FIPS 201 Evaluation Program -
Suppliers Policies and Procedures Handbook

Version 3.0.0
August 11, 2008

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	10/17/07	Document creation	Public
Approved	2.0.0	05/06/08	Updates based on formalized policy: • Transfer of Product Evaluation to a different Lab • Addition of request for extension to Product Update timeframes Updated policy for products that contain functionality relating to multiple categories	Public
Approved	3.0.0	08/11/08	Following updates were made: • Update to the policy regarding timeframes for extensions • Rules for updating the APL • Addition of the RPL • Clarification of types of part number changes allowed during product upgrades	Public

Table of Contents

1. Introduction

1.1 Background

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors. The goal of HSPD-12 is to increase security and Government efficiency, reduce identity fraud and terrorist exploitations and protect the privacy of the individual.

The Office of Management and Budget (OMB) has designated the General Services Administration (GSA) as the Executive Agent for government-wide acquisitions for the implementation of HSPD-12. Additionally, OMB has directed Federal agencies to purchase only products and services that are compliant with the Federal policy, standards and supporting technical specifications.

The FIPS 201 Evaluation Program is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within GSA. The goal of the FIPS 201 Evaluation Program is to evaluate products and services against the requirements outlined in FIPS 201-1 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.

Once evaluated and approved by the FIPS 201 Evaluation Program, products and services are placed on the FIPS 201 Approved Products List (APL). Agencies can then procure these products and services from Suppliers for their HSPD-12 implementations having full assurance that they meet all the requirements of FIPS 201-1 as well as the GSA interoperability and performance criteria.

1.2 Purpose

This document provides the policies and procedures that need to be followed by Suppliers as they submit their products and services for evaluation to the Evaluation Program (EP) Laboratories. Suppliers must use this document in conjunction with the applicable approval procedures in order to successfully complete an evaluation of their product or service.

The specific policies and procedures that apply to all evaluations are described and referenced in the sections that follow.

1.3 Effective Date

The policies and procedures prescribed in this handbook may be refined or modified based on Industry feedback, to align with current best practices in the Industry, or to achieve maximum Lab efficiency.

Labs operating within the purview of the FIPS 201 Evaluation Program are instructed to follow the latest version (effective immediately once posted on the EP Website) of this handbook as they perform evaluations of Suppliers products and services.

1.4 Evaluation Categories

Based on the requirements extracted from FIPS 201-1 and its supporting special publications, the GSA FIPS 201 Evaluation Program performs evaluations currently in twenty-four (24) different product and service categories. Below is a list of these categories. Definitions and evaluation criteria for these products and services can be obtained from the corresponding approval procedures.

1. Authentication Key Reader
2. Biometric Reader
3. Biometric Authentication Reader
4. Card Printer Station
5. CHUID Authentication Reader (contact)
6. CHUID Authentication Reader (contactless)
7. CHUID Reader (contact)
8. CHUID Reader (contactless)
9. Cryptographic Module
10. Electromagnetically Opaque Sleeve
11. Electronic Personalization
12. Electronic Personalization (Service)
13. Facial Image Capturing Camera
14. Facial Image Capturing (Middleware)
15. Fingerprint Capture Station
16. Graphical Personalization
17. OCSP Responder
18. Single Fingerprint Capture Device
19. PIV Card
20. PIV Card Delivery
21. PIV Middleware
22. Template Generator
23. Template Matcher
24. Transparent Reader

Please note that as FIPS 201-1 and its supporting documents are updated, the GSA FIPS 201 Evaluation Program may change/update these product categories (and/or associated requirements) as needed.

Suppliers whose products and services do not fall under any one of these categories are eligible to sell these to Agencies without going through the Evaluation Program and being placed on the APL. Since no requirements are identified by FIPS 201-1 and its supporting documents for such products and services, the Evaluation Program is not responsible for determining conformance at this time. On the other hand, if Suppliers feel that their product falls under two or more categories, they need to submit separate applications under each of these categories. If found to be compliant, the product will be listed separately under each category on the APL.

Suppliers must only submit products and services that meet the definition of the category as described on the EP Website. If a product being submitted under one category has the capability to meet the requirements of another category, the submitted product will be required to be evaluated against the other category as well. For example, if a transparent reader also has the

ability to capture a fingerprint, then it will have to be evaluated against the single fingerprint capture device or one or both of the biometric reader categories prior to being listed on the APL. Similarly, a card printer station that includes a reader will need to be evaluated against the transparent reader category. Permitting Suppliers to submit such products under only one (1) category may result in the product being used by an Agency for a function that it hasn't been approved for by the Evaluation Program leading to a false sense of security and compliance. That being said, each product being submitted will be reviewed on a case-by-case basis to make this determination. If a Lab determines that a submitted product needs to be evaluated under another category as well and the Supplier disagrees with the Lab's decision, the Supplier may complete and submit the Appeals Form to the Lab. GSA, in consultation with the Lab and the Supplier will provide a ruling within five (5) business days after all information has been made available by the respective parties.

If Suppliers are reselling products of other original equipment manufacturers under part numbers of their own, they must submit the product for evaluation to the Evaluation Program. Additionally, they will have to follow the requirements specified in Section 2.5.1. On the other hand, if Suppliers are reselling already approved products using the same part number and versions as the original manufacturer, then the product does not need to go through evaluation again.

Considering that the Evaluation Program's primary objective is that of "evaluation" i.e. to check compliance of a product or service with the applicable FIPS 201-1 requirements, the Lab will not entertain submission of identical components whose method of sale is different (e.g. out-right purchase vs. lease) or the same product with a different part number based on the quantity for sale. This is considered to be an acquisition method and is independent of the technical functionality of the product and service, the only concern of the Evaluation Program.

2. Approval Process

2.1 Overview

The evaluation of a Supplier's products and services are executed primarily through the FIPS 201 EP Website.

Suppliers who believe that their product or service falls into one of the categories listed in Section 1.4 need to submit the same for evaluation prior to being made available for procurement to Agencies. This is a pre-condition for offering products and services as part of a PIV system to the Federal Government.

Suppliers can gather relevant information regarding the Evaluation Program, its goal and what is expected from them when they submit their product or service for evaluation against the requirements of FIPS 201 and its related publications from this Website. Some examples of such information include, but are not limited to, application forms, product/service categories, approval and test procedures, and the evaluation status.

2.2 Login Request

The first step toward completing the evaluation process is for the Supplier to request a Userid and Password. Under most circumstances, an organization can only receive one login credential, for use by one official contact person. Directions for completing a login request can be obtained from the Obtain Login link on the EP Website.

2.3 Application Creation

Once the Supplier has been provided with their Userid and Password, they can log in to the EP Web Tool and create an application for evaluation of their product or service. Besides completing all the details in the application sheet, the Supplier needs to select a Lab that they would prefer to perform the evaluation of their product or service.

Once an application is created, the selected Lab needs to set the evaluation status to "*Package Submitted*" within ten (10) business days, after which the application will be automatically deleted. Setting the evaluation status to "*Package Submitted*" implies that the Lab has acknowledged the application submitted by the Supplier and has negotiated the fees that will be charged for that product or service. This mechanism prohibits Suppliers from creating applications and assigning their evaluations to a Lab without negotiating the fee upfront which results in applications remaining stationary in the evaluation queue.

2.4 Evaluation Fees

In order for the Lab to evaluate the Supplier's product or service, the Supplier is expected to pay the necessary evaluation fees to the Lab. The Evaluation Program doesn't dictate the fees that are to be charged per category by the Labs. The Labs determine fees independently and these fees can be based on a number of variables. Please contact an Approved EP Lab to learn about the fees that the Lab would charge to perform the evaluation.

2.5 Application Package Submission

Once the application is acknowledged by the Lab (i.e. the Lab sets the status to "*Package Submitted*"), the Supplier can upload all the documentation and artifacts necessary to perform the evaluation. The details of the necessary items that need to be submitted are based on each

category and can be found in Section 2 of the relevant Approval Procedure. A supplier has five (5) days within which they must complete all uploads.

Once the evaluation fees are negotiated and the application package is found to be complete, it will be placed in queue by the Lab where it waits its turn for evaluation. At this stage, the evaluation status will be set to "*Evaluation in Progress*".

Please note that as part of the evaluation, any products and/or artifacts submitted by the Supplier will not be returned as these have to be retained for Lab records.

2.5.1 Reseller Repackaging

For cases in which a Supplier desires to resell a product from an original manufacturer under the reseller's brand as a whole or as part of the Supplier's integrated product suite, the Supplier must complete the Reseller Acknowledgment Form.

This form is used to inform the Evaluation Program that the Supplier is using products (from the EP category list) that are from another manufacturer. It must be signed by the original manufacturer only when the intellectual property belonging to that manufacturer is submitted by the reselling manufacturer for the purposes of the evaluation.

2.6 Execution of Evaluation Procedures

Once the application package exits the evaluation queue, the Lab schedules the evaluation and assigns the necessary resources. The Lab performs an evaluation of the product or service in accordance with the evaluation criteria for that category as described in Section 4.3 of each Approval Procedure. Coupled with the evaluation criteria, the approval mechanisms (discussed in Appendix A) are used as a means to determine compliance against the requirements.

The Lab documents the results as they execute the evaluation procedures.

2.7 Evaluation Report Preparation

An evaluation report is prepared for the product or service, irrespective of whether it passes or fails to comply with the applicable requirements of FIPS 201-1.

If the product or service is found to comply with all application requirements, the evaluation report is submitted to GSA along with the Lab's recommendation for the product or service to be placed on the APL. In the event of non-compliance, the evaluation report and a non-conformance letter is sent to the Supplier by the Lab.

2.8 Government Approval

After the Lab submits the evaluation report to GSA, the Approval Authority provides the final decision. The Approval Authority will contact the Lab if there are questions or concerns regarding an item in the evaluation report.

Once placed on the APL, Agencies can procure the Supplier's product or service for their HSPD-12 implementations.

2.9 Non-Conformance Review

If a Supplier disagrees with a Lab decision, they can submit a request for a non-conformance review meeting to the Lab within thirty (30) calendar days after receiving the non-conformance letter. The non-conformance review is initiated upon the Lab's receipt of the Appeals Form.

The Lab along with the Approval Authority reviews the submission and researches the facts of the non-conformance result. This review includes thoroughly examining all documentation in the case file and interviewing the appropriate personnel assigned to evaluate the Supplier's product or service.

The Lab then discusses the submission and findings with the Supplier. If the disagreement is resolved during this discussion, the results are documented. The Lab then issues a formal letter of resolution to the Supplier and makes any needed changes to the approval status of the Supplier's product or service. If approved, the product or service is now placed on the APL.

3. Approval Procedure Updates

As the PIV Program evolves i.e. FIPS 201-1 and its supporting technical publications get updated, changes will need to be made to the procedures that the Lab uses to evaluate Supplier products and services. It is expected, although not guaranteed, that updates made to these procedures will be minimal. Technical specifications (e.g. NIST Special Publications) are continually updated as technology advances and products get obsolete. This coupled with the fact that the primary goals of PIV are security, reliability and interoperability, Suppliers that currently have products and/or services already on the APL will be required to update the same, as necessary, and attest that the product and/or service submitted meets all the necessary requirements at all times if they want to continue to remain on the APL. ***In this respect, the Evaluation Program, at any point in time, shall only list products and services on the APL that are in conformance with the current version of the Standard and its specifications.***

3.1 Applications being Submitted

Suppliers submitting a product or service for evaluation must ensure that the latest version of Approval Procedure has been downloaded and followed during application submission. It is recommended that before uploading any documents to the EP Web Tool, that the latest Application Submission Package be downloaded and reviewed. Suppliers should compile the list of documents and/or artifacts that need to be submitted prior to upload.

3.2 Applications in Evaluation

If an Approval Procedure is updated while a Supplier's application is in the queue, the Lab will inform the Supplier as soon as possible. Suppliers may be required to sign a new version of the attestation form which may contain a list of updated requirements as reflected in the Approval Procedure.

The notification to the Supplier will outline the changes made from the previous version as well as the timeframe in which Supplier have to update any documentation. This timeframe will be determined by the Lab based on discussions with GSA and is typically based on the type and number of requirements/test scenarios that are being changed/added to the Approval Procedure. In the event that the Supplier desires to recall their product or service until all new requirements have been adequately addressed, the Supplier may do so.

3.3 Listings on the APL

If the Lab determines that a previously approved product or service needs to be either partially or fully re-evaluated and/or re-tested based on the updates to the Approval Procedure, the Lab will inform the Supplier.

The notification sent to the Supplier by the Lab will outline the changes made from the previous version as well as the time frame by which the Supplier needs to comply. This timeframe is determined by the Lab based on discussions with GSA and is typically based on the type and number of requirements/test scenarios that are being changed/added to the Approval Procedure. Therefore for each update, the Lab in collaboration with GSA will identity a suitable timeframe for submission of new artifacts.

In the event that the Supplier cannot comply within the established timeframe, the Supplier may request an extension through the Lab. Supplier's requests for extensions must be made in writing

and cannot exceed more than ten (10) business days beyond the established deadline.. Requests made for extension beyond this timeframe will not be accepted. Please note that the Labs are not authorized to accept any requests for extension on behalf of the FIPS 201 Evaluation Program. Final authorization for all extension requests will be granted by GSA only.

Products and services that are in the midst of a re-evaluation will be identified as such on the APL until the re-evaluation has been completed. Depending on whether the product or service is found to be conformant or not, its listing on the APL will either continue to exist or will be moved to the Removed Products List (RPL).

In the event that a product that is cross-referenced as part of another APL line item is removed from the APL, the Supplier for the latter product will be notified by the Lab. The Lab will inform the Supplier of the steps that are necessary to be taken to remain on the APL.

Suppliers who do not comply will have their product or service removed from the APL (and placed on the RPL) until compliance has been established (met through the current or updated Product or Service).

4. Supplier Upgrades

Over the course of a product lifecycle, Suppliers may need to update their product based on advances in technology and/or changes to NIST specifications. This section discusses the details that Suppliers must follow in order to have an upgraded product listed on the Approved Products List.

4.1 Process Determination

If the Supplier makes an update to their product that necessitates a change to the version, and the Supplier desires to have the new version of their product listed on the APL, the Supplier needs to have the Lab re-evaluate the product.

Similarly for services, if the Supplier changes any products (including their versions) approved to execute the Service or makes changes to the service itself (e.g. change of location), the Supplier needs to have the Lab re-evaluate the service for continued compliance.

In both cases mentioned above, the type of changes made determines what course of action needs to be taken. Currently, two options exist within the GSA FIPS 201 Evaluation Program. The scenarios are as discussed below:

Scenario #1: Update to Part Number

If the Supplier makes an update to their product that necessitates a change to the Part Number[1], and the Supplier desires to have the new Part Number listed on the APL, the Supplier will have to process the product/service as a new evaluation.

Please note that in the context of the Evaluation Program, an upgrade implies that the updated product will be sold using the same, original part number. In the event that a Supplier changes the part number, the upgrade process shall not be followed. Additionally, in the case that the Supplier desires to have both the original and the updated product listed on the APL, the updated product needs to have a new part number.

Scenario #2: No change to Part Number

If the Supplier makes an update to their product that does not necessitate a change to the Part Number, the upgrade process will be followed. The versions (h/w, s/w or f/w) of the product may be updated; however the part number needs to remain the same as the original product that was evaluated. In this scenario, the Supplier needs to complete the Upgrade Form and follow the process as defined in Section 4.2.

4.2 Using the Upgrade Form

The Upgrade Form is used to describe to the Lab the detail of the changes that have been made to the Supplier's product or service. A new application needs to be created by the Supplier and the Upgrade Form needs to be signed and uploaded to the new case. The person signing the Upgrade Form needs to be at minimum a "C" level individual within the organization (e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner). Along with the Upgrade Form, the Supplier needs to provide the necessary documentation such as

[1] Changes to alphanumeric characters following a dash (-) in the Part Number are not considered as a Part Number change and can be processed under Scenario #2: No change to Part Number. For example, the original Part Number is XXXX-AAA and the Part Number after product upgrade is changed to XXXX-BBB.

diagrams/drawings, configuration management documents, developer/release notes, product literature, samples, etc. that substantiate their claim.

Once the Upgrade Form is completed and the relevant documentation uploaded, the Lab will evaluate the changes and determine whether the updated product or service needs to go through partial or complete re-evaluation, or whether the changes do not affect the current requirements. In the latter case, the Lab will simply facilitate the update of the existing listing on the APL to include the updated product or service.

4.3 Additional Lab Testing

For cases where the Lab performs testing (via a Lab Test Data Report [LTDR]), the Supplier may need to submit the new version of the product and/or artifacts to the Lab as part of the upgrade evaluation. Timeframes for submission of such data must comply with the time limits set under the evaluation process in order to avoid rejection of the application.

5. Lab Transfer Notification

A Supplier may wish to use the services of a different Lab instead of the initially selected Lab under a variety of circumstances. Lab transfers may be made midstream of an evaluation or can be made during an upgrade evaluation, i.e. wherein one Lab performed the initial evaluation, while another performs the upgrade.

In order to change the Lab assigned to a particular case, the Supplier must submit, in writing, a request for change to GSA at fips201eplabmain@gsa.gov. Below is a list of the minimum information that must be included in the request for change.

- Point of Contact Information (Name, email address, telephone number),
- Direction of transfer (Old Lab name to New Lab name),
- Product Name,
- Case Number, and
- APL Number (If applicable)

Once the request is received and found acceptable, GSA will make the provisions necessary to transfer the evaluation to the new Lab. The Supplier point of contact will be notified by GSA once the transfer process has been completed.

6. Updates to the Approved Products List

The Approved Products List (APL) is a list of products and services that have been evaluated by the Labs and have been deemed to meet the requirements necessary for compliance to a particular product or service category respectively. In this context, the APL is dynamic and only lists those products and services that are in compliance with the current version of the Standard and it's supporting Publications.

Updates are made to the APL as products and services are upgraded based on the revisions to the Standard, the product development lifecycle, and technology advancements.

Suppliers update their products and services as described in Section 4 or they may wish to remove their listing from the APL when the product has completed its lifecycle and is no longer being offered for sale. In the latter case, Suppliers need to contact the Lab that performed their evaluation and request removal. The Lab then coordinates with GSA to ensure that the necessary updates are made to the APL. Product dependencies and cross-referencing rules apply as mentioned in Section 3.3.

Products that are removed from the APL are placed on the Removed Products List (RPL) in order to maintain a history and for archiving purposes.

In other situations, Supplier point of contacts listed on the APL may change due to employee turnover, reorganization or change in responsibilities. In order to change the point of contact for an APL line item, the Supplier must submit, in writing, a request for change to GSA at fips201eplabmain@gsa.gov. Below is a list of the minimum information that must be included in the request for change.

- APL Number(s)
- Product Name(s)
- Supplier Name, and
- New Point of Contact Information (Name, telephone number, email address)

Once the request is received, GSA will make the necessary updates within one (1) business day. The Supplier point of contact will be notified via email once the change has been completed[2].

[2] Please note that only the Point of Contact (POC) on the APL can be updated. The POC that was listed on the Application cannot be changed as this needs to be maintained as part of the evaluation record.

Appendix A – Approval Mechanisms

The Lab uses the following means to evaluate submitted products and services. Based on the category type, one or more approval mechanisms may be used in order to determine compliance.

A.1 Site Visit

A *Site Visit* (SV) primarily involves Lab Engineers visiting the specified site in order to evaluate the Product/Service offered by the Supplier. Site visits are considered necessary in those circumstances when the Supplier is offering a Product/Service that cannot be brought into the Lab due to some constraint (e.g. size).

The duration of a site visit is limited to two (2) consecutive business days. Lab Engineers participating in the site visit will be available to the Supplier to identify and help to remediate any areas of non-conformance. After two business days, the site visit activity will end and the evaluation report will be written based on the status of the site visit at the end of the second day.

A.2 Vendor Test Data Report

The *Vendor Test Data Report* (VTDR) is a technical report submitted by the Supplier demonstrating the conformance of the product or service to one or more requirements for that category. The submitted test report is reviewed and evaluated to determine how the product or service was tested to arrive at the conclusion that it meets the requirements set forth and should be forwarded to the Lab, via electronic upload during application package submission.

The VTDR must contain sufficient data to show that each applicable VTDR requirements is met. The VTDR must at a minimum include:

- Date and time the test was performed
- Name, phone number, and e-mail address of the tester.
- Detailed description of the test procedure performed
    - A statement justifying how this test meets/satisfies the requirement specified.
    - If test procedures are automated (e.g. – test program or scripts), the VTDR should detail the procedural steps performed within the software.
    - Data values verified/stored in reference implementations must be included in the VTDR.
    - A description of hardware and software used to test conformance, including model numbers and versions (if applicable for testing).
- Test results of each test procedure

Note: Use of reference devices (e.g. – smart cards or readers) may be used for confirmation of requirements. However, it is ultimately the Supplier's responsibility to ensure that reference devices are adequate and comply with the necessary and applicable requirements.

A.3 Lab Test Data Report

The *Lab Test Data Report* (LTDR) is a technical report generated by the Lab during the evaluation process. This report provides the test results for requirements that are tested in the Lab.

A.4 Vendor Documentation Review

Vendor Documentation Review (VDR) is a review of the documentation provided by the Supplier to determine compliance of the product or service to one or more applicable requirements. “Attestation Letters” or documentation which regurgitates the requirement in another form for use by Evaluation Program will not be accepted as legitimate vendor documentation. Vendor documentation should be documentation that is developed to coexist with the Product or Service provided by the Supplier and must not be targeted specifically to meet the requirements of the Evaluation Program. Examples of valid vendor documents include user guides, developer guides, third party testing, whitepapers, etc.

A.5 Certification

Certification (C) refers to the process by which the vendor produces a certification (from an authority other than an EP Lab) statement stating the compliance of the product or service to a particular requirement (e.g. FIPS 140-2 certification).

A.6 Attestation

Attestation (A) refers to a formal statement provided by the Supplier (a minimum “C” level individual, e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner) providing testimony to the fact that the product or service meets the necessary requirements for that category.

Appendix B – Abbreviation and Acronyms

APL	Approved Products List
CHUID	Card Holder Unique Identifier
EP	Evaluation Program
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
LTDR	Lab Test Data Report
NIST	National Institute of Standards and Technology
OGP	Office of Government-wide Policy
OMB	Office of Management and Budget
PIV	Personal Identity Verification
SV	Site Visit
VDR	Vendor Documentation Review
VTDR	Vendor Test Data Report