PCI and a transmittal letter similar to the example in Appendix D. The alternatives include— (i) full authorization to operate (e.g., perform identity proofing, enroll PIV Applicants, and issue PIV Cards); (ii) interim authorization to operate (i.e., perform these services under specific terms and conditions); or (iii) denial of authorization to operate (i.e., the PCI may not perform PIV services).

The **Monitoring Phase** consists of three tasks: (i) PCI management and control review; (ii) PCI status monitoring; and (iii) PCI status reporting and documentation. This phase provides continued oversight and ensures that monitoring of PCI operations 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 PCI. The activities in this phase should be 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. It should be stressed to a PCI that good information and facility security not only includes establishing and verifying a claimed identity but also the creation of processes to protect that identity and related information in identifiable form (IIF) through trusted procedures and technically enforced processes in accordance with FIPS 201, FISMA, and other applicable policies and standards of good practice. A PCI 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 of 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 PCI; (ii) analyzes the impact of those changes; and (iii) reports the status of the PCI changes to appropriate agency officials.

The following questions should be answered during the monitoring phase—

- Have there been changes made to the PCI, its environment, or its automated support systems that could affect the PCI's services or reliability?
- 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 when applicable and creditable.

2.2 Roles and Responsibilities

The following sections describe the roles and responsibilities of key participants (see Figures 1-3) involved in the certification and accreditation of a PCI.[2] 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[3]). However, the basic functions remain the same. The certification and accreditation processes described in these guidelines allow agencies to achieve the goals of specific tasks within their organizational structures in a way that best support their access control systems.

Senior Authorizing Official

The Senior Agency Official (SAO) (see Figure 2) is responsible for the establishment, budget, and oversight of the PIV functions and services of an agency.

Designated Accreditation Authority

The Designated Accreditation Authority (DAA) is a senior agency official with the authority to formally accredit the reliability of PCIs as required by HSPD-12.

PCI Manager

The PCI Manager (may be called an Agency Identity Management Official) is responsible for ensuring that all the services specified in FIPS 201 are provided reliably and that PIV Cards are produced and issued in accordance with its requirements.

Certification Agent

The Certification Agent (CA) should be an individual, group, or organization that has the appropriate skills, resources, and competencies to perform certifications (i.e., comprehensive assessments) of a PCI. The CA should identify discrepancies between the current status of the PCI and the requirements of FIPS 201, and present them to the PCI Manager who will prepare recommended corrective actions to reduce or eliminate the discrepancies. The CA should review the corrective actions, report if they are adequate or not, and then ensure that the final set of acceptable corrective actions are properly applied. Prior to initiating the activities of the certification process, the CA provides a plan to ensure that a realistic assessment of the current reliability of the PCI will be obtained.

To preserve the impartial and unbiased nature of certifications, the CA should be independent of, and organizationally separate from, the persons and the office(s) directly responsible for the day-

[2] 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.

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

to-day operation of the PCI. The CA should also be independent of those individuals responsible for correcting deficiencies and discrepancies identified during the certification phase. The independence of the CA is an important factor in assessing the credibility of the assessment results and ensuring that the DAA receives objective information in order to make an informed accreditation decision.

PIV Card Applicant Representative

A PIV Card Applicant Representative represents the interests of current or prospective Federal employees and contractors who are the Applicants for PIV Cards. They should represent the privacy concerns of applicants, assist an applicant who is denied a PIV Card because of missing or incorrect information in an Identity Source document, or act as a surrogate for an applicant that is not available for performing required actions. These representatives should be interviewed during certification to assess if the rights of Applicants are being protected and that all Applicants obtain useful information or assistance when desired.

Agency Official for Privacy

The role of the Agency Official for Privacy (AOP) is defined in FIPS 201 and may not assume any other operational role in the PIV system. The AOP oversees privacy-related matters in the PIV system and should work with the PIV Card Applicant Representative to ensure that the rights of Applicants and PIV Subscribers (approved Applicants who have been issued a PIV Card) are protected.

Delegation of Roles

Each agency should document its PIV certification and accreditation program, the operational plan to be performed by its PIV Card issuing organization, and the geographical facility and organizational model it has chosen. The SAO should document all the responsibilities, roles, and procedures to be followed by the PCI and the certification and accreditation processes selected to be used. The SAO should appoint, if they have not been previously appointed, qualified individuals as the DAA, the Certification Agent(s), and the PCI Facility Manager for each facility (i.e., location) that will be issuing PIV Cards. This selection will depend upon the FIPS 201 Appendix A Model selected, the appropriate roles required of the model, and the detailed PIV credentials and technical details chosen. At the discretion of the SAO, certain certification and accreditation responsibilities may be delegated to individuals and organizations, including contractors. ***The SAO, DAA, and CAs should be Federal employees***. All other roles should serve under the auspices and oversight of the SAO. Table 1 designates different roles involved in C&A and the two models specified in FIPS 201 Appendix A. Note that no correspondence is implied among the rows of the table.

Certification and Accreditation Roles	PIV Role-Based Model Roles (See FIPS 201 Appendix A)	System-Based Model Roles (See FIPS 201 Appendix A)
Senior Agency Official	PIV Card Applicant	Applicant
Designated Accreditation Authority	PIV Applicant Sponsor	Employer/Sponsor
Certification Agent	PIV Registrar	Enrollment Official
PCI Manager	PCI (Manager)	Issuing Authority
PIV Card Applicant Representative	PIV Digital Signatory	Approval Authority
Agency Official for Privacy	PIV Authentication Certification Authority	

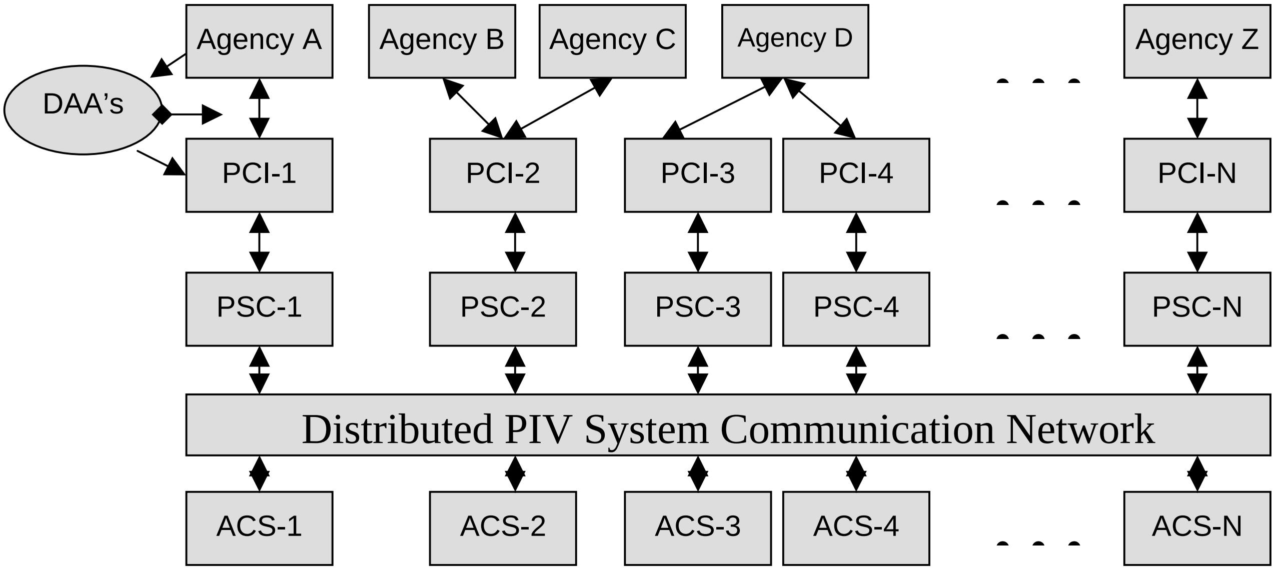
Table 1. "Roles" in PIV Context

Sample PIV Card Issuing Organizations

Each agency could have a different structure for the organization that it establishes or uses for issuing PIV Cards. Figure 1 provides a logical view of the PIV system. Agency A is shown with its own PCI. The PCI uses a computer support system or systems connected to a network to communicate with peer PCI support systems and access control systems. Agencies B and C have chosen to utilize the services of a shared PCI and its associated support systems. Agency D is large and geographically distributed and therefore has multiple (two are shown) PCIs. The DAA for each agency is responsible for accrediting the reliability of the PCI or PCIs used.

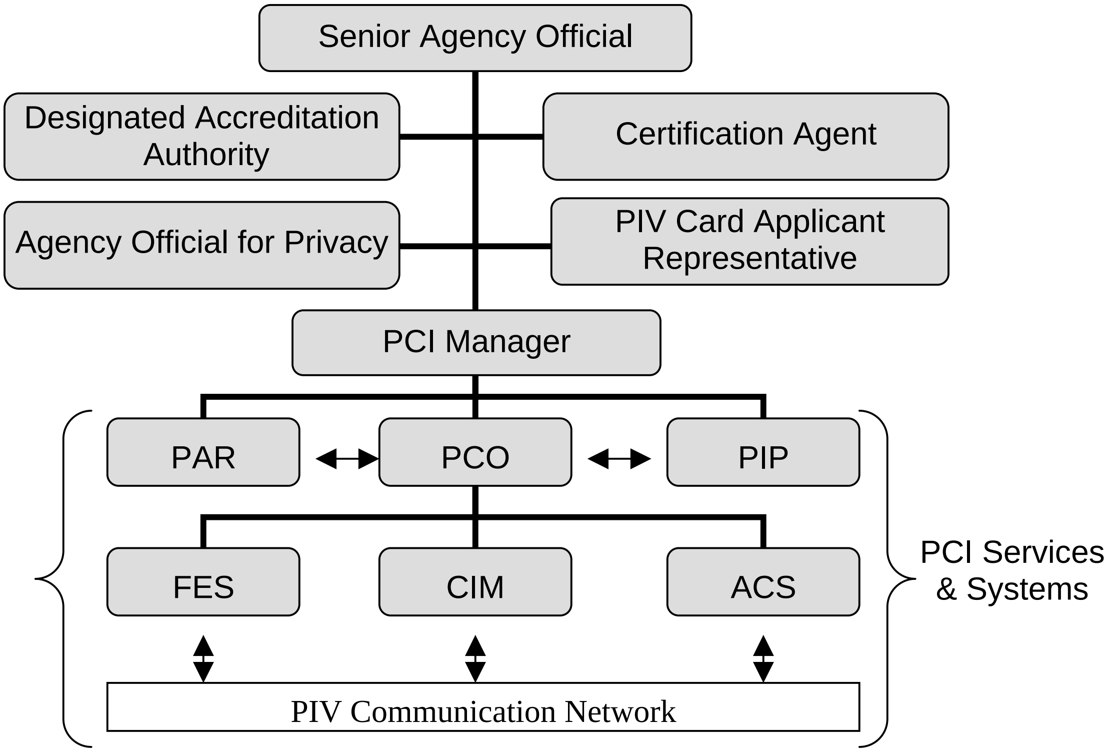
A simple model of a centralized PCI is depicted in Figure 2. This model could be used by a small, centralized agency that does not have remote facilities. An SAO has, or is assigned, the responsibility for creating or obtaining the services of a PCI. Several of the roles and responsibilities established by FIPS 201 can be fulfilled by one person, multiple people, or an entire organization. Most agencies will already have an AOP, a DAA and one or more Certification Agents. They may be assigned additional responsibilities for the PIV processes if appropriate. Agencies may already have a person or an organization for physical building access identity badges, for information systems access control, or both. The sample organization shows the services of Applicant identity proofing, registration, and Card issuance (including life cycle management) to be under a single manager but these responsibilities could be fulfilled by different managers with a coordinator or senior manager. For accreditation, the organizational structure is not as important as ensuring that there is a formal structure with clear lines of authority and the PCI is assessed for reliability assurance before PIV Cards are issued.

Figure 3 depicts a model of a distributed PCI. This model could be used by a large, geographically distributed agency having several remote facilities. A senior agency official that has jurisdiction and authority over all the facilities is depicted at the top of the organizational chart. An agency-wide DAA is shown that would be responsible for reviewing all the certification documentation of each of the PCI facilities and issuing an appropriate accreditation decision and documentation for each. However, each of the other roles is shown having one person or organization serving an agency-wide role (e.g., the AOP) with staff at each facility performing that role locally. These guidelines should be interpreted within the context of each agency, its mission(s), its organization structure, its geographical location(s), and its automated systems when selecting and performing the certification and accreditation procedures that are appropriate for that agency and its PCI(s) and using those that will provide the highest expectation of producing an accurate assessment of reliability.



DAA: Designated Accreditation Authority; PCI: PIV Card Issuer;
PSC: PCI Computer Support; ACS: Access Control Systems

Figure 1. A Logical View of the PIV System


Senior Agency Official
Designated Accreditation Authority
Certification Agent
Agency Official for Privacy
PIV Card Applicant Representative
PCI Manager
PAR
PCO
PIP
FES
CIM
ACS
PIV Communication Network
PCI Services & Systems

PAR: PIV Applicant Registrar; PCO: PIV Card Operations; PIP: PIV Identity Proofing; FES: PIV Front End System; CIM: Card Issuance & Management; ACS: Access Control System

Figure 2. Sample Centralized PIV Card Issuing Organization

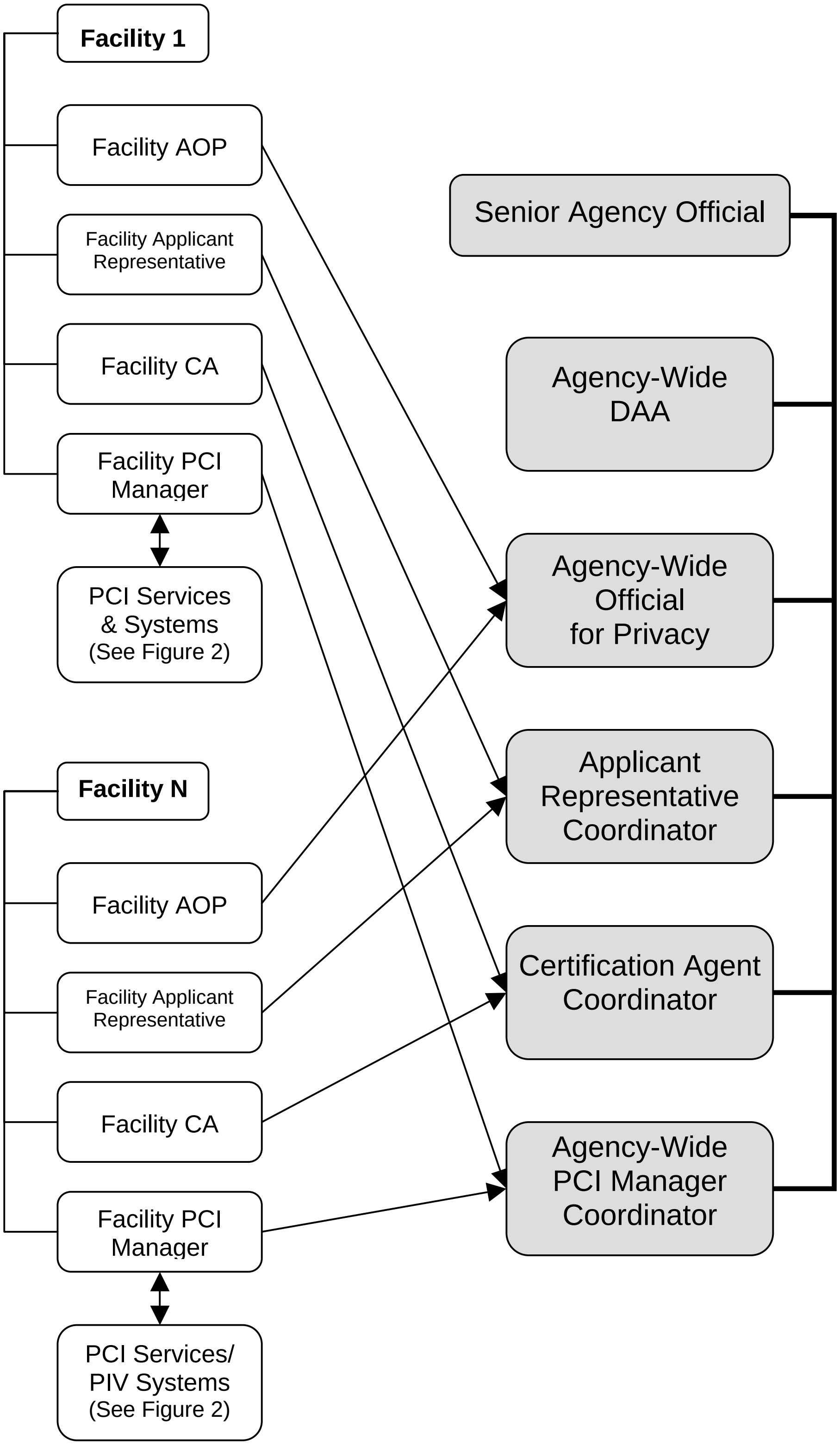

Facility 1
Facility AOP
Facility Applicant Representative
Facility CA
Facility PCI Manager
PCI Services & Systems (See Figure 2)
Facility N
Facility AOP
Facility Applicant Representative
Facility CA
Facility PCI Manager
PCI Services/ PIV Systems (See Figure 2)
Senior Agency Official
Agency-Wide DAA
Agency-Wide Official for Privacy
Applicant Representative Coordinator
Certification Agent Coordinator
Agency-Wide PCI Manager Coordinator

Figure 3. Sample Distributed PIV Card Issuing Organization

2.3 Accreditation Decisions

Accreditation recommendations resulting from certification processes should be conveyed to the DAA by the CA. To ensure the agency's business and operational needs are fully considered, the DAA should meet with the CA and the PCI Manager prior to issuing an accreditation decision to discuss the certification findings and the terms and conditions of the authorization. There are three accreditation alternatives that can be rendered by the DAA:

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

Authorization to Operate

If, after reviewing the results of the certification phase assessments, the DAA deems that PCI exhibits all the required attributes to an acceptable degree, an *authorization to operate* (ATO) is issued. The PCI is authorized to perform without restrictions or limitations those services that have been certified as being reliable. Re-accreditation should occur at the discretion of the DAA when significant changes occur in the PCI's status or within a specified time period (three years is recommended).

Interim Authorization to Operate

If, after reviewing the results of the certification phase assessments, the DAA 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 (IATO)* may be issued. An interim authorization to operate is rendered when the identified deficiencies in PCI procedures are significant but can be addressed in a timely manner. An interim authorization is an authorization to operate under specific terms and conditions. Re-accreditation should be initiated within three (3) months. PIV Cards issued during the Interim Authorization to Operate period should be noted in the PIV system so that agencies may determine if a requested access should be granted. No more than two (2) consecutive Interim Authorizations to Operate may be granted for a PCI. Failure to correct deficiencies for a third period should result in a Denial of Authorization to Operate.

A PCI is *not considered* accredited during the interim authorization to operate. When the deficiencies have been corrected, the interim authorization should be lifted and the PCI should be accredited. Monitoring phase activities should focus on the identified deficiencies. Significant changes in the status of the PCI that occur during the period of limited authorization to operate should be reported immediately to the DAA.

Denial of Authorization to Operate

If, after reviewing the results of the certification phase assessments, the DAA deems operation of the PCI to be unacceptable, a *denial of authorization to operate (DATO*) is transmitted to the PCI Manager. The PCI is not accredited and PIV Cards should not be issued. If the PCI is currently in operation, all issuance of PIV Cards should be halted. If the PCI was previously accredited and had issued PIV Cards under a ATO, the PIV Cards issued since the last accreditation should be marked in the PIV System (not on the Cards themselves) with a code that may be read by an access control system and used in making a decision to grant or deny a requested access. Cards so marked may be reviewed by an accredited PCI and the encoded mark in the PIV System may be removed if the Card's information and the Subscriber's identity are found to be correct. Failure to receive authorization to operate indicates that there are major deficiencies in the required attributes of the PCI. The DAA, CA, or their designated representatives should work with the PCI 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 DAA with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the PCI. Unless specifically designated otherwise by the DAA, the PCI Manager is responsible for the assembly, compilation, and submission of the accreditation package. The accreditation package contains the following documents:

- PCI's operational plan
- PCI's assessment reports
- PCI's corrective action plan

The PCI's ***operations plan*** that is prepared by the PCI Manager and previously approved by the SAO 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 PCI'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 PCI.

The PCI's attribute ***assessment reports***, prepared by the certification agent, provide the results of assessing the required attributes of the PCI 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*** (CAP), which is prepared by the PCI Manager, describes the measures that are being implemented— (i) to correct deficiencies noted during the assessment; and (ii) to reduce or eliminate vulnerabilities to the creation and issuance of secure PIV Cards.

The Manager submits the accreditation package to the DAA.[4] Figure 4 illustrates the primary sections of the accreditation package.

[4] 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.

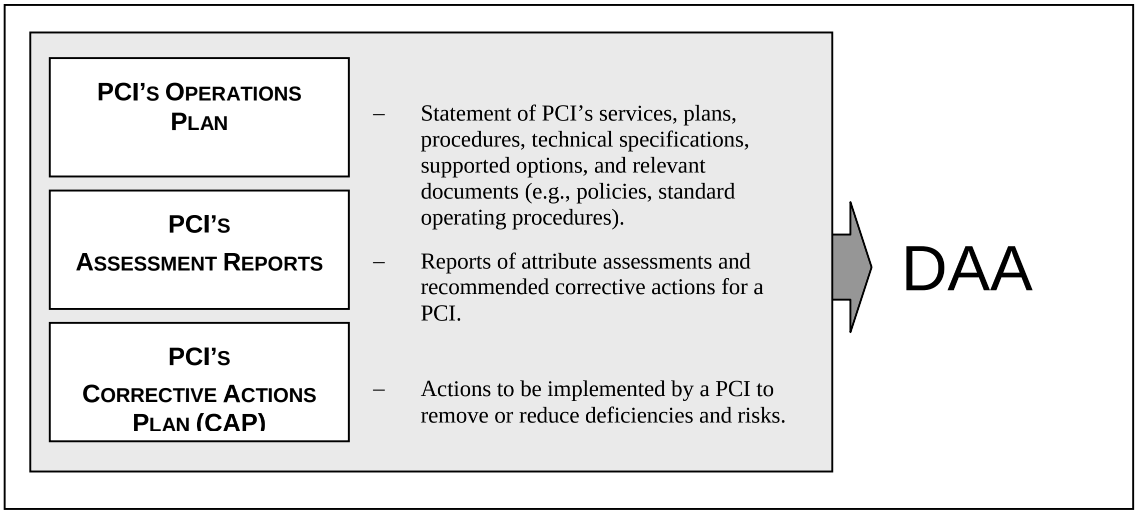

PCI's Operations Plan
– Statement of PCI's services, plans, procedures, technical specifications, supported options, and relevant documents (e.g., policies, standard operating procedures).
PCI's Assessment Reports
– Reports of attribute assessments and recommended corrective actions for a PCI.
PCI's Corrective Actions Plan (CAP)
– Actions to be implemented by a PCI to remove or reduce deficiencies and risks.
DAA

Figure 4. Accreditation Package

The accreditation decision letter transmits the accreditation decision from the DAA to the PCI Manager. The accreditation decision letter contains the following information:

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

The accreditation decision letter (see Appendix D for examples) indicates to the PCI 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 DAA's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the PCI. The accreditation decision letter is attached to the original accreditation package and provided to the PCI. A copy of the decision letter and the transmittal letter should be e-mailed to PIVaccreditation@nist.gov.

Upon receipt of the accreditation decision letter and accreditation package, the PCI manager should review the terms and conditions of the authorization. The DAA should also retain 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.

3.0 ATTRIBUTES OF PCIS AND ASSESSMENT METHODS

This chapter discusses the attributes that should be assessed when determining a PCI's reliability and the ability to comply with the requirements of FIPS 201.

3.1 Attributes

HSPD-12 requires that all PIV Cards be issued by providers whose reliability has been established through an official accreditation process. Reliability is the primary attribute to be exhibited and accredited in a PCI and is the characteristic of an organization that requires functions be performed and services provided as expected and that this expectation will continue in the future. ***A PCI's reliability should be evaluated and established by assessing that it is—***

- **Knowledgeable—** the characteristic of a person or organization of having both the ability and capacity of understanding all the management, documentation, document control, work flow, privacy, security, technical foundation, data, devices, communications, and electronic processing requirements in FIPS 201;

- **Capable—** the characteristic of a person or organization of 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.

- **Accountable—**the requirement of a person or organization for accepting responsibility for assigned tasks and then being held personally or organizationally responsible for performing the tasks successfully or for accepting the results of failing to accomplish them.

- **Available—** the characteristic that required functions and services will be performed, by the PCI, 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.

- **Well Managed—** possessing the abilities needed to plan, initiate, coordinate, and provide services required by FIPS 201 with the cooperation and support of all its operations personnel and staff.

- **Trustworthy—**the characteristic of a person or organization in which their statements may be accepted as being true without question and that their functions will be performed and services provided as advertised or expected.

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

- **Secure—**the characteristic of a person, organization, facility, or information system that safety, valuable asset protection, and sensitive and critical information assurance will be provided to the level desired and expected.

The following desired attributes of a PCI should similarly be exhibited and assessed**—**

- **Prepared/responsive/efficient—** characteristics of a person or organization exhibiting proper planning to be able to perform a service, capable of responding to it in a 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.

- **Cooperative—**characteristic of a person or organization to work with other people or organizations in performing a service without causing delay, anxiety, or frustration.

These organizational attributes or characteristics are not independent. They are defined to provide a foundation of attributes of a PCI 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 PCI 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 the recommended and additional selected methods of assessing the attributes, determine if they are presently in, and adequately exhibited by, the PCI now and determine if they 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 DAA and the accreditation requirement of HSPD-12 should be considered satisfied. If one or more of the required attributes are not present or not expected to continue in the future, then accreditation should be postponed or denied. If postponed, an action plan for improving the attribute or removing discrepancies between expectations and assessment should be produced and implemented within three months. Re-accreditation should then be initiated.

3.2 Assessment Methods

The following methods of assessment are described in the context of being used to determine if the required attributes of a PCI are adequately exhibited in order to achieve successful accreditation. They are common methods of assessing or evaluating an organization and comparing one organization with others seeking to provide products or services to consumers and customers. The following descriptions may be used by a DAA in selecting appropriate methods for establishing that the required attributes of the PCI 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/Observation—** a product producer or service provider showing an assessor how a product works or a service is performed.

- **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 of a product, service, or organization using a metric that is selected to produce a result useful for assessing a quality and reliability.

- **Compliance/conformance with standards—** analyzing a product, service, or organization 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 that it has become a de facto standard.

- **Comparison with peers—** assessing an attribute of a person or organization by comparing the result of an assessment with that of a similar person or organization; comparing the certification and accreditation documentation and results of one PCI against those of others to seek equivalence in operational capability and reliability and trust.

- **Experience—** assessing one or more attributes of an organization based on evaluating previously provided products or services similar or identical to those required by FIPS 201.

- **Testing/validation—** actively testing a product or service against a set of specifications using applicable test methods and metrics; validation is testing against a standard; PIV Cards produced by a PCI may be tested for quality and may be validated against the specifications of FIPS 201.

The methods of assessment described above should be used to verify that a PCI exhibits all required attributes in order to become accredited. The desirable attributes should also be assessed and included in a certification report but accreditation should not be denied if they are not adequately exhibited.

4.0 PCI FUNCTIONS AND OPERATIONS

The attributes and methods of assessment described in chapter three should be used to assess the reliability of PCI functions and operations. The primary PCI functions are overviewed in this document to give the DAA information about the expected operations needed to support services provided by a PCI. Certification and accreditation processes should look to determine the reliability of these functions and operations. Detailed technical specifications and service descriptions required of a PCI are provided in FIPS 201, and additional information is provided in the FICC Identity Management Handbook.

4.1 Planning

A ***PCI Manager*** plays a significant role and has major responsibilities in planning, initiating, operating, and managing a PCI 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. In addition, the Manager must be able to create 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 access to 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 by the CA.

4.2 Documentation

A PCI is required to collect, organize, store, and disseminate many documents important to its operations. 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. Appropriate references listed in Appendix A should be reviewed and analyzed to assure that the organization is operating in accordance with legal and standards requirements. Document management should be patterned after other experienced PCIs to show adherence to precedence. All of the documentation should be kept current.

- **Plans—** includes PCI’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 NIST 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 so that a PCI can 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 that their contents are protected, used only for authorized purposes, and be able to be retrieved at some later time for re-verification if needed.

- **Forms/Reports**— Various forms will be used to obtain information and reports will be produced to provide information. Agency officials may obtain or provide information in various ways without resorting to developing new forms whose formats may require prior approval.

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

4.3 Implementation

Subsequent to planning the services and documenting the needed operations of a PCI, the PCI Manager implements the operations plan. The following items should be addressed in the plan and will be assessed during the certification phase of the PCI.

Personnel

Obtaining knowledgeable, qualified, trustworthy, honest, and reliable personnel for the PCI is the first task of the PCI Manager. These people may already be operating the existing agency identity badge management system and may need only 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 PCI. They will need to be organized in a structure that supports the requirements of FIPS 201 and to be assigned the roles and responsibilities specified in that standard. Assessments of the required attributes of the PCI personnel may include interviews, direct observation, and testing for knowledge of FIPS 201 and organizational policy requirements.

Facilities

Adequate facilities are required to house and support—

- Personnel (Note— All actions pertaining to personnel recommended in these guidelines should be coordinated with appropriate agency Human Resource Management organizations.),

- 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, interviewing the operations staff, assessing the security of IIF storage facilities, and testing the computer system components in accordance with FIPS 201 requirements.

Equipment

Obtaining adequate and reliable equipment to support the services provided by the PCI 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, and ensuring that PIV system components have received validation certificates from NIST accredited testing laboratories.

Procurement

If adequate personnel, facilities, or equipment are not available, they must be procured by the PCI. 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 assessments attesting to these attributes may be used to assess the success of procurement. (Note— All action pertaining to procurement recommended in these guidelines should be coordinated with appropriate agency procurement organizations.)

4.4 Operation

A critical aspect of the certification and accreditation processes is the post-accreditation period involving the monitoring of the operations and status of the PCI. An effective monitoring program requires—

- Configuration management processes;
- Review and analysis of changes to the PCI’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 PCI 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 PCI changes and assessing their potential impact is an essential aspect of monitoring and maintaining 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 of the day-to-day operations of the PCI for periods selected on a random basis during certification.

5.0 PIV SERVICES AND OPERATIONS

The PCI attributes and methods of assessment described in chapter three should be used to assess the capabilities of a PCI and the reliability of its services and operations.

5.1 Applicant Identity Proofing and Registration

FIPS 201 Sections 2.2 and 5.2 require the adoption and use of an approved identity proofing and registration process. FIPS 201 Appendix A describes two models that satisfy the requisite PIV control objectives and requirements and are approved for PIV Identity Proofing and Registration.

The Role Based Model defines the roles that must be played by various individuals or organizations in order to prove the identity of an Applicant and then register the Applicant in the PIV System and then authorize the Applicant to be issued a PIV Card. The roles in this model are Applicant, PIV Sponsor, PIV Registrar, PIV Card Issuer, PIV Digital Signatory, and PIV Authentication Certification Authority. ***The roles of Applicant, Sponsor, Registrar, and PCI 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 (PCI). 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 PCI 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 PCI needs to implement and support only one approved model.

Applicant Interactions

Both identity proofing and registration approved models are designed to service PIV Card Applicants by processing their identity source documents and obtaining authorization for issuing a PIV Card to approved applicants in accordance with FIPS 201. A PCI must interact with the applicant at various times under various circumstances. An Applicant should be notified electronically or in writing of his/her responsibilities regarding identity proofing, registration/enrollment, and issuance of a PIV Card. An Applicant should be notified all his/her rights if a PIV Card is not approved. A PCI must be capable of assuring appropriate privacy to the Applicant and his/her IIF, fairness and consistency in processing PIV Card Applications, and protection of the Integrity and Confidentiality of information in the PIV System. The PCI should exhibit the attributes of being knowledgeable, capable, accountable, available, trustworthy and reliable in all dealings with an Applicant. These attributes should be assessed using document review and analysis, interviews, direct observation, sampling, evaluation, and accepted practice.

Notification of Responsibilities and Rights

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 Information in Identifiable Form (IIF), 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 Applicant should be notified of the responsibilities of holding a PIV Card and notified of requirements to protect it in accordance with agency, PCI, and the PIV System's policies and rules. Such rules/agreements should 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 his/her rights under all applicable laws, rules, regulations, directives, and policies. These include all privacy rights of the Applicant, including notification how the IIF 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 decisions based on them should be disclosed.

The PCI 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. To ensure protection of the rights of the Applicant as well as the security of the PIV System, the PCI should exhibit the attributes of being knowledgeable, accountable, legal, compliant, trustworthy, adequately supported, and secure. The most appropriate assessment methods include review and analysis of documented plans and procedures; assessing the knowledge of the PCI Manager and senior staff about laws, policies, human resource management requirements, and Applicant legal rights and responsibilities; interviews of Applicants (both successful and unsuccessful) selected using appropriate sampling and statistical practices; comparison of the PCI under assessment with peer PCIs; and verification of organizational adherence to established standards and SOPs. Interviews of Applicants and Applicant Representatives selected by approved statistical sampling techniques and of Applicant Representatives should be performed.

Application for a PIV Card

The following information should be 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 full name; date and place of birth; Identity Source Documents as required in FIPS 201; and other relevant information useful for proving the claimed identity of the Applicant. PCIs should exhibit knowledge of the Identity Proofing processing models and documentation requirements; legal rights of the Federal government and the applicant; be available and responsive to the needs of an Applicant and the Applicant's sponsor/employer; be compliant with standards of good practice; be trustworthy in handling of the Applicant's IIF; and be adaptable and cooperative in responding to an agency's needs. PCI attribute assessment methods should include review and analysis of application forms; interviews with sponsors, employers, registrars, Applicants, and Applicant Representatives; and comparison of experience with peer PCI's.

Authorization to Conduct Identity Proofing

The Applicant should be requested to authorize the PCI 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 that 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 PCI. The PCI must be knowledgeable and capable of identity proofing, trustworthy in performing sensitive applicant interviews and background reviews, available and accountable for performing the needed services, and cost effective in providing a potentially time consuming and expensive procedure. The most appropriate assessment methods should include review of documentation kept by PCI during the application process; comparison with peers in obtaining identity proofing results rapidly and efficiently; and testing of the procedures by submitting false claims of identity on a random basis.

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

Agency Interactions[5]

A PCI should be explicitly authorized by an agency to issue PIV Cards for its employees, its contractors, and other parties as defined in FIPS 201. One or more agencies may use the same PCI and one agency may utilize more than one authorized PCI (see Figure 1). There will be numerous interactions between an agency and its PCI(s).

The certification and accreditation processes specified in this document include initial and periodic interactions between the agency DAA and the PCI Manager, often through a CA that is an employee of the agency but not connected with the PCI. A primary goal of the PCI Manager and the PCI'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 established to optimize PIV Card adoption and utilization, and interviews of agency officials and PCI 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 PCI assessment method may be review of documentation kept by the PCI during the application process.

[5] One or more agencies may use the same PIV Card Issuer. In this case, only one accreditation is needed but the PCI policy and accreditation package should be reviewed and approved by all agencies that use the PCI's services.

Enrollment/Registration of Applicant

Subsequent to satisfactory completion of Applicant Identity Proofing, 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 PCI assessment method may be review of documentation kept by the PCI 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 PCI assessment method may be review of documentation kept by the PCI during the application process.

5.2 PIV Card Issuance

The PCI Manager is responsible for ensuring that PIV Cards are designed and produced in accordance with the requirements in FIPS 201 and of the agencies using the PCI's services. During the design and production planning, the PCI 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 PCI. 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 PCI 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, PCI System components, PIV Card Readers/Writers, and other materials needed to operate a competent and reliable PCI and set of services. The most appropriate PCI 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 PCI 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 PCI assessment methods include review and analysis of plans.

Validation testing should be performed on the first PIV Cards produced by a PCI 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. PCI assessment methods should include evaluation of the results of validation testing, sampling of PIV components tested and passed by the validation laboratory, and comparison with peers performing the testing services.

The PCI 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 standards' 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 PCI assessment methods include review and analysis of supplier contracts, testing and validation of the products, review and analysis of the experience of the supplier, accepted practice within the PIV component industry, and conformance with standards required for the products.

The PCI 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 PCI Manager and documented for later assessment. The appropriate PCI 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 the 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 PCI 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 PCI should 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 PCI in accordance with regulations and organizational requirements. The PCI 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 PCI 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 PCI assessment method may be review and analysis of plans and sampling and statistics of organizational adherence to established standards and SOPs.

The PCI Manager is responsible for ensuring 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 PCI. 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 PCI 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 PCI 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 PCI's documentation; and ensuring the availability of appropriate resources for the PCI. *The PCI 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.

5.3 PIV Card Life Cycle Management

The PCI 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 PCI assessment methods include review and analysis of reports and other documentation.

PCI vital records should include PIV Applicant Enrollment/Registration performance, status of recommended corrective actions, changes to the PCI'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 PCI assessment methods include review and analysis of plans and other records.

PCI personnel need to be reliable as determined by adherence to policies and standards including FIPS 201 and HSPD-12, by appropriate interviews, and by passing background checks and security clearances applicable to the position of the individual. The PCI's Manager should satisfy this requirement by determining the necessary education, experience, and areas of competence needed by employees and contractors. The CA should assess if the management and training of employees is being appropriately performed.

The PCI 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 PCI assessment method is direct observation and demonstration of the components, systems, and sub-systems. Comparison with peers and compliance with accepted practice should be used to assess that the facility is adequately supported, well managed, available when needed, secure and adaptable to change.

6.0 CERTIFICATION AND ACCREDITATION

Certification and accreditation consists 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., DAA, CA, PCI Manager,). Figure 5 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.

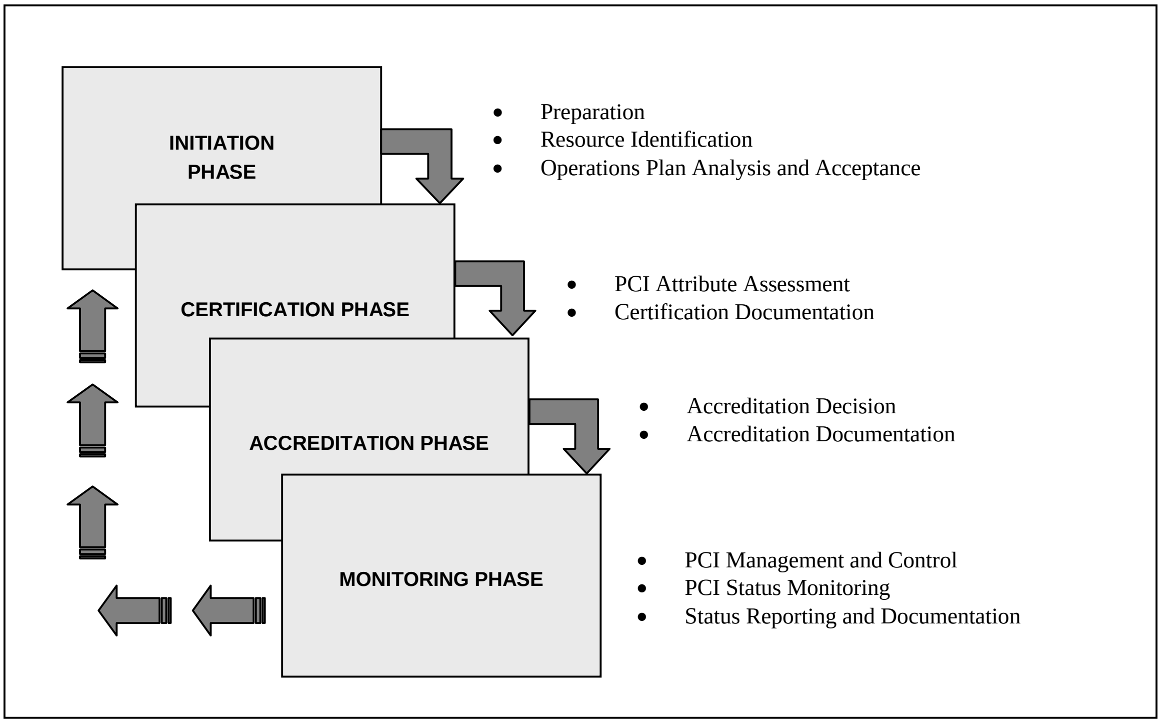


Figure 5. Certification and Accreditation Processes

6.1 Initiation Phase

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

Task 1: Preparation

The objectives of this task are to prepare for certification and accreditation by reviewing the PCI 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 PCI system has been fully described and documented in the PCI's operations plan.

Responsibility: PCI Manager

Guidance: A PCI description includes— (i) the names of the agencies sponsoring and using the PCI; (ii) a unique identifier for the PCI; (iii) the status of the operations plan; (iv) the name of the DAA; (v) contact information for the PCI

Manager; (vi) the applicable laws, directives, policies, regulations, and standards affecting the operations of the PCI; (vii) the PCI's organization chart; (viii) a description of the automated system(s) used by the PCI in performing the required services; (ix) a description of the network used for communicating with information systems and the PIV System; (x) encryption algorithms and cryptographic key types and sizes used for protecting information processing, transmission, and storage; (xi) identification of public key infrastructures and certificate authorities; (xii) the physical environment in which the PCI and supporting automated systems operate; and (xiii) the distributed, collaborative computing environments comprising the PIV System.

Subtask 1.2: Confirm that the applicability of the PCI's services and supporting automated system has been documented in the PCI's plan and that it is not categorized as National Security.

Responsibility: PCI Manager

Guidance: Consult NIST Special Publication (SP) 800-59, *Guideline for Identifying an Information System as a National Security System*, to confirm that the applicability of the PCI's services are not related to National Security.

Subtask 1.3: Confirm that the PCI has adopted and will use approved identity proofing and registration processes as required in FIPS 201 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 PCI operations plan and are used for performing the required services.

Responsibility: PCI 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 based on 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 PCI has adopted and will use approved PIV Card Issuance and Life Cycle maintenance procedures.

Responsibility: PCI Manager

Guidance: Section 2.3 of FIPS 201 requires the adoption and use of an approved PIV Card 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 objectives of the resource identification task are to— (i) identify and document the resources required for providing the services of FIPS 201 its specifications; and (ii) prepare a plan of certification and accreditation activities indicating the proposed schedule and key milestones.

Subtask 2.1: Identify the DAA, AOP, CA(s), PIV Applicant representative(s), 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: PCI Manager

Guidance: Identification of key agency officials is an important activity to establish that certification and accreditation processes are an integral part of the PCI system development life cycle and to verify that they will be participating in the processes. Identification and role assignments serve as a notification that the officials will be participants in the upcoming certification and accreditation tasks.

Subtask 2.2: Determine the resources required for the certification and accreditation of the PCI services and supporting automated system and prepare a plan of execution.

Responsibility: PCI Manager; DAA

Guidance: The level of effort required for certification depends on— (i) the size the PCI; (ii) its location and proximity to the agency personnel being served; (iii) the history and status of the PCI; 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 essential and is typically integrated within development life cycle and capital planning and budgeting processes. Once a CA is selected (or certification services procured), an execution plan for conducting the certification and accreditation is prepared by the CA in conjunction with the PCI Manager and DAA. 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: Operations Plan Analysis and Acceptance

The objectives of the operations plan analysis and acceptance task are to— (i) perform an analysis of the PCI attributes required and desired by the senior agency officials; (ii) obtain an independent analysis of the PCI operations plan and revise as needed; and (iii) obtain acceptance of the plan by the DAA prior to conducting an assessment of the attributes of the organization.

Subtask 3.1: Review the list of desired attributes of a PCI described in these guidelines and select those that should be exhibited by the PCI in addition to the required attributes in order to satisfy agency requirements.

Responsibility: DAA; CA

Guidance: HSPD-12 specified that the reliability of a PCI be officially accredited before it could issue PIV Cards. Reliability includes all required attributes. The attributes to be exhibited by an accredited PCI must be specified by the agency using a PCI'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 PCI.

Responsibility: CA

Guidance: The CA(s) should review FIPS 201 and these guidelines to select methods and procedures for assessing the required and desired attributes of the PCI. The CA, as directed by the DAA, may supplement these assessment methods and procedures as desired by the agency using the services of the PCI. Assessment methods and procedures may need to be created or tailored for assessing additional attributes of, or services provided by, a PCI.

Subtask 3.3: Analyze the PCI operations plan to determine if there are vulnerabilities that would result in not satisfying all the policies, procedures, and other requirements in FIPS 201 and of the agency being serviced by the PCI if the plan was implemented properly and the specified operations performed as planned.

Responsibility: DAA; CA

Guidance: The PCI operations plan should specify the PIV Applicant vetting; identity source document proofing; and PIV Card creation, issuance, and life-cycle management services and procedures of the PCI. The independent analysis of the plan by the CA and review by the DAA determine if the plan is complete and consistent with the requirements of FIPS 201. The CA and DAA can then determine if potential risks vulnerabilities in the provided services and automated support system appear to be adequately assessed, countered, and that the residual risks are reasonable. Based on the results of the analysis by the CA and review by the DAA, changes to the operations plan should be recommended to the PCI Manager.

Subtask 3.4: Accept the PCI operations plan as acceptable.

Responsibility: DAA

Guidance: If the PCI operations plan and the residual risks are deemed acceptable, the DAA accepts the plan. Acceptance allows the certification and accreditation processes to advance to the next phase. Acceptance of the PCI 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) PCI attribute assessment; and (ii) certification documentation. The purposes of this phase are 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 PCI. This phase also specifies actions to be taken to correct deficiencies in the operations of the PCI and to minimize risks and mitigate vulnerabilities. Upon successful completion of this phase, the DAA will have the information needed from the certification activities to recommend the appropriate accreditation decision.

Task 4: PCI Services and Attribute Assessment

The objectives of this task are to— (i) initiate assessments of the required and desired attributes of the PCI; (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 CA should determine that the specified attributes of the PCI 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 PCI. The CA should also be in a position to make recommendations on corrective actions for discovered deficiencies and offer advice to the PCI Manager and DAA on how to proceed with the certification.

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

Responsibility: PCI Manager; CA

Guidance: The PCI Manager should assist the CA 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 PCI. Supporting materials include PCI policies, the approved PCI service description and operations plan, relevant standards, guidelines, identity management handbooks, documentation available from other previously accredited PCIs, and any records showing evidence of the required and desired attributes of the PCI. Assessment results from validation programs that test and evaluate features of commercial PIV components and products are especially important. If assessment results of similar PCI support systems are available, the CA may incorporate those results into the certification. CAs should maximize the use of previous assessment results whenever feasible.

Subtask 4.2: Assess the required and desired attributes of the PCI using methods and procedures selected or developed.

Responsibility: CA

Guidance: Assessment should determine the extent to which the attributes are inherent in, or exhibited by, the PCI. The results of the assessments, including recommendations for correcting any deficiencies in the attributes of the PCI, PIV Card services offered, or procedures used should be documented in the assessment report.

Subtask 4.3: Prepare the assessment report.

Responsibility: CA

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 PCI operations plan and corrective actions plan (CAP). The assessment report is the CA's statement regarding the capabilities and reliability, among other required and desirable attributes, of the PCI.

Task 5: Certification Documentation

The security certification documentation task— (i) provides the certification findings and recommendations to the PCI Manager; (ii) recommends revision of the PCI's plan as needed; (iii) prepares the CAP (including milestones); and (iv) assembles the accreditation package. The PCI Manager has an opportunity to reduce or eliminate vulnerabilities in the PCI operations plan prior to the assembly of the accreditation package and submission to the DAA. This is accomplished by implementing corrective actions recommended by the CA. The CA should assess service modifications or enhancements added during this process.

Subtask 5.1: Provide the PCI Manager with the certification report.

Responsibility: CA

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

Subtask 5.2: Revise the PCI operations plan.

Responsibility: PCI Manager

Guidance: The PCI operations plan should reflect changes made in response to recommendations for corrective actions from the CA. 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 PCI considered to be required or desirable will be continued throughout the life cycle of the organization.

Subtask 5.3: Prepare the CAP.

Responsibility: PCI Manager

Guidance: The CAP, one of the three primary documents in the accreditation package, describes actions to be taken by the PCI Manager to correct deficiencies identified in the Certification phase. The CAP 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 DAA.

Responsibility: PCI Manager; CA

Guidance: The PCI Manager is responsible for the assembly and compilation of the accreditation package with inputs from the CA. The accreditation package contains— (i) the assessment report from the CA providing the results of the assessment of the attributes of the PCI and recommendations for corrective actions if needed; (ii) the CAP from the PCI Manager; and (iii) the revised PCI operations plan. Certification agent input to the accreditation package provides an independent assessment of the capabilities and reliability, along with the other required and desired attributes, of the PCI in fulfilling all FIPS 201 requirements. The PCI Manager may also wish to consult with other key agency participants (e.g., the AOP and the PIV Applicant's representatives) prior to submitting the final accreditation package to the DAA. The DAA should use this information during the Accreditation Phase to determine if the PCI procedures, operations, and reliability should be accredited and that the PCI should be 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 PCI Manager will have— (i) an authorization to operate the PCI services defined in its operations plan; (ii) an interim authorization to operate under specific terms (e.g., three (3) months) and conditions; or (iii) a denial of authorization.

Task 6: Accreditation Decision

The accreditation decision task determines if the certification phase has resulted in a recommendation to authorize operation of the PCI in accordance with the operations plan. The DAA, working with the CA and the assessments produced during the previous phase, reviews the identified vulnerabilities and the CAP to reduce or eliminate those vulnerabilities. This information 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 PCI's vulnerabilities and the CAP and perform a final certification review.

Responsibility: DAA

Guidance: The DAA receives the final accreditation package from the PCI Manager or the CA. The vulnerabilities in the PCI should be assessed by the CA to determine how those particular vulnerabilities translate into risk to agency operations, agency assets, or individuals. The DAA should judge which PCI vulnerabilities are of greatest concern to the agency and which vulnerabilities can be tolerated without creating unreasonable agency-level risk. The CAP should also be considered in determining the risk to the agency. The DAA may consult the PCI manager, CA, 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, that the required and desired attributes are exhibited as needed, that the reliability of the PCI has been adequately assessed, and prepare the final accreditation decision letter.

Responsibility: DAA

Guidance: The DAA 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 DAA 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 DAA deems that the agency-level risk is acceptable, an authorization to operate is issued. The PCI is accredited without any restrictions or limitations on its operation.

If, after assessing the results of certification, the DAA deems that the agency-level risk is unacceptable, but there is an important mission-related need to place the PCI into operation, an interim authorization to operate may be issued. The interim authorization to operate is a limited authorization under specific terms and conditions (e.g., a three (3) month duration) including corrective actions to be taken by the PCI Manager and a required timeframe (e.g., two (2) months) for completion of those actions. A detailed CAP should be submitted by the PCI Manager and CA and approved by the DAA prior to the interim authorization to operate taking effect. The PCI is not accredited during this period. The PCI Manager is responsible for completing the corrective actions identified in the CAP and resubmitting an updated accreditation package upon completion of those actions.

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

The DAA's 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 PCI'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 DAA'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 PCI's operations plan.

Subtask 7.1: Provide copies of the final accreditation package including the accreditation decision letter, in either paper or electronic form, to the PCI Manager and any other agency officials having interests, roles, or responsibilities in the PIV System. A copy of the submittal letter and the selected authorization letter should be forwarded electronically to PIVaccreditation@nist.gov when they are delivered to the intended recipient.

Responsibility: DAA

Guidance: The accreditation package including the accreditation decision letter is transmitted to the PCI manager. Upon receipt of the accreditation decision letter and accreditation package, the PCI manager reviews the terms and conditions of the authorization. The original accreditation package is kept on file by the PCI manager. The DAA retains copies of the decision letter and accreditation package. The accreditation package should be appropriately safeguarded and stored, whenever possible, in a centralized agency filing system to ensure accessibility. The accreditation package should be readily available to auditors and oversight agencies upon request. The accreditation package should be retained in accordance with the agency's records retention policy.

Subtask 7.2: Update the PCI's operations plan.

Responsibility: PCI Manager

Guidance: The operations plan should be updated to reflect any changes made as the result of the C&A processes. Any conditions set forth in the accreditation decision should also be noted in the plan. Any PIV Card issued by a PCI (i) between accreditation and the loss of accreditation; and/or (ii) during a three-month period of operation with an interim authorization should be encoded in the PIV system with an appropriate warning to any agency making an access control decision based on the PIV Card.

6.4 Monitoring Phase

The Monitoring Phase consists of three tasks— (i) PCI management and control; (ii) PCI status monitoring; and (iii) status reporting and documentation. The purposes of this phase are to provide oversight and monitoring of the day-to-day operations of the PCI on an ongoing basis and to inform the DAA 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 agency policies require periodic re-accreditation or independent accreditation of the PIV system or its components. No more than three (3) years should pass between PCI reliability accreditations.

Task 8: PCI Management and Control

The objectives of the PCI management and control task are to— (i) document proposed or actual changes to the PCI and its operations plan; and (ii) determine the impact of proposed or actual changes on the services, operations, and reliability of the PCI. 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: PCI Manager

Guidance: An orderly and disciplined approach to managing, controlling, and documenting changes to PCI policies, procedures, services, and support systems is critical to the assessment of the PIV Card life cycle management of the PCI. 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 PCI Manager should use this documentation in assessing the potential impact of changes to the required and desired attributes of the PCI. Significant changes should not be undertaken without assessing impact of such changes.

Subtask 8.2: Analyze the proposed or actual changes to the PCI (including hardware, software, firmware, and surrounding environment) services and operations and analyze them to determine the impact of such changes.

Responsibility: PCI Manager

Guidance: Changes in the PIV System may affect the operations of the PCI, produce new vulnerabilities in the system, or generate requirements for new procedures. If the results of the impact analysis indicate that changes to the PCI could affect the PCI's operations, corrective actions should be initiated and the CAP updated. The DAA or the PCI Manager should consult with potentially affected agency officials prior to making the changes.

Task 9: PCI Status Monitoring

The objectives of the monitoring task are to— (i) select an appropriate set of attributes to be monitored; and (ii) assess the selected attributes using methods and procedures selected by the PCI 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 PCI to be monitored.

Responsibility: PCI Manager

Guidance: The attributes of the PCI established by the PCI 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 DAA and PCI 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 sensitivity of the assets being protected by PIV Cards, and the risks remaining in the PCI (i.e., the level of effort should be increased corresponding to increases in the potential impact on agency operations, agency assets, or individuals increases).

Subtask 9.2: Assess the required and selected desired attributes to determine the extent to which they are exhibited by the PCI 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: DAA, PCI 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 PCI's attributes during the monitoring process are at the discretion of the DAA coordinating with the PCI Manager. The monitoring process should be documented and available for review by the DAA, an 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 PCI, corrective actions should be initiated and the CAP updated.

Task 10: Status Reporting and Documentation

Status reporting and documentation includes— (i) updating the PCI's operations plan to reflect changes that could affect the reliability of the PCI and; (ii) updating the CAP based on the results of assessments conducted during the monitoring phase; and (iii) reporting the status of the PCI's reliability critical and desirable attributes and experiences (problems and successes) to the DAA. 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 specified requirements (e.g., re-accreditation should be performed at least every three (3) years).

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

Responsibility: PCI Manager

Guidance: The PCI's operations 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 PCI 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 DAA, PCI Manager and CA should use the plan to guide future certification and accreditation activities.

Subtask 10.2: Update the CAP based on the documented changes to the operations plan and the results of the monitoring process.

Responsibility: PCI Manager

Guidance: The CAP is used by the DAA to monitor progress in correcting deficiencies noted during certification. The CAP should— (i) report progress in correcting deficiencies noted in the operations plan; (ii) address vulnerabilities in the PCI discovered during monitoring; and (iii) describe how the deficiencies will be corrected and the vulnerabilities eliminated or minimized.

Subtask 10.3: Report the status of the PCI to the DAA.

Responsibility: PCI Manager

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

APPENDIX A: REFERENCES

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

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

United States Office of Management and Budget, *Circular No. A-130*, Appendix III, Security of Federal Automated Information Resources, February 1996.
(Available at http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.
(Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Security Controls for Federal Information Systems*, projected for publication December 2005.
(Will be available at http://csrc.nist.gov/publications.)

Committee for National Security Systems, Instruction 4009, *National Information Assurance Glossary*, Revised May 2003.
(Available at http://staff.washington.edu/dittrich/center/4009.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, February 2005.
(Available at http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
(Available at http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* Version 2.0, June 2003 draft.
(Available at http:/csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, Version 1.9, October 2003.
(Available at http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.)

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

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-73, *Interfaces for Personal Identity Verification*, April 2005.
(Available at http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf .)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, Draft, February 2005.
(Available at http://csrc.nist.gov/piv-project/fips201-support-docs/SP800-76-Draft.pdf.)

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, March 2005.
(Available at http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf.)

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

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.
(Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.)

Federal Identity Credentialing Committee, *Federal Identity Management Handbook*, Draft Version 0.2, March 2005.
(Available at http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf.)

APPENDIX B: GLOSSARY AND ACRONYMS

Terminology as used in this document	Definition or explanation of term
Access Control	The process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Accreditation (as applied to a PCI)	The official management decision of the Designated Accreditation Authority to authorize operation of a PCI after determining that the PCI's reliability has satisfactorily being established through appropriate assessment and certification processes.
Accreditation Package	The evidence and supporting documentation 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.
AOP	Agency Official for Privacy
Applicant	An individual applying for a PIV Card/credential. The Applicant may be a current or prospective Federal employee or contractor.
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a PCI.
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 PCI are exhibited.
ATO	Authorization to Operate
Authorization to Operate (ATO)	One of three possible decisions concerning a PCI made by a Designated Accreditation Authority after all certification activities have been performed stating that the reliability of the PCI is accredited and the PCI is authorized to perform specific PIV services.
Authorizing Official	See Designated Accreditation Authority
CA	Certification Agent

Terminology as used in this document	Definition or explanation of term
CAP	Corrective Action Plan of a PCI for removing or reducing deficiencies or risks during PCI operations.
Certification (as applied to a PCI)	Certification in this context means a formal process of assessing the attributes (e.g., knowledge, availability, accountability, trustworthy, security) of a PCI using various methods of assessment (e.g., interviews, document reviews, test results, evaluations, validation reports) that support the assertion that a PCI is reliable and capable of identity proofing and enrolling approved applicants and issuing PIV Cards in accordance with FIPS 201.
Certification Agent (CA)	The individual, group, or organization responsible for conducting certification activities under the guidance and direction of a Designated Accreditation Authority.
Component	An element of a large system, such as an identity card, PCI, PIV Registrar, card reader, or identity verification support, within the PIV system.
Corrective Action Plan	The document that identifies corrective action tasks that need to be performed in order to obtain or sustain accreditation.
Credential	Evidence attesting to one’s right to credit or authority; in FIPS 201, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
DAA	Designated Accreditation Authority (also called an Authorizing Official)
DATO	Denial of Authorization to Operate; issued by a DAA to a PCI that is not accredited as being reliable and capable of issuing PIV Cards.
Designated Accreditation Authority	A senior agency official that has been given the authorization to accredit the reliability of a PCI.
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive; HSPD-12 established the policy for which FIPS 201 was developed.

Terminology as used in this document	Definition or explanation of term
IATO	Interim Authorization to Operate a PCI performing specified services (e.g., identity proofing and registration, issuing PIV Cards).
Identification	The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.
Identifier	Unique data used to represent a person’s identity and associated attributes. A name or a card number are examples of identifiers.
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
Identity Proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.
Identity Registration	The process of making a person’s identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person’s relevant attributes into the system.
Identity Verification	The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.
IIF	Information in Identifiable Form
Information in Identifiable Form	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. [E-Gov]
IPR	Identity Proofing and Registration; verifying the claimed identity of an Applicant by authenticating the identity source documents provided by the Applicant and then entering the information into the PIV system needed to authorize access for the Applicant.
ISD	Identity Source Document
Issuer	An organization that is authorized and accredited to issue PIV Cards to approved Applicants. See PIV Card Issuer.

Terminology as used in this document	Definition or explanation of term
ITL	Information Technology Laboratory
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
PCI	PIV Card Issuer
PCI Manager (or Agency Identity Management Official)	The individual, or group of individuals in a distributed PCI, responsible for the operations required of Identity Proofing and PIV Card Issuance as specified in FIPS 201 and for performing certain roles and responsibilities as specified in these Guidelines.
PCI support automated system	The automated (computer-based) system used by a PCI 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	Personal Identity Verification as specified in FIPS 201.
PIV Card	A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity markers or credentials (e.g., photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Terminology as used in this document	Definition or explanation of term
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 PCI.
PIV Card Issuer	An authorized PIV Card issuing organization that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.
PIV Registrar	An entity that establishes and vouches for the identity of an Applicant to a PIV Card Issuer. The PIV Registrar authenticates the Applicant’s identity by checking identity source documents and identity proofing, and ensures a proper background check has been completed, before the Card is issued.
PIV Sponsor	An individual who can act on behalf of a department or agency to request that a PIV Card be issued to an Applicant after appropriate identity authentication and background checks.
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 PCIs to store the data about PIV Subscribers that is needed by all 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.
SAO	Senior Agency Official
SP	Special Publication

Terminology as used in this document	Definition or explanation of term
Subscriber	A person who was a PIV Card Applicant who passed all identity proofing and registration requirements, was issued a PIV Card, and is now an authorized participant in the PIV System.
Trustworthiness	The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Appendix C: Certification and Accreditation Tasks for PIV Card Issuing Organizations (PCIs)

Phases, Tasks, and Subtasks	Person(s) Responsible
Initiation Phase	
Task 1: Preparation	
Subtask 1.1: PCI Operations Plan Review	PCI Manager
Subtask 1.2: PCI National Security Categorization	PCI Manager
Subtask 1.3: Identity proofing and registration Processes Review	PCI Manager
Subtask 1.4: PIV Card Issuance and Life Cycle Review	PCI Manager
Task 2: Resource Identification	
Subtask 2.1: C & A Personnel Identification	PCI Manager
Subtask 2.2: C & A Resources Identification	PCI Manager, DAA
Task 3: Operations Plan Analysis and Acceptance	
Subtask 3.1: PCI Desired Attributes Selection	DAA, CA
Subtask 3.2: Assessment Methods and Procedures	CA
Subtask 3.3: PCI Operations Plan Analysis	DAA, CA
Subtask 3.4: PCI Operations Plan Acceptance	DAA
Certification Phase	
Task 4: PCI Attribute Assessment	
Subtask 4.1: Documentation and Supporting Materials	PCI Manager, CA
Subtask 4.2: Attribute Assessment	CA
Subtask 4.3: Attribute Assessment Report	CA
Task 5: Certification Documentation	
Subtask 5.1: Findings and Recommendations	CA
Subtask 5.2: PCI Operations Plan Update	PCI Manager
Subtask 5.3: Corrective Action Plan (CAP) Preparation	PCI Manager
Subtask 5.4: Accreditation Package Assembly	PCI Manager, CA

Phases, Tasks, and Subtasks	Person(s) Responsible
Accreditation Phase	
Task 6: Accreditation Decision	
Subtask 6.1: Final Certification Review	DAA
Subtask 6.2: Determine Attribute (Reliability) Acceptability	DAA
Task 7: Accreditation Documentation	
Subtask 7.1: Accreditation Package Transmission	DAA
Subtask 7.2: PCI Operations Plan Update	PCI Manager
Monitoring Phase	
Task 8: PCI Management and Control	
Subtask 8.1: Documentation of PCI Operations Plan Changes	PCI Manager
Subtask 8.2: Services and Operations Analysis	PCI Manager
Task 9: PCI Status Monitoring	
Subtask 9.1: Attribute Selection	PCI Manager
Subtask 9.2: Selected Attribute Assessment	DAA, PCI Manager
Task 10: Status Reporting and Documentation	
Subtask 10.1: Update PCI's Operations Plan	PCI Manager
Subtask 10.2: Update CAP	PCI Manager
Subtask 10.3: Report Status of PCI to DAA	PCI Manager

APPENDIX D: SAMPLE TRANSMITTAL AND DECISION LETTERS

Sample Certification/Accreditation Package Transmittal Letter

From: PCI Manager Date:

To: Designated Accreditation Authority (DAA)

Subject: PCI Accreditation Package for [PCI]

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

The PCI operations plan, its procedures, and its attributes have been assessed by [CERTIFICATION AGENT] using the assessment methods and procedures defined in SP 800-79 and specified in the assessment report to determine the extent to which the required and desired attributes of a capable and reliable PCI are exhibited and if the PIV Card issuing procedures are operating as intended and producing the desired results. The CAP describes the corrective actions that we plan to perform to remove or reduce any remaining deficiencies detected in the PCI's procedures and attributes.

Signature

Title

Sample Accreditation Decision Letter (Authorization to Operate)

From: Designated Accreditation Authority Date:

To: PCI Manager

Subject: Accreditation Decision for [PCI MANAGER]

After reviewing the results of the certification and accreditation package of the [PCI] and its supporting automated PIV system support components located at [LOCATION] and the evidence provided in the associated accreditation package, I have determined that the PCI's plan and procedures and capabilities are in compliance with FIPS 201 and our privacy and security policies and are acceptable. Accordingly, I am issuing an *authorization to operate* (ATO) the PCI's services in its existing or specified operating environment. The PCI is accredited without any significant restrictions or limitations. This accreditation is my formal declaration that adequate attributes are being exhibited by the PCI, that a satisfactory level of capability and reliability is present, and that the PCI is expected to this maintain this capability, reliability, and operational status for at least the next three years or until a major change is made to its operation.

This accreditation and ATO will remain in effect as long as— (i) the required monitoring is performed and status reports for the PCI are submitted to this office every [TIME PERIOD – ONE YEAR IS RECOMMENDED]; (ii) the problems detected during the monitoring process do not result in agency-level risks that are unacceptable; and (iii) the capability and reliability of the PCI is re-accredited within the lesser time of three (3) years or the re-accreditation requirements established by 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

Sample Accreditation Decision Letter (Interim Authorization to Operate)

From: Designated Accreditation Authority Date:

To: PCI Manager

Subject: Accreditation Decision for [PCI]

After reviewing the results of the certification of the [PCI] and its supporting automated PIV system support components located at [LOCATION] and the evidence provided in the associated accreditation package, I have determined that the required attributes exhibited by the [PCI] are *not* acceptable. However, I have determined that there is an overarching need for the PCI to provide the needed services due to mission necessity and other considerations. Accordingly, I am issuing an *interim authorization to operate* (IATO) the PCI services in its existing operating environment. Operation of the PCI must be performed in accordance with the enclosed terms and conditions during the IATO period and all detected risks of operation and problems encountered during operation should be documented. The PCI is *not* considered accredited during the IATO period.

Reliability of the PCI operations and security of the PCI's automated support systems must be monitored rigorously during the IOTA period. Monitoring activities should focus on the specific areas of concern identified during the certification assessments. Significant changes in the status of the operations during the IOTA period should be reported immediately. All PIV Cards issued by the PCI during this period should be marked in the PIV System so that agencies accepting the Cards for access control decisions are aware they were issued by the PCI during an IOTA period. Once accreditation is obtained by the PCI, these Cards should be examined and the marking removed for the Cards that are determined to meet the requirements of the accredited PCI.

This interim authorization to operate is valid for a maximum of three (3) months. The limited authorization will remain in effect as long as— (i) the required status reports for the system are submitted to this office every month; (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 CAP. At the end of the IOTA period, the PCI must either be certified and accredited and authorized to operate or the authorization for further operation will be denied. A second IOTA will be granted only under extenuating circumstances. This office will review the CAP submitted with the accreditation package during the IOTA period and monitor progress on removal or reduction of concerns and discrepancies before re-accreditation is initiated.

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

Signature

Title

Sample Accreditation Decision Letter (Denial of Authorization to Operate)

From: Designated Accreditation Authority Date:

To: PCI Manager

Subject: Accreditation Decision for [PCI Manager]

After reviewing the results of the certification of the [PCI] located at [LOCATION] and the supporting evidence provided in the associated accreditation package, I have determined that the attributes exhibited by the PCI are unacceptable. Accordingly, I am issuing a denial of authorization to operate (DATO) the PCI in its planned or existing operating environment. The PCI is *not* accredited and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED].

The Corrective Action Plan (CAP) should be pursued immediately to ensure that proactive measures are taken to correct the deficiencies found during the assessment. Re-certification and re-accreditation should be initiated 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