GSA U.S. General Services Administration

**PIV Card Delivery
Approval Procedure**
VERSION **9.0.0**

**April Giles
Nabil Ghadiali**

GSA FIPS 201 APPROVED

FIPS 201 EVALUATION PROGRAM

October 31, 2007

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	04/21/06	Document creation	Limited
Draft	0.1.0	04/21/06	Submitted to GSA for approval	GSA
Draft	0.1.1	05/02/06	Updated based on GSA feedback	Limited
Draft	0.1.2	05/03/06	Updated based on internal feedback	Limited
Draft	0.2.0	05/03/06	Submitted to GSA for approval.	GSA
Approved	1.0.0	05/10/06	Approved by GSA	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval	GSA
Revision	1.1.1	06/30/06	Updated based on feedback from GSA	Limited
Revision	1.2.0	06/30/06	Submitted to GSA for approval	GSA
Approved	2.0.0	06/30/06	Approved by GSA	Public
Revision	2.1.0	09/12/06	Updated based on feedback from the Evaluation Lab	GSA
Approved	3.0.0	09/20/06	Approved by GSA	Public
Revision	3.1.0	11/28/06	Updated based on preliminary Site Visit	Limited
Approved	4.0.0	12/14/06	Approved by GSA	Public
Approved	5.0.0	02/09/07	Updated definition for clarification of PIV Card Delivery Service; Updated to include process for product updates, resubmissions and evaluation fees	Public
Revision	5.1.0	02/15/07	Updated Vendor Documentation and Site Visit mechanism evaluation procedures for clarity.	GSA
Revision	5.2.0	02/19/07	Updated based on feedback from GSA and the Lab	GSA
Approved	6.0.0	02/22/07	Approved by GSA	Public
Approved	7.0.0	04/02/07	Updated with details for the evaluation fees.	Public
Approved	8.0.0	04/26/07	Updated with details for the upgrade process.	Public
Approved	9.0.0	10/31/07	Updated to split approval processes from document. Processes can now be found in Suppliers Handbook.	Public

Table of Contents

List of Tables

1   Introduction

1.1   Overview

The FIPS 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. In addition to derived test requirements developed to test conformance to the National Institute of Standards and Technology (NIST) Standard, GSA has also established interoperability and performance metrics to further determine product suitability. A set of approval and test procedures have been developed which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category.

A Supplier desiring to submit a PIV Card Delivery (hereafter referred to as the Service) for evaluation must follow the Suppliers Policies and Procedures Handbook. In addition to this handbook, Supplier also need to refer to this Approval Procedure which provides the necessary category-specific details in order to have a Supplier's Product evaluated by the EP and placed on the Approved Products List (APL).

1.2   Category Description

The *PIV Card Delivery* is a service that delivers personalized PIV cards to cardholders. The delivery service entails verification of the identity of the cardholder (whom the background check was completed) to credentials found on the personalized card. PIV Card Delivery provides the necessary services to deliver those cards to the respective applicants in accordance with the requirements of FIPS 201. The diagram below depicts the functions of various service providers. The PIV Card Delivery service is shown in the lower right corner.
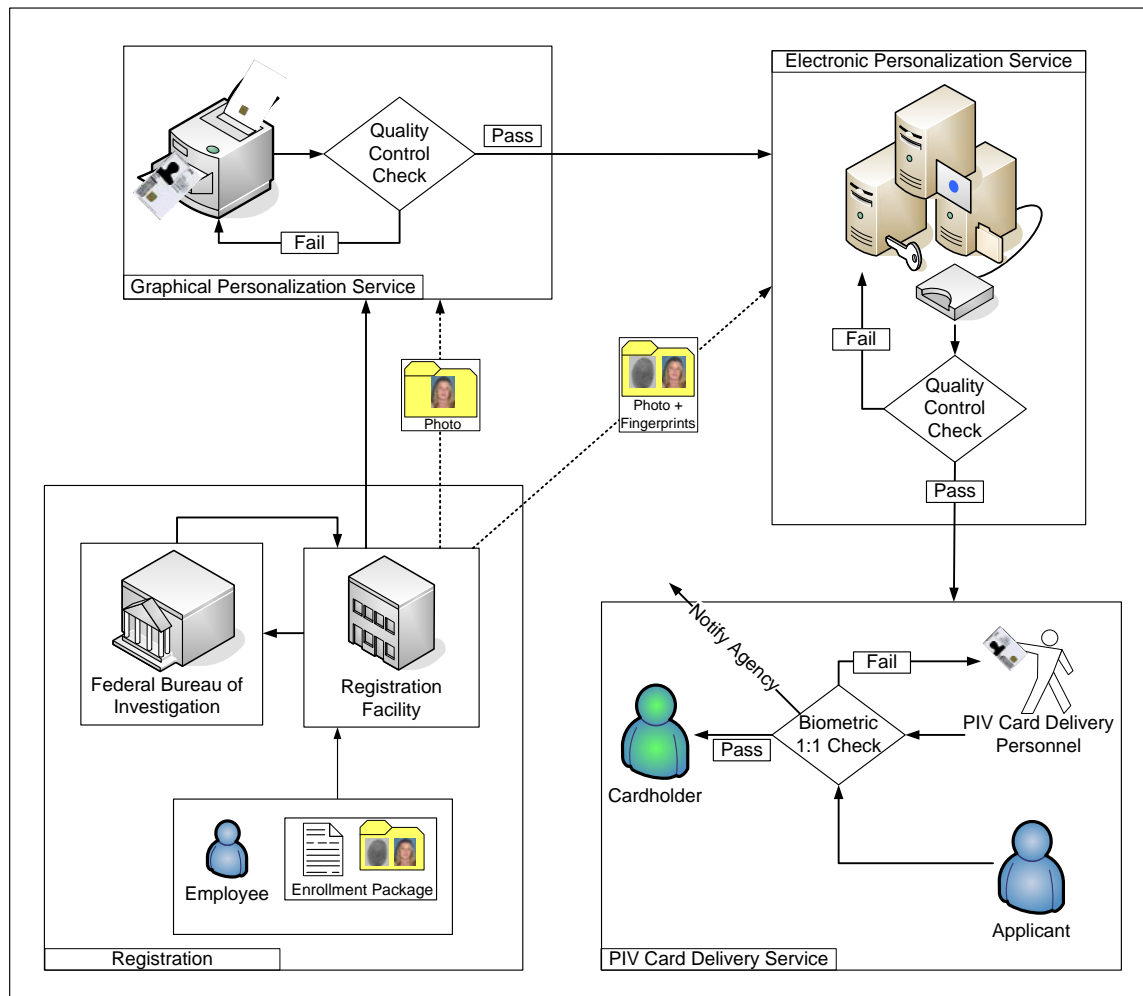
Figure 1 - PIV Card Delivery Service

1.3 Purpose

The purpose of this document is to provide the following information:

(i) Provide a list of the artifacts and/or documentation that needs to be submitted to the Evaluation Lab as part of the application package submission.

(ii) Document the list of the requirements that apply to this category

(iii) Specify the evaluation criteria along with their approval mechanisms that will be used by Evaluation Labs to verify compliance of the Product against the requirements that apply to this category.

2   Application Package Contents

The Application Package Contents include the artifacts, documentation and in some cases the product itself that needs to be submitted to the Evaluation Lab so that evaluation can be performed. The Application Package Contents for this category include the following:

- Completed Application Form, provided on the Evaluation Program website. (This form will be available through the web interface once users have been assigned a login credential.);

- Completed and signed Attestation Form (found in the application submission package ZIP file). The Attestation Form should be completed and scanned into a document to be uploaded to Evaluation Program website;

- Supplier VDR-VTDR justification worksheet (found in); Completed Credit Card Authorization Form;

- Completed and signed Non-Disclosure Agreement (found in the application submission package ZIP file) The Non-Disclosure Agreement should be completed and scanned into a document to be uploaded to Evaluation Program website; and

  Note: This NDA can be substituted with a Supplier-provided document, however, for this will slow the evaluation process as the NDA submitted will need to be reviewed by the Lab.

- Completed Supplier VDR-VTDR justification worksheet provided as part of the application submission package ZIP file; and

- All necessary Supplier documentation providing proof that the Product complies with the subset of requirements (as outlined in Section 4.1) for this category which has Supplier documentation review as its approval mechanism. Examples of specific documentation would include: user guides, technical specifications, white papers, line cards, etc.

  As part of the submitted documentation, please provide details (product name and version) of FIPS 201 Approved products that have been used by the Service (e.g. for 1:1 biometric match prior to release of the PIV Card to the card holder).

  Additional documentation that must be submitted to the lab includes:

  - A list of the Supplier site(s) that will be delivering PIV Cards
  - PIV Card Delivery Facility Standard Operating Procedures
  - Human Resources Standard Operating Procedures
  - The background investigations service contract
  - The Security Plan for the facility
  - The Security Equipment Inventory List
  - The PIV Cardholder Acceptance Form (sample provided in Appendix A)
  - Server penetration reports for all servers which are publicly available on the Facility's network
  - A screenshot of the PIV Card Automated Inventory Control System
  - Server security vulnerability report
  - Privacy Impact Assessment

3 Evaluation Procedure for PIV Card Delivery Approval

3.1 Requirements

In order to approve the Service as conformant to the requirements of PIV, it at a minimum, must comply with all the requirements listed below. The approval mechanism column describes the technique utilized by the Lab to evaluate compliance to that particular requirement.

Identifier #	Requirement Description	Source	Reqt. #	Approval mechanism
ISS.1	Delivery facilities shall use a common set of standard operating procedures for delivery of PIV Cards.	Derived Test Requirement	N/A	Vendor Documentation Review
ISS.2	The [service] shall, at the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.	FIPS 201, Section 2.3	1.1-22	Vendor Documentation Review Site Visit
ISS.3	The issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record.	FIPS 201, Section 5.3.1	1.1-161	Vendor Documentation Review Site Visit
ISS.4	The PIV Card shall be released to the applicant only upon a successful biometric match.	FIPS 201, Section 5.3.1	1.1-161	Vendor Documentation Review Site Visit
ISS.5	The card issuer shall verify the cardholder's identity against the biometric information stored on the expiring card.	FIPS 201, Section 5.3.2.1	1.1-170	Vendor Documentation Review Site Visit
ISS.6	Expired PIV Cards must be collected and destroyed.	FIPS 201, Section 5.3.2.1	1.1-171	Vendor Documentation Review Site Visit

Identifier #	Requirement Description	Source	Reqt. #	Approval mechanism
ISS.7	Delivery facilities shall maintain records as to which process, issuance or renewal, should be used for each PIV Card issued.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.8	Delivery facilities shall employ personnel who are knowledgeable of the organization's operating procedures.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.9	Delivery facilities shall employ personnel who are not on the list of known terrorists.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.10	Delivery facilities shall perform background checks on personnel handling PIV Cards. Background checks must reflect Federal, State and Local databases to ensure felonies have not been committed by PIV Card handlers.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.11	Delivery facilities shall maintain adequate security on the premise of the building.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.12	Delivery facilities shall utilize a PIV Card storage container which contains a multi-factor form of authentication to access the contents of the container.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.13	Delivery facilities shall maintain a log of visitors who enter the area which has been designated to deliver PIV Cards to cardholders.	Derived Test Requirement	N/A	Site Visit
ISS.14	Delivery facilities shall require cardholders to sign an acknowledgement form prior to the release of the PIV Card.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit

Identifier #	Requirement Description	Source	Reqt. #	Approval mechanism
ISS.15	Delivery facilities shall utilize automated card inventory control, which utilizes the CHUID to track and manage the following transactions: • Inventory to be delivered from the personalization facility • Inventory on hand • Inventory which has been delivered to cardholders.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.16	Facility personnel shall demonstrate issuance of a card in accordance with the Facility Standard Operating Procedure	Derived Test Requirement	N/A	Site Visit
ISS.17	Delivery facilities shall utilize a mechanism to notify Agencies, on a regular basis, which PIV Cards have been received and delivered to cardholders.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.18	Delivery facilities shall have a procedure in which to notify applicants, at a minimum using written communication, that their PIV Card is ready to be picked up.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.19	Delivery facilities shall deliver renewed and reissued cards in accordance with Section 5.3 of FIPS 201.	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.20	Delivery facilities shall utilize only FIPS 201 approved equipment according to the GSA FIPS 201 Approved Product List (e.g. biometric readers or single fingerprint capture devices for 1:1 match of the biometric record to the Applicant prior to release of the PIV Card).	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit
ISS.21	Any server which is publicly	Derived Test	N/A	Vendor

Identifier #	Requirement Description	Source	Reqt. #	Approval mechanism
	available on the Facility's network (e.g. web or email server), which holds information pertaining to applicants shall be tested using penetration tests to prove that the server is not vulnerable to common attacks through public networks.	Requirement		Documentation Review
ISS.22	All servers, which serve a purpose for the PIV Card Delivery Service, residing on the facility's network, shall be scanned for security vulnerabilities, and the appropriate security patches applied to the affected software.	Derived Test Requirement	N/A	Vendor Documentation Review
ISS.23	IT Information Systems containing information in identifiable form (IIF), used to deliver a PIV Card to an applicant, shall have a Privacy Impact Assessment (PIA), as directed by OMB Memorandum M-03-22[1], performed on that system.	Derived Test Requirement	N/A	Vendor Documentation Review
ISS.24	PIV Card Delivery Facilities shall be reviewed every two (2) years, from the date of GSA approval, to ensure Standard Operating Procedures are followed by PIV Card Delivery Personnel	Derived Test Requirement	N/A	Vendor Documentation Review Site Visit

Table 1 - Applicable Requirements

---

[1] Memorandum can be found at http://www.whitehouse.gov/omb/memoranda/m03-22.html

3.2 Approval Mechanism Matrix

The table below provides an indication of the total number of requirements applicable for the Service and provides a breakup of how the evaluation will be conducted based on the different approval mechanisms available to the Lab.

Total Requirements	Approval Mechanisms					
	SV	**VTDR**	**LTDR**	**VDR**	**C**	**A**
22	19	N/A	N/A	14	N/A	1
Legend: SV – Site Visit; VTDR – Vendor Test Data Report; LTDR – Lab Test Data Report; VDR – Vendor Doc. Review; C – Certification; A - Attestation						

<p align="center">Table 2 - Approval Mechanism Matrix</p>

3.3 Evaluation Criteria

This section provides details on the process employed by the Lab for evaluating the Product against the requirements enumerated above

3.3.1 Vendor Documentation Review

Reference(s):	ISS.1 to ISS.6, ISS.8, ISS.9, ISS.13, ISS.15 to ISS.22

Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to "VDR Begun" as instructed in the Web-enabled Tool Laboratory User Guide.
	2. The Lab will review the Issuer's documentation (Standard Operating Procedures and supporting documents) to determine the following:
	
	▪ *Standard Operating Procedures (ISS.1)*
	
	    • The Supplier has submitted detailed documentation for the complete process of delivering PIV Cards at the Facility. The SOP should include, at a minimum, roles defined for the Facility, the hours of operation for the Facility as well as the PIV Card delivery area, procedures for handling personalized cards, handling procedures, a list of authorized PIV Card handlers and their supervisors, contact information for local law enforcement, storage procedures for personalized PIV Cards.
	
	▪ *Identity Verification (ISS.2 to ISS.4)*
	
	    • A process is documented in the Standard Operating Procedures which describes the steps to verify that the individual whom the background investigation was completed is the same as the credential who is being given.
	    • A process is documented in the Standard Operating Procedures which describes the steps to verify that the individual who is receiving the card visually appears to be the same person as printed on the card prior to handing over the card.
	    • A process is documented in the Standard Operating Procedures which

describes the steps to verify that the biometrics stored on the card match against the live authentication scan taken at the time of issuance.

- *Card Renewal (ISS.5, ISS.6)*
    - A process is documented in the Standard Operating Procedures which describes the steps of biometric verification of the cardholder to the expiring PIV Card.
    - A process is documented that describes the process used to destroy expired PIV Cards in the Standard Operating Procedures. Destroyed PIV Cards are physically altered such that the printed information is no longer able to be read and the smart chip processor and memory ruined. Acceptable methods of card destruction include melting and shredding.
    - A process is documented in the PIV Card Delivery Facility Standard Operating Procedures which describes a process whereby the Facility notifies the sponsoring Agency that a renewed card was picked up.
- *Delivery Type (ISS.7)*
    - Processes are documented for issuing and renewing PIV Cards in the Standard Operating Procedures. The documented procedures must be clearly separated and identifiable in case of variations between different issuing procedures for different Agencies.
- *Personnel Training & Knowledge (ISS.8)*
    - Training materials of the Facility's Operating Procedures have been developed for each role in the printing facility.
    - A list of trusted roles in the Facility system has been defined as part of the Standard Operating Procedures.
    - A list of authorized personnel is maintained by the Facility and is referenced by the Standard Operating Procedures. The list of authorized has been furnished to the Lab for review.
    - A statement by the Service Provider that when the list of authorized personnel changes for any reason, the Lab who has performed the original evaluation will be provided with an updated list.
    - The Standard Operating Procedures states that training occurs on at least an annual basis for all personnel serving a role within the Facility.
    - The Facility Standard Operating Procedures state that employees are retrained within one week of a procedure-based changed to the SOP.
- *Personnel History Checks (ISS.9, ISS.10)*
    - A statement from the background investigation service provider has been submitted which states the source of the Federal agency responsible for maintaining the list(s) of known terrorists for which Facility personnel are checked against. Examples of Agencies maintaining lists of known terrorists include the Department of Homeland Security, the Federal Bureau of Investigations, and

INTERPOL. Human Resources personnel records should indicate that this check has been performed on all personnel of the PIV Card Facility.

- The contract with the service provider for Federal, State, and Local criminal history has been provided and personnel records indicate that this check has been performed on all PIV Card handlers.
- Human Resources Standard Operating Procedures indicate that employees whose job function is to handle PIV Cards (trusted roles), are to undergo a background check before performing functions a particular role in the Electronic Personalization Facility.

- *Premise Security (ISS.11)*

  - The security plan for the premise has been provided and all security protections on the building are documented, and listed within the security inventory list.

- *PIV Card Storage Container (ISS.12)*

  - The security equipment inventory list includes the make and model of the container used to store PIV Cards.
  - The Standard Operating Procedures describes the type of factors for authentication to the container.

- *Cardholder Acknowledgement Form (ISS.14)*

  - The Standard Operating Procedures state that the form is used when a card is issued, renewed, or reissued to an Applicant.
  - A blank form has been provided and is made available to Applicants which formally confirms that an Applicant has received their personalized PIV Card and the results of the 1:1 biometric match has been successfully completed. A sample of the minimum requirements for the form has been provided in Appendix A.

- *Card Inventory Control (ISS.15)*

  - An automated inventory control system has been developed to track incoming, outgoing, and the number of on-hand PIV Cards which utilizes, at a minimum, the FASC-N value in the CHUID. The following values will be extracted from the FASC-N to identify cards:
    a. Person Identifier – The PI shall be used as the primary key to identify a cardholder
    b. Credential Number – The CN shall be used as the secondary key, in the event that multiple PIs exist in the inventory control system.
    c. The facility may optionally choose to populate records with the card holder name which is printed on the card; however, the PIN value of the card is never to be used to access privileged data objects on the card for the purposes of card inventory.
  - A screenshot of the automated inventory control system has been

furnished for review by the Lab. The data found in the system may be mocked up for the purposes of demonstration of the functional system.

- *Agency Notification (ISS.16)*

  - The Standard Operating Procedures describe the processes in place to notify an Agency that an attempt was made to pick up a PIV Card by a person other than the applicant of the said PIV Card.

- *Applicant Notification (ISS.18)*

  - The Standard Operating Procedures describe the process in place to send notification to an Applicant that his or her card is ready to be delivered within 24 hours of the Facility receiving the PIV Card.
  - A sample (i.e. a template) of the written communications (e.g. email or letter) has been provided for the Lab to review.

- *Reissuance and Renewal Procedures (ISS.19)*

  - The Standard Operating Procedures describes a process, which is consistent with Section 5.3 of FIPS 201, to authenticate the cardholder to the expiring card using a biometric match.
  - The Standard Operating Procedures describes a process which states that that the expiring PIV Card is collected from the cardholder, if applicable.
  - The Standard Operating Procedures contains a process which describes the steps to destroy the PIV Card once it has been collected from the cardholder, if applicable. Destroyed PIV Cards are physically altered such that the printed information is no longer able to be read and the smart chip processor and memory ruined. Acceptable methods of card destruction include melting and shredding.
  - The Standard Operating Procedures describes a process whereby the sponsoring Agency is notified upon receipt of PIV Card reissuance or renewal.

- *Biometric Matching Equipment (ISS.20)*

  - The security equipment inventory list states the equipment make and model number to ensure use of FIPS 201 approved products by GSA. The Approved Products List reference number must be provided to the Lab as well.

- *Server Penetration Testing (ISS.21)*

  - A formal penetration test has been performed on any server which is publicly available on the Facility's network.
  - The report which has been generated as a result of this test shall be provided.
  - The security equipment inventory list contains a description of each server and its function in the PIV Card Delivery Facility.
  - The Standard Operating Procedures states that publicly available are

	monitored on a continuous basis for intrusion detection and the associated logs are reviewed, at a minimum, on a monthly basis.
	▪ *Server Security Vulnerability Updates (ISS.22)*
	• A formal security vulnerability test has been performed on all servers that provide functionality to the Facility's ability to deliver PIV Cards to applicants.
	• The report, which has been generated as a result of this test, shall be provided.
	• The security equipment inventory list contains a description of each server and its function in the PIV Card Delivery Facility.
	• The Standard Operating Procedures states the electronic source for obtaining security fixes such as patches and updates and states the frequency of such updates. The minimum acceptable frequency for updates is bi-weekly.
	▪ *Privacy Impact Assessment (ISS.23)*
	• An assessment has been developed by the Facility which identifies what information in identifiable form (IIF) will be stored by the facility and how IIF will be protected by the system for all machines participating in the PIV Card Delivery Service function.
	▪ *Facility Review (ISS.24)*
	• The Facility maintains a written record of the 2 year reevaluation of the Facility.
	• The Standard Operating Procedures state that the Facility is prepared for the Lab to visit every 2 years to ensure that the Facility is operating as per the Standard Operating Procedures.
	3. The Lab will update the status to "VDR Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	All necessary procedures and other documentation are formally documented within the Facility.

3.3.2   Site Visit

A Lab Technician will perform a site visit[2] at a Card Delivery Facility to determine whether the documented procedures and other necessary requirements are adhered to and followed by the Service Provider.

Reference(s):	ISS.1 to ISS.18
Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to "SV Begun" as instructed in the Web-enabled Tool Laboratory User Guide.
	2. The Lab will conduct an on site review of the Facility to determine the following. In this respect the Lab Technician shall review processes

---

[2] Site visits not only include documentation review but may also include observing the actual process being carried out. Service Providers need to have equipment and processes in place for identity authentication and verification to demonstrate execution of the PIV Card Delivery Service.

employed at the facility for:

- *Identity Verification (ISS.1, ISS.2, ISS.3)*

  - Performing 1:1 match of the biometrics of the Applicant with that on the PIV Card (i.e. verification of the biometrics stored on the card match against the live authentication scan taken at the time of issuance).
  - Verifying the ability of the biometric reader(s) used at the Facility to perform a 1:1 biometric match of a valid and invalid cardholder using the Lab's designated "golden" cards.
  - Verifying that the individual whom the background investigation was completed is the same as the credential who is being given.
  - Verifying that the individual who is receiving the card visually appears to be the same person as printed on the card prior to handing over the card.

- *Delivery Type (ISS.6)*

  - Verifying that the facility is following the documented process(es) for issuing and renewing PIV Cards. In the event that the Service is used for issuing PIV Cards to multiple Agencies having different requirements, there is a clear distinction on which procedure to use.

- *Knowledge of Personnel (ISS.7)*

  - Interviewing a sample of the key personnel serving various roles within the PIV Card Delivery Facility to determine whether they are knowledgeable of the standard operating procedures

- *Personnel Background Checks (ISS.8, ISS.9)*

  - Reviewing HR records at the Facility to determine whether the current employees at the facility have been checked against the list of known terrorists specified in the vendor documentation.
  - Reviewing HR records at the Facility to determine whether trusted roles within the PIV Card Delivery Facility have had a background check completed.

- *Security Provisions (ISS.10, ISS.11, ISS.12)*

  - Reviewing security mechanisms that are in place on the premise of the facility to be consistent with vendor documentation.
  - Reviewing logging procedures of visitors who enter the designated PIV Card delivery area to be consistent with vendor documentation.
  - Ensuring security mechanisms are in place on the storage container of PIV Cards waiting to be delivered. Mechanisms must employ a multi-factor form of authentication to gain access to the container and must be enforced at all times.

- *Acknowledgement Forms (ISS.13)*

  - Verifying that the sample form used to acknowledge that an Applicant has received his or her PIV Card from the card delivery facility.

	• *Inventory Control (ISS.14, ISS.15, 1SS.16)*
	• Verifying that the procedures are in place for the facility to determine which PIV Cards are expected to arrive in each batch of cards received from the personalization facility.
	• Verifying that the procedures are in place to log incoming and outgoing (delivered) PIV Cards and to communicate the same with the Agency.
	• Verifying that the procedures are in place to notify Applicants that their PIV Cards are ready for pickup.
	• Verifying that the procedures are in place to notify the Agency when PIV Cards are issued.
	• *Reissuance and Renewal Procedures (ISS.4, ISS.5, ISS.17)*
	• The vendor demonstrating the reissuance process to be performed by the role responsible for reissuing a card to an applicant. The demonstration is consistent with the procedure stated in the Standard Operating Procedures.
	• The vendor demonstrating the renewal process to be performed by the role responsible for renewing a card to an applicant. The demonstration is consistent with the procedure stated in the Standard Operating Procedures.
	• *APL Approved Equipment (ISS.18)*
	• Verifying that the equipment used at the facility corresponds to the list of equipment that is from the GSA FIPS 201 Approved Products List.
	• *Facility Review (ISS.22)*
	• The Facility maintains a written record of the 2 year reevaluation of the Facility.
	• The Facility is prepared for the Lab to visit every 2 years to ensure that the Facility is operating as per the Standard Operating Procedures.
	3. The Lab will update the status to "SV Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	All necessary controls and procedures are implemented and being followed as documented.

3.3.3 Attestation

Reference(s):	N/A
Evaluation Procedure:	1. The Lab will update the status in the Web-Enabled Tool to "A Begun" as instructed in the Web-enabled Tool Laboratory User Guide.
	2. Review the Attestation Form provided by the Supplier, confirming that the Product to the best of their knowledge, conforms to all the necessary requirements of the category under which the Product applies. Verify that person signing this Attestation Form has the authority to do so (a

	minimum "C" level [e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner]). 3. The Lab will update the status in the Web-Enabled Tool to "A Complete" as instructed in the Web-enabled Tool Laboratory User Guide.
Expected Results:	1. The Attestation Form has been signed by an authorized individual (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner).

Appenix A—Sample Acknowledgement of Receipt

FIPS 201 Evaluation Program
Sample Acknowledgement Receipt for PIV Card Delivery

This receipt of acknowledgement is a sample that provides guidance Card Delivery Facilities as to what type of information will be collected at a minimum when issuing PIV Cards to Applicants. Note that contracting Agencies can provide additional requirements beyond the scope of this example or may incorporate these fields into their forms.

Date:	Date
Employee Name:	Employee who is releasing the PIV Card
Employee ID:	ID number used to uniquely identify an employee

PIV Card Information

Card ID:	Unique number assigned to PIV Card during transit.
Applicant Name:	

Card Renewal

Biometrics Matched:	☐ Yes ☐ No
Card Collected:	☐ Yes ☐ No (Reason:_____)
Card Destroyed:	☐ Yes ☐ No (Reason:_____)

Statement of Receipt

By signing below, I hereby confirm that the information contained on this page is complete and accurate. I understand that by signing this form I am claiming that the Personal Identity Verification Card I am about to receive is my own and am not claiming to impersonate the identity of the true owner of this card. I also understand that crimes related to identity impersonation will be pursued to the fullest extent of the Law.

Signature: _____   Date: _____

Printed Full Name: _____

PIV Card Delivery -
Employee Signature: _____   Date: _____

Appenix B— Document Release Summary of Changes

Identifier #	Reference	Description of Change
N/A	N/A	Removed Evaluation Program approval processes from document. Approval process can be found in Supplier Handbook.
ISS.1	Section 3.1 p.9	Derived test requirement added calling for common set of standard operating procedures for delivery of PIV Cards.
ISS.16	Section 3.1 p.11	Derived test requirement added calling for demonstrate issuance of a card in accordance with the Facility Standard Operating Procedure. Requirement compliance will be verified during vendor site visit.
VDR (ISS.1)	Section 3.3.1 p.13	ISS.1 evaluation procedures documented for verification of vendor PIV Card delivery standard operating procedures.
VDR (ISS.8)	Section 3.3.1 p.14	Evaluation procedure updated to specify vendors will need to demonstrate that FOP training material has been developed for each role in the printing facility. Previously, requirement specified personnel issuing PIV Cards only.