



Federal Information Processing Standard (FIPS) 201 Evaluation Program Concept of Operations (ConOps)

Version 1.3.3

Final

June 12, 2014

Table of Contents

1	Introduction	3
1.1	Background	3
1.2	Goals and Objectives	4
1.3	Scope	4
2	FIPS 201 Product and Services Evaluation Program	5
2.1	GSA Responsibilities	5
2.2	NIST Responsibilities	5
2.3	Elements of Testing.....	6
2.3.1	<i>Physical Access Control Systems (PACS)</i>	6
2.3.2	<i>Logical Access Control Systems (LACS)</i>	6
2.3.3	<i>Credentialing Systems</i>	6
2.3.4	<i>Usage</i>	6
3	Testing Framework	7
4	Test Design Phase	9
4.1	Requirements Management	9
4.2	Test Suite Package	9
4.3	Testing Types	10
4.4	Roles and Responsibilities	11
5	Two-Stage Evaluation (Testing) Phase	12
5.1	Testing Process Overview.....	12
5.2	Evaluation Modes	16
5.2.1	<i>Vendor Assertion</i>	16
5.2.2	<i>Vendor Self-testing</i>	16
5.2.3	<i>Witness Testing</i>	17
5.2.4	<i>Independent Verification</i>	17
5.3	Lab Interaction with Applicants.....	18
5.4	Laboratory Principles and Practices.....	18
5.4.1	<i>Privacy and Confidentiality</i>	18
5.4.2	<i>Scheduling</i>	18
5.4.3	<i>Security</i>	19
6	Approval Phase	20
6.1	Approval Process	20
6.2	Approval Documentation	21
6.3	Non-Conformance Review	22
7	Optimization Phase	23
7.1	Program Review	23
7.2	Stakeholder Feedback	23
7.3	Special Review Team.....	24
Appendix A	Acronym List	25
Appendix B	References	26

Tables

Table 1: FICAM Test Specification Components.....	10
Table 2: Benefits and Limitations of Vendor Assertion Testing	16
Table 3: Benefits and Limitations of Vendor Self-Testing.....	17
Table 4: Benefits and Limitations of Witness Testing.....	17
Table 5: Benefits and Limitations of Independent Verification.....	17
Table 6: ICAM Testing Approval Documentation	21
Table 7: Stakeholder Feedback Mechanisms.....	24

Figures

Figure 1 FICAM Testing Program.....	4
Figure 2: FIPS 201 Evaluation Program Testing Framework.....	7
Figure 3: FIPS 201 Evaluation Program Approval Process Flow.....	15
Figure 4: FIPS 201 Evaluation Program Approval Process.....	20

1 Introduction

1.1 Background

The landscape for Identity, Credential, and Access Management (ICAM) is constantly evolving. Several policy drivers ([Homeland Security Presidential Directive 12](#) [HSPD-12], [Office of Management and Budget \(OMB\) Policy Memorandum 11-11](#) [OMB M-11-11], [OMB Memorandum 06-18](#) [OMB M-06-18], [OMB Memorandum 05-24](#) [OMB M-05-24], OMB's memorandum entitled "Requirements for Accepting Externally Issued Identity Credentials" [Credentialing Memo], and the [FICAM Roadmap and Implementation Guidance](#) [FICAM Roadmap]) have required federal agencies to upgrade their ICAM technologies to support new functionality and needs. The Federal Government's emphasis on strong authentication for physical and logical access to federal agencies contributes to the growing need to support agency implementers as they upgrade existing ICAM systems.

Agency support includes clear, consistent policy and guidance regarding acquisition of products and services (e.g., HSPD-related products and services). For example, [Federal Acquisition Circular 2005-19 Sub part 4.13](#) [FAC 2005-19] states that "in order to comply with FIPS PUB 201, agencies must purchase only approved personal identity verification products and services." Other key acquisition policy and guidance includes, but is not limited to [OMB M-05-24], [OMB M-06-18], [OMB M-11-11], , [Federal Acquisition Regulation Case 2005-017](#) [FAR Case 2005-017], and National Institute of Standards and Technology (NIST) Special Publication 800-53 R4 [NISTSP 800-53] security controls IA-5(15), IA-8(3), and SA-4(10).

The General Services Administration (GSA) is responsible for both the Federal ICAM (FICAM) initiative and the tools and programs related to the federal acquisition process. These responsibilities uniquely position GSA to provide testing services related to acquiring products and services for ICAM implementation. Accordingly, the GSA is responsible for supporting the adoption of interoperable and standards-based ICAM technologies throughout the Federal Government. As part of that responsibility, GSA operates the FICAM Testing Program to ensure product and service conformance and compliance. As Figure 1 shows, the FICAM Testing Program includes:

- ***The Federal Information Processing Standard (FIPS) 201 Evaluation Program*** - focuses on the HSPD-12 / FIPS 201 initiative through the authority assigned in [OMB Memorandum 05-24](#). In addition, as [OMB Memorandum M-06-18](#) notes, "GSA has established the FIPS 201 Approved Products List for all products and services that have been approved under the GSA FIPS 201 Evaluation Program."
- ***The HSPD-12 Shared Provider / Integrator Program*** - identifies qualified integrators for HSPD-12 / PIV related products and services.
- ***The Trust Framework Solutions (TFS) Testing Program*** - focuses on products and services that enable secure and streamlined citizen and business facing online service delivery through the authority assigned in [Credentialing Memo] and *National Institute of Standards and Technology (NIST) Special Publication 800-53* [NISTSP 800-53] control enhancements IA-8(2) and IA-8(3).

1.2 Goals and Objectives

The overall goal of these Testing Programs is to provide a comprehensive evaluation capability to support the selection and procurement of qualified products and services for the implementation of a federated and interoperable ICAM segment architecture. The primary objectives are to:

1. Provide a common government-wide testing capability for ICAM products and services;
2. Provide compliance, consistency and alignment of commercially-available products and services with the requirements and functional needs of government ICAM implementers;
3. Ensure availability and choice among vendor products and services to support different ICAM components;
4. Coordinate interaction and coordination with the ICAM vendor community to improve the inclusion of ICAM requirements into product and service offerings; and
5. Promote cost effective ICAM implementation through qualification of products and services that have been demonstrated to perform successfully.

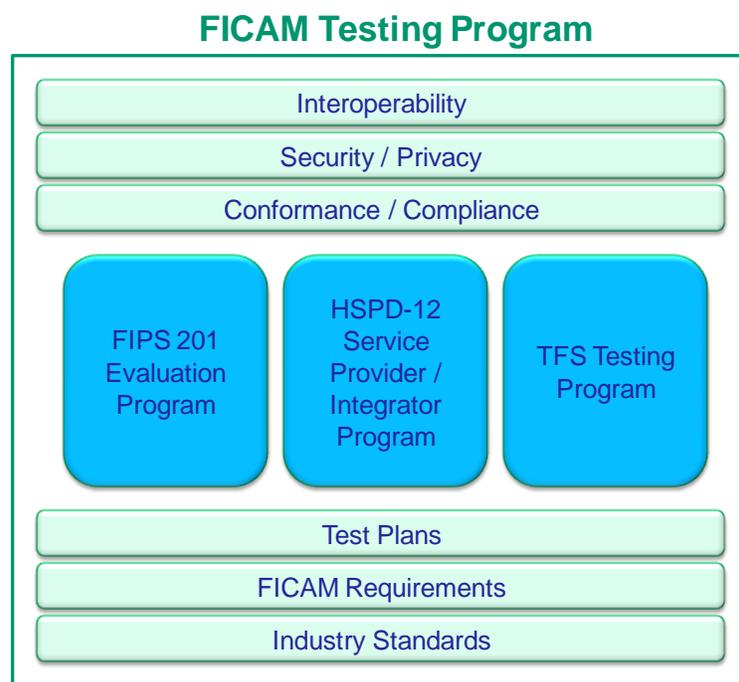


Figure 1 FICAM Testing Program

1.3 Scope

This document focuses solely on the FIPS 201 Evaluation Program. Information regarding the TFS Initiative and its TFS Testing Program can be found at <http://idmanagement.gov/trust-framework-solutions>. For Information regarding the HSPD-12 Service Provider / Integrator Program, contact Chi.Hickey@gsa.gov.

2 FIPS 201 Product and Services Evaluation Program

2.1 GSA Responsibilities

To support the implementation of HSPD-12 and the goals and objectives of the Federal ICAM effort, GSA manages the FIPS 201 Evaluation Program (Program). As specified in [OMB M-06-18], the Program is responsible for evaluating and approving products and services required for the implementation of HSPD-12 as compliant with specified FIPS 201 requirements. [OMB M-06-18] also notes that the Program is responsible for providing product interoperability and performance testing.

Towards this, GSA has identified categories of products and services for which normative requirements are expressed in NIST publication FIPS 201 and associated technical specifications. Specific evaluation and approval requirements for each of the categories of products and services have been established and publicly posted. Each Approval Procedure cites the specific FIPS 201 requirements that are evaluated for that category of product/service and the type of evaluation needed for approval. The categories of products and services for the Program and Approval Procedures for all of those categories are posted at the [FIPS 201 Evaluation Program website](#). GSA has established the [FIPS 201 Approved Products List \(APL\)](#) to list all products and services that have been approved by the Program.

As noted in [OMB M-06-18], there are other types of services that may be necessary for HSPD-12 systems and deployments, but have no normative requirements specified in FIPS 201 and, therefore, are not included in the Program (e.g., integration services, contractor managed services and solutions). Qualification requirements for these services and a list of qualified vendor services are posted at [IDManagement.gov](#).

The goals and objectives of the Program are consistent with the directives and objectives of [OMB M-05-24] and [OMB M-06-18], both of which give GSA the authority to implement and manage the Program.

2.2 NIST Responsibilities

NIST also has responsibilities for supporting implementation of HSPD-12 and the goals and objectives of the Federal ICAM effort. NIST authors authoritative specifications and supporting guidance (e.g., FIPS 201, NIST SP 800-73). The documents include guidelines for testing PIV Card Application and Middleware Interfaces (NIST SP 800-85A) and conformance to the PIV Data Model (NIST SP 800-85B).

NIST has established the [Personal Identity Verification Program \(NPIVP\)](#) to validate Personal Identity Verification (PIV) components required by Federal Information Processing Standard (FIPS) 201. The objectives of the NPIVP are (a) validate the compliance/conformance of two PIV components: PIV middleware and PIV card application with the specifications in NIST SP 800-73; and (b) provide the assurance that the set of PIV middleware and PIV card applications that have been validated by NPIVP are interoperable.

NIST oversees the [National Voluntary Laboratory Accreditation Program \(NVLAP\)](#), which provides third-party accreditation to testing and calibration laboratories in response to legislative actions or requests from government agencies or private-sector organizations.

NIST also has published the [Public Key Interoperability Test Suite \(PKITS\)](#), which is a comprehensive X.509 path validation test suite designed to test applicable HSPD-12 products against most of the features specified in the [X.509 Certificate and CRL Profile](#) and [RFC 3280](#).

2.3 Elements of Testing

The elements of testing under the current Program will expand to cover a comprehensive set of policies and technologies that are critical to the implementation of the target-state architecture. The updated Program includes solution segments such as Physical Access Control Systems (PACS), Logical Access Control Systems (LACS), Credentialing Systems, and Usage. In general, solution segments are comprised of different components related to ICAM-specific technologies and solutions. The detailed listing of test segments is available at the [FIPS 201 Evaluation Program website](#).

2.3.1 Physical Access Control Systems (PACS)

PACS serve to physically guard and control points of access to individuals through restricted entryways. Key elements of PACS include forward-facing physical access security features such as validation systems, card readers, and head end systems. These elements together are tested end to end to certify system interoperability and compliance with FIPS 201 standards

2.3.2 Logical Access Control Systems (LACS)

LACS are used for authentication, authorization, and accountability within computer information systems. They enforce access control measures for humans, devices, and processes seeking access to an information system resource.

2.3.3 Credentialing Systems

Credentialing systems support the full life cycle management of physical cards that are used by end users (e.g., in PACS or LACS systems, as flash pass). Test elements in this category address enrollment of a person seeking a card (e.g., capturing the person's biometrics to put in the card and to identify the person in subsequent enrollment or card management activities), production and issuance of cards, and maintaining information on the card and about the card and cardholder.

2.3.4 Usage

Usage pertains to tools, utilities, and services that support features such as digital signature, digital encryption, X.509 certificate validation, and secure communication. All these services play a vital role either as a stand-alone service or as part of another APL component.

3 Testing Framework

The Program is a continuously-improving process with the ability to adapt to new products and services developed by industry. The Program provides a feedback loop for vendors that undergo the evaluation process and agencies that are the end customers of the APL, thus enabling the Program to make improvements as necessary. New product and service categories and test procedures are introduced and incorporated into the Program as a result of the feedback process and changing federal requirements. This allows GSA to meet the needs and challenges of its customers and stakeholders as requirements and technology evolve. This new continuous adaptation to always keep the Program current, reliable, and optimized is referred to as the “Spiral Implementation” methodology.

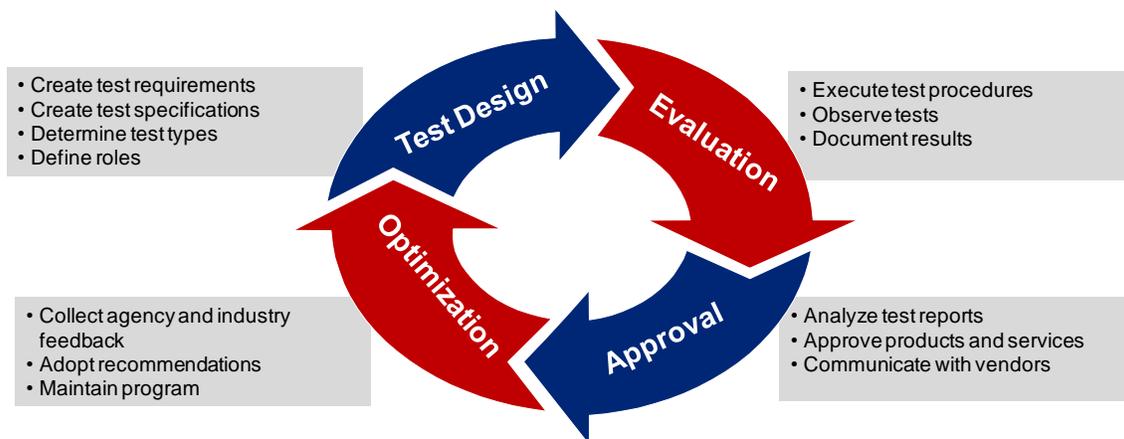


Figure 2: FIPS 201 Evaluation Program Testing Framework

As Figure 2 illustrates, the Program's testing framework is a four-phase cyclical process that includes clear entry and exit points and creates a fluid mechanism for product and service evaluation and testing program maintenance and improvement. The four phases that comprise the Program's testing framework are listed below. Each phase is discussed in detail in Sections 4 through 7:

- **Test Design.** Test design includes defining the types of testing to be performed and the roles and responsibilities of the stakeholders involved across the entire Program. Test processes and procedures will be developed by leveraging existing and creating new requirements from federal standards, policy, and guidelines. As new testing approaches are developed, they will be first implemented and vetted by the GSA's ICAM Test Lab.
- **Two-Stage Evaluation (Testing).** Once the objectives are defined and established, the testing processes and procedures can then be executed. In evaluation, the testing artifacts developed in test design are used to evaluate products and services. The test results will indicate whether a product or service conforms to [Federal Information Processing Standards \(FIPS\) Publication 201, Personal Identity Verification \(PIV\) of Federal Employees and Contractors](#) [FIPS 201] and/or FICAM. As mentioned earlier, the Program is continuously adapting in order to respond to new technologies and federal requirements. Therefore, the testing approach incorporates two-phased testing. Testing using proven, well-established techniques are performed by the Certified Testing Labs (CTLs). Testing for new technologies, or using new methods, are performed at the ICAM

Test Lab. When new federal requirements or technology evolves that effect changes in categories and testing procedures, the development and implementation of those changes will be performed by the ICAM Test Lab until the category and testing is deemed well-defined and repeatable, and can be transitioned to the CTLs. Lastly, for specific product and service categories, additional testing may be required by International Organization for Standardization (ISO)-certified laboratories. To determine if these special testing requirements apply, review the Test Requirements and Approval Procedures for categories of interest. Note that CTLs must be certified by the National Voluntary Laboratory Accreditation Program (NVLAP).

- **Approval.** Observations made during the evaluation phase will be analyzed by the validation agent and a decision will be made by the approval authority to approve the product/service.
- **Optimization.** As part of the “Spiral Implementation” methodology, GSA will actively seek input from vendors, agencies, and Labs in order to maximize Program efficiency and to keep the Program current as well as responsive to community needs. A continuously-improving Program will enhance GSA’s ability to serve all stakeholders and will provide the ability to adapt to changes in industry standards and technology, and enhance GSA’s capability to drive FICAM alignment across the federal environment. Data gathered from feedback in the optimization phase will be used to optimize all phases of the Program.

4 Test Design Phase

The test design phase captures the objectives of the testing approach, establishes test boundaries, and consists of sub-phases and elements that, in combination, are used to guide and define the steps that make up the evaluation phase. This phase includes gathering and managing testing requirements, defining specifications for tests that will be conducted, selecting types of testing that will be performed, and determining roles and responsibilities across the evaluation process.

4.1 Requirements Management

Requirements management is the process of documenting, analyzing products and/or services, and determining types of testing that will be needed. For the Program, test requirements will be collected from known and trusted sources including but not limited to:

- Standards bodies such as ISO and the National Institute of Standards and Technology (NIST);
- Federal agencies;
- Industry; and
- CTLs.

When new requirements need to be identified and developed, it is expected that the process would include an integrated team (including developers and testers) within the Program to ensure system functionality and product/service knowledge perspectives.

Each product and service will be tested against a common set of requirements. Those requirements will be isolated and aggregated for each product and service test, and organized in the form of a requirements traceability matrix (RTM). The RTM enables the performance of standardized tests in the evaluation phase, resulting in consistent procedures and accurate comparative results.

4.2 Test Suite Package

The process for developing test specifications will establish the validation and approval procedures for the test requirements. This process focuses on the desired outcomes of the test requirements and establishes the benchmarks for what constitutes a valid and successful test. The test specification adds value to the test process by standardizing the test execution. Standardization provides validity to the tests and ensures that the CTLs will complete each individual test consistently, providing for more accurate test results. The test specification will define the scripts, data, software, and hardware for each type of testing (see 4.3 for more details).

Several elements comprise the test specification process to include test procedures, approval procedures, test data, test tools, test environment requirements, and test scenarios. Table 1 outlines what will be included in the test specification for FICAM testing.

Test Specification Output	Description
Test Procedures	Standardized, executable instructions for testing requirements.
Approval Procedures	Standardized process for analyzing Test Reports and approving or denying products and services for listing on the APL.
Test Data	Input values for specific tests, which are used to verify that a test has been executed and that the expected outcome has been achieved.
Test Tools	Common artifacts and resources used by the vendors and Labs for configuration and testing of products and services.
Test Environment Requirements	Mandated requirements and specifications for preparing and configuring the test environment to execute the test procedures. Also includes the list of equipment needed to prepare and configure the test environment.
Test Scenarios	Specific use cases for testing products and services based on positive and negative products and services and the real-world application of products and services.

Table 1: FICAM Test Specification Components

4.3 Testing Types

A sub-element of the test specification development process is the determination of the type of testing that will be completed during the testing process. For the purposes of FICAM Testing, tests will be designed to validate that vendor solutions meet the requirements and prerequisites for [FIPS 201].

The types of testing that will be performed under the Program are:

- **Technical Conformance.** Technical conformance testing validates the functionality of individual components in an isolated environment and confirms that the individual components meet the detailed design standards and specifications. The test requirements and test specifications under this type of testing are driven by [FIPS 201]. Conformance with [FIPS 201] testing is considered to be a baseline for ICAM compliance.
- **Functional.** Functional testing validates the functionality of the complete system in an environment that mimics real-world use and confirms that the complete system meets the functional, technical, and business requirements. Functional testing acts as a baseline reference for the test platform, and provides insight into how components might work in an operational environment. The test requirements and test specifications under this type of testing are driven by specific applications and use cases the product or service must fulfill in order to achieve proper functionality (e.g., email encryption using a PIV certificate).
- **Interoperability.** Interoperability testing validates that multiple products and services can successfully work together utilizing standard interfaces, protocols, and specifications.
- **Performance.** Performance testing validates the system capacity, response time, and throughput under different stresses, loads, and volume in an environment that mimics real-world use.
- **Security.** Security testing analyzes system threats and vulnerabilities and assures the issues identified are mitigated.

4.4 Roles and Responsibilities

The final element of the test design phase is establishing the roles and responsibilities across the evaluation program. The roles may be (in some cases are) required to be filled by more than one individual.

- **Approval Authority.** The Approval Authority is established by GSA Office of Government-wide Policy (OGP) and is responsible for reviewing final Test Reports, approving or rejecting products and services for the APL, and communicating approval decisions with the Applicant in conjunction with the CTLs. GSA OGP will be responsible for developing and maintaining test documentation, maintaining test tools and infrastructure, providing access to a web based case management system, and maintaining the Program website.
- **Applicant.** The Applicant submits a product or service to CTLs for evaluation. The Applicant is responsible for submitting completed applications and providing the CTL with evidence, documentation, and access to technical staff as needed during the evaluation process. Applicants should make every effort to debug their products or services prior to submission. Applicants should also visit the Program website or contact the Program Approval Authority for questions and detailed information on the importance of the Program evaluation process and how the evaluation process works. Applicants shall self-certify that their products and services are interoperable with any other systems, products, services, or components on the APL and have passed security testing according industry standards.
- **CTL Staff.** CTL staff are responsible for the overall operation of the Lab, product/service evaluation and evaluation oversight, quality assurance, managing relationships, and communicating status of testing, and assisting applicants within navigating the testing process. CTLs must be compliant with *GSA FIPS 201 Laboratory Specification Version 7.0.0* [Lab Spec] and the *FIPS 201 Evaluation Program Development Laboratory Concept of Operations* [Lab ConOps], which specify the minimum number of staff required for a CTL.
- **Validation Agent.** The Validation Agent is established by GSA OGP and is responsible for reviewing and validating the Test Reports delivered by the CTLs. Once the Test Reports are reviewed and validated, the validation agent sends a validation report to the Approval Authority.

5 Two-Stage Evaluation (Testing) Phase

The evaluation phase is where the testing execution is performed. Inputs to this phase include the test procedures that will test products and services against the requirements developed in the test design phase. The output from this phase is the Test Report, which includes detailed observations of a completed product or service test. The Test Report indicates to the Approval Authority whether a product or service is suitable for publication on the APL.

5.1 Testing Process Overview

The testing process occurs in five phases, which are detailed below. The main method of communication between all primary actors (i.e., Applicants, Labs, Validation Agent, Approval Authority) in the testing process is a web-based tool. Applicants will submit a complete application to a CTL for product or service evaluation. The CTL will evaluate the product or service and enter information on the web-based tool at various points during the evaluation process. If the product or service does not pass evaluation testing, the CTL notifies the Applicant. If the product or service passes the evaluation testing, the Approval Authority will be notified and will make an approval decision.

- **Registration.** The evaluation of products and services under Evaluation Program Development (EPD) is carried out using a GSA-provided website. Applicants who desire to have their product or service evaluated will go to the website, register, and obtain information regarding the evaluation process. Applicants can gather relevant information (e.g., application forms, product and service categories, approval procedures) regarding the evaluation program, its goal, and what is expected from them if they were to submit their product and/or service for evaluation against the requirements of [FIPS 201] and its related publications.
- **Application submission.** The applicant submits a complete application package to the CTL. Note that details of the contents of the application package may vary based on the product or service category and are available to Applicants from the Program website. The application package contains the following: *Evaluation Application Form*, evaluation fees, *Lab Service Agreement*, the product (hardware and / or software) or service intended for evaluation, complete documentation (e.g., user manuals, installation guides), other necessary hardware or software to enable use of the product/service; and required approval mechanism data (i.e., certifications, attestations, vendor test data).

Upon receipt of the application package, the CTL schedules the evaluation based on a First-In-First-Out (FIFO) scheme. The CTL reviews the package for completeness. If the application is complete, the product or service submitted for testing is entered into the testing queue and the CTL updates the evaluation status for the Applicant's product or service on the Program's website. In addition, a case file is created for the Applicant's product or service in order to manage all Applicant submissions to the CTL. The Applicant's submission is then placed in the Lab evaluation queue whereby it will wait its turn to undergo evaluation for compliance against the mandatory requirements of the applicable category.

If the application is incomplete, the application is returned to the Applicant with notification of any deficiencies and information on next steps. The Lab will retain a copy of the application package. An incomplete package will be held on file for thirty (30) days and destroyed after sixty (60) days if deficiencies are not addressed. If an application package is destroyed, the Applicant must resubmit their application package.

- **Evaluation.** The CTL conducts the required tests for the submitted product or service. This step includes configuring the Lab for the correct tests, executing the test procedures, documenting the test results, and recording observations. In the case where the Applicant submits a product to the Lab for evaluation, the Lab Engineers will begin their evaluation by reading the installation procedures and installing any associated product software and/or hardware device drivers.

During the testing, if the Lab identifies issues (e.g., corrupted software, incorrect version, damaged components, missing data reports / documentation), the Lab will contact the Applicant within one (1) business day to resolve the issues. If the Lab Engineers are experiencing difficulty with a product and the Applicant is not available or able to assist the evaluation process, evaluation may be suspended until all issues have been rectified by the Applicant. Communication between the Lab and the Applicant is considered necessary as it is important for the Lab to ensure that the product is installed and configured properly such that it behaves as expected, in a consistent manner and is capable of meeting the criteria for approval. As testing is conducted, the Program website is updated to reflect status. When testing has commenced, the CTL updates the evaluation status to “Evaluation under progress” in the Program Website.

- **Reporting.** The CTL summarizes the evaluation process and the Lab Director provides the final sign-off on the evaluation report. The CTL then submits a Test Report. If the Test Report indicates a product or service passed the testing, the report is sent to the Validation Agent. If the Test Report indicates a product or service failed the testing, the CTL notifies the Applicant. The Applicant can review the report with the CTL to discuss deficiencies in the product or service, repair the deficiencies, and then resubmit the product or service for testing. Once prepared, the CTL updates the evaluation status for the Applicant’s product or service in the Program Website to reflect “Evaluation Report Complete” or “Failure Noticed Submitted” (as applicable). The CTL will ensure that the evaluation report displays the sensitivity marking “EPD CONFIDENTIAL” on each page of the report. Additionally, the CTL restricts the distribution of the report only to the Approval Authority for products and services that are compliant with all requirements in their respective category(ies).

The Applicant can dispute the evaluation result with the Lab via a non-conformance review process. Details of the non-conformance review are provided in later in this document. Applicants whose products or services have failed need to resubmit their application packages after correcting the deficiencies and wait their turn once again in the evaluation queue.

- **2ND Stage Evaluation.** If for the given product or service second-stage testing is relevant, the Lab will forward the test package and tested equipment to the ICAM Test Lab for 2nd stage testing evaluation. Should the testing process at this stage result in a “Fail”, the ICAM Test Lab will provide a failure report to the vendor and provide assistance in understanding the result. Should the evaluations be successful, a final Test Report will be prepared and submitted to the Validation Agent for review.
- **Approval.** If a product or service has passed the evaluation testing stages(s), then the Approval Authority will write a Letter of Approval for the Applicant and send the letter to the CTL that conducted the testing. The CTL notifies the Applicant by sending the Letter of Approval and adds the product or service to the APL.

Figure 3 graphically represents the testing process.

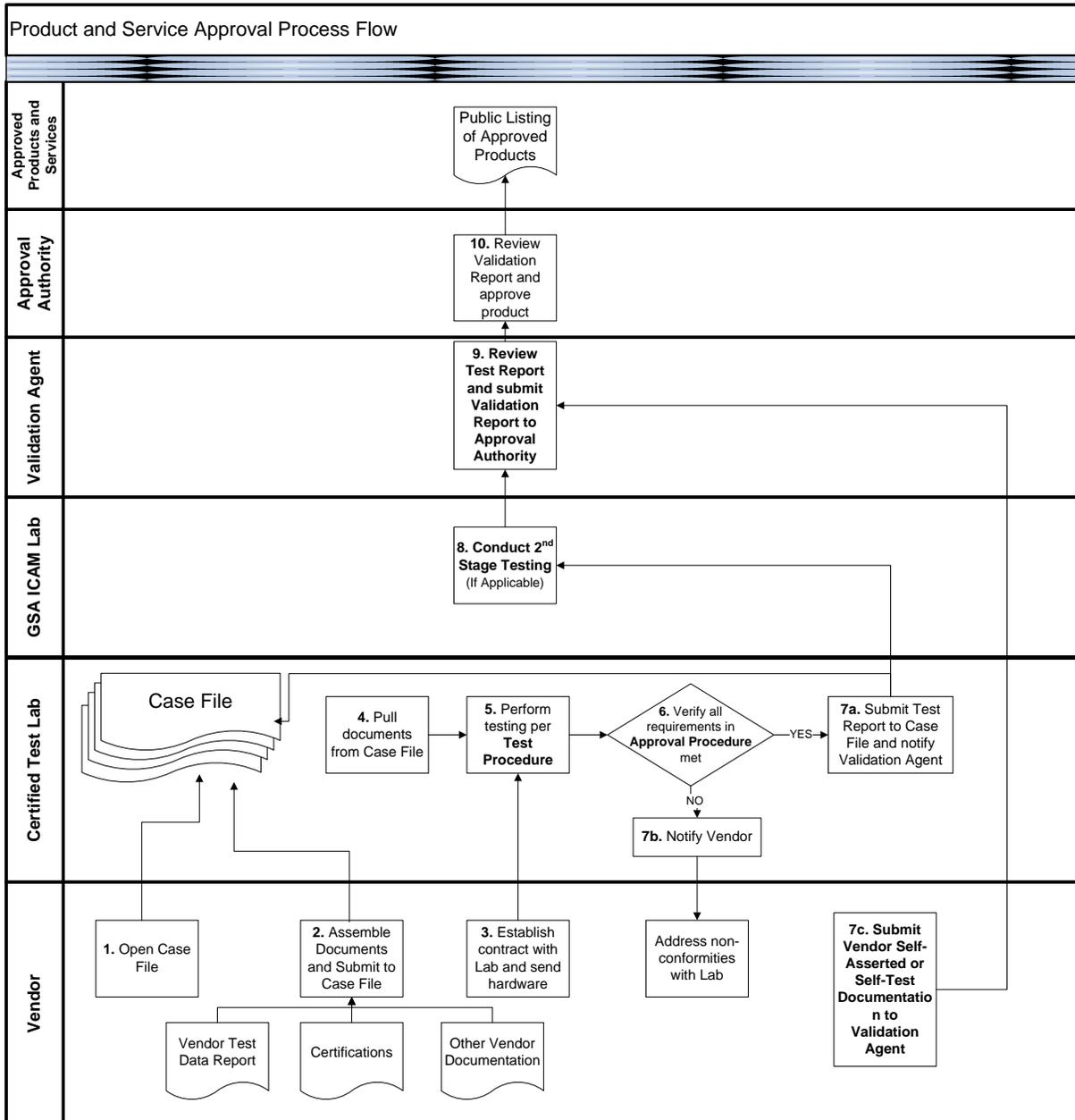


Figure 3: FIPS 201 Evaluation Program Approval Process Flow

5.2 Evaluation Modes

There are several methods for evaluating vendor products and services: vendor assertion, vendor self-testing, witness testing, and independent testing. Based on the risk, priority, cost, time, and complexity of validating FICAM requirements, GSA may accept different methods or a combination of methods to develop the evidence required for evaluation.

5.2.1 Vendor Assertion

Vendor assertions enable product and service vendors to provide documentation packages stating how their product or service passes a test for conformance and interoperability with HSPD-12/FICAM requirements. This package may include a summary of functionality and implementation approaches for meeting the HSPD-12/FICAM requirements and the basis for stating compliance. Additionally, the documentation package may include product/service test evaluation results from evaluation or testing entities independent of CTLs. Depending on the product/service test evaluation results, GSA would have the discretion to accept the results without requiring the product/service to undergo repetitive testing under the Program. Testers will in turn inspect the product/service documentation to verify that the information is complete without judging the quality of the documentation or its accuracy. This method of evaluation may be appropriate for tests that are low priority for GSA and require by-products of the vendor product developments. For example, vendor assertion used to reference part numbers and components, product certifications, partner agreements, and published guides or manuals.

Benefits	Limitations
<ul style="list-style-type: none"> • Low level of effort for GSA • Provides references to existing published documentation, such as certifications, to reduce testing redundancy 	<ul style="list-style-type: none"> • Accuracy relies on vendor claims about their own product

Table 2: Benefits and Limitations of Vendor Assertion Testing

5.2.2 Vendor Self-testing

Vendor self-testing enables product/service vendors to execute GSA-approved and NIST-approved test procedures and provide the supporting documentation for evaluation. Testers will review the documentation to determine if the test was appropriately executed and if the results are acceptable. This method of evaluation may be appropriate for tests that are low priority for GSA and require an extensive level of effort for integration of the vendor product/service into a test environment. In addition, this method may be used to verify that the vendor has performed initial compliance testing and debugging prior to submitting a product/service for evaluation. For example, a vendor may self-test pre-requisite requirements before submitting for independent testing.

Benefits	Limitations
<ul style="list-style-type: none"> • Low level of effort for GSA • Enables vendor to perform integration of their own product/service • Enables vendor to perform initial testing of low risk requirements and resolve issues during product/service development 	<ul style="list-style-type: none"> • Requires vendors to have the tools and data necessary to execute the test procedures • Requires accurate configuration of test environment by vendor • Accuracy relies on vendor testing of their own product/service • Accuracy relies on vendor expertise with HSPD-12/FICAM testing

Table 3: Benefits and Limitations of Vendor Self-Testing

5.2.3 Witness Testing

Witness testing enables testers from a CTL to oversee, or witness, live test execution in the field or a vendor facility in person. The tester will observe the vendor personnel execute the tests on vendor equipment and analyze the test results. As part of the witness testing process, the testers will also verify that the test configuration and test procedures meet GSA and NIST specifications. This method of evaluation may be appropriate for tests that are medium priority to GSA and products/services that are too large to transport or are integrated systems.

Benefits	Limitations
<ul style="list-style-type: none"> • Low level of effort for GSA • Enables vendor to perform integration of their own product/service • Enables independent oversight of testing activities and results • Provides technical expertise in executing the tests and analyzing the results 	<ul style="list-style-type: none"> • Requires vendors to have the tools and data necessary to execute the test procedures • Requires travel for testers of certified Labs • Test results may be specific to vendor configuration • Test environment may not be controlled

Table 4: Benefits and Limitations of Witness Testing

5.2.4 Independent Verification

Independent verification enables testers to integrate and test vendor products/services in a CTL. The testers will follow vendor documentation to install and configure the product/service for testing and then execute GSA-approved and NIST-approved test specifications in a controlled test environment. After executing the tests, the testers will analyze the Test Reports to determine if the results are acceptable. This method of evaluation may be appropriate for tests that are high priority to GSA.

Benefits	Limitations
<ul style="list-style-type: none"> • Enables independent execution of testing activities and results • Provides consistent testing platform for consistency and repeatability • Provides technical expertise in executing the tests and analyzing the results 	<ul style="list-style-type: none"> • High level of effort for GSA • Requires testers to determine how to integrate and configure vendor products/services

Table 5: Benefits and Limitations of Independent Verification

5.3 Lab Interaction with Applicants

The Lab interacts with the Applicant in the following circumstances:

1. **Application package completeness:** During submission of the Application package, if the Lab determines that the submission of the Applicant is incomplete for any reason (e.g., incomplete Application Form, the Lab Service Agreement has not been signed by the Applicant), the Lab will contact the Applicant to resolve the issue.
2. **Deficiency remediation:** During the evaluation process, if the Lab identifies a minor deficiency (e.g., lack of critical documentation, corrupted software module), the Lab may contact the Applicant to seek assistance.
3. **Approval letter delivery:** Once the Approval Authority authorizes the placement of a vendor product or service on the APL and provides the Lab with the formal notification letter stating the same, the Lab forwards this approval letter to the Applicant after keeping a copy for their records.
4. **Failure notice delivery:** If the product or service does not meet the requirements for compliance with [FIPS 201], the Lab will notify the Applicant of the failure. The Lab notifies the Applicant in writing of each deficiency, and provides a detailed description of each deficiency.
5. **Non-conformance review:** If the Applicant disagrees with the results of the evaluation process, the Applicant can request a non-conformance review with the Lab to discuss any deficiencies found in the product or service.

5.4 Laboratory Principles and Practices

This section discusses the core principles and practices that underlie Lab operations.

5.4.1 Privacy and Confidentiality

Lab operations is predicated on privacy and confidentiality in accordance with applicable laws. Certain information collected and maintained by the Lab may be vendor confidential. Examples include the desire by a vendor to get its products/services evaluated in the Lab, failure to comply, or engineering information about the vendor's product or service. Similarly, some information is Lab confidential. Examples include which vendors are in, or planned to be in, the Lab for evaluation. For all these reasons, all vendors are required to sign a *Lab Service Agreement* to prevent the disclosure of proprietary information. The *Lab Service Agreement* protects all parties by establishing the terms and conditions for engaging the Lab, including a non-disclosure agreement.

5.4.2 Scheduling

Lab scheduling is flexible to accommodate priorities as they may evolve over time. As staff and resources allow, evaluation may occur in parallel. This includes evaluation of products or services within a product or service category or across different categories.

The Lab typically uses a FIFO scheme for evaluating products and services. After an application package is considered complete and accepted by the Lab, it awaits its turn for evaluation until all other products and services that have been received prior to it have been

completed. FIFO is typically used unless the Program directs the Lab to operate in another sequence based on current priorities.

5.4.3 Security

Lab security is critically important, particularly regarding the risk of disclosing proprietary or confidential information. Accordingly, the Lab institutes appropriate management controls, operational controls, and rules of conduct that are documented in [Lab Spec].

6 Approval Phase

The approval phase involves the review and analysis of the Test Report from the evaluation phase, resulting in a decision to include a product or service on the APL. In the broader framework for the Program, the approval process encompasses the new testing areas referenced in Section 2 to reflect a more diverse set of possible test results.

This section outlines the intended approval process, the approach for maintaining the APL, and making pertinent information available to agency customers and implementers.

6.1 Approval Process

The approval process starts when the Lab sends the Test Report to the Validation Agent, which is the point of exit for the evaluation phase (see Two-Stage Evaluation (Testing) Phase). Figure 4 illustrates the key steps in the approval process.

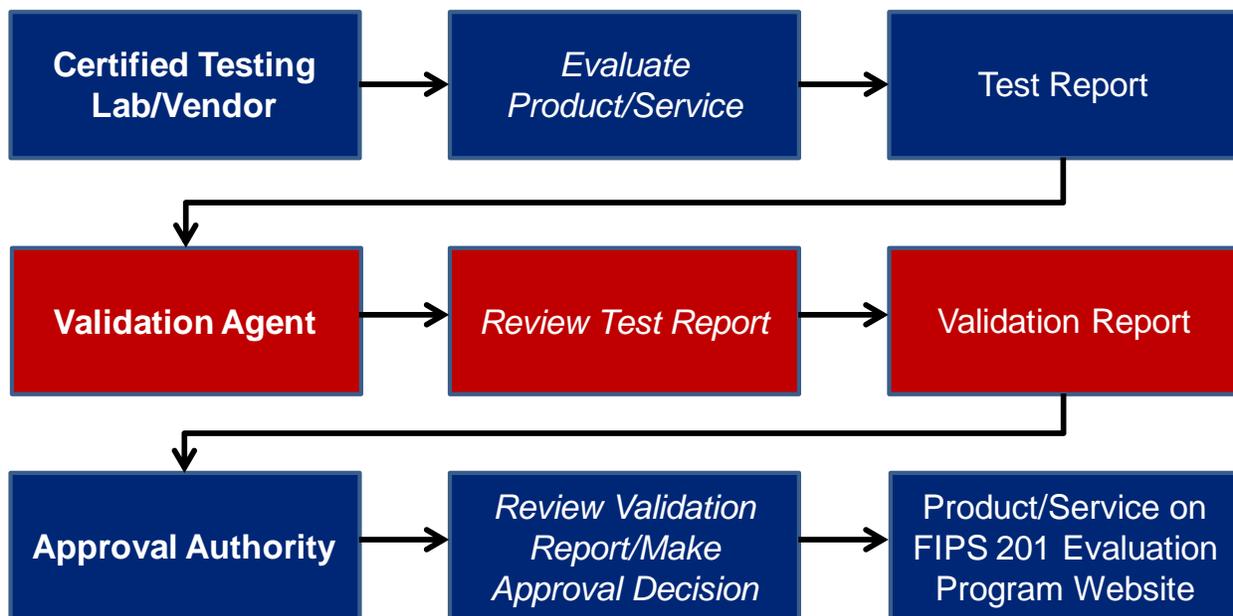


Figure 4: FIPS 201 Evaluation Program Approval Process

The following steps detail the approval process:

1. The CTL, Vendor, or ICAM Test Lab sends the Test Report to the Validation Agent.
2. The Validation Agent reviews and confirms the successful test completion of the particular product or service referenced in the Test Report.
3. The Validation Agent submits a validation report to the Approval Authority.
4. The Approval Authority reviews the validation report and approves the product or service.
5. The Approval Authority provides the Vendor with a certificate which contains details noting what product or service has been approved and what requirements the product or service was approved against.

6. The Approval Authority publishes the approved product and service information and accompanying report package on the Program webpage and changes the product/service website status to “Approval Complete”.

The maintenance of the approved products and services and the associated documentation is discussed further in the following section.

6.2 Approval Documentation

The approval process will generate several documents that will provide vendors with official recognition and certification and agency customers with detailed test information. Table 6 details the various approval documentation, the owners and recipients of each document, and a short description of each document.

Approval Process Document	Owner	Recipient	Description
Validation Report	Validation Agent	Approval Authority	Analyzes the Test Report generated by the CTL or Vendor at the end of the evaluation phase and confirms the successful completion of testing by a particular product or service.
Approval Letter	Approval Authority	Vendor	Confirms the successful completion of testing for a particular product or service and placement on the APL.
Product/Service Certificate	Approval Authority	Vendor	Formal recognition of successful test completion for vendors to attach to their approved products or services.
APL	Approval Authority	Agency customers, public	Web-based list of products and services available for procurement by agency customers.
Associated test information	Approval Authority	Agency customers, public	Information may vary based upon product or service category or test performed. The intended use is to provide additional usage details of items on the APL for agency implementers.

Table 6: ICAM Testing Approval Documentation

The information captured and distributed via the approval documentation achieves the Program objective to provide a useful service to the ICAM implementation community and to improve the selection and procurement of products and services that meet agency implementation needs.

6.3 Non-Conformance Review

An Applicant that has a disagreement with a Lab decision submits a *Non-conformance Review Form* along with the appropriate non-conformance review fees to the Lab Director. This form can be obtained from the Program website.

The form is reviewed for completeness. Incomplete submissions are returned to the Applicant who has fifteen (15) business days to re-submit the form.

The Lab Director reviews the submission and researches the facts of the non-conformance result. This review includes thoroughly examining all documentation in the Applicant's case file and interviewing the Lab Team Lead and the Technical Evaluation Team that were originally assigned to the Applicant.

The Lab Director then discusses the submission and findings with the Applicant. If the disagreement is resolved during this discussion, the Lab Director documents that result. The Lab Director issues a formal letter of resolution to the Applicant and all necessary updates to the product or service evaluation status will be made at this time.

7 Optimization Phase

The optimization phase creates a living and continuously evolving testing program. The major input for this phase is industry and agency feedback gathered at defined time periods. This feedback should help GSA evaluate and analyze strengths and suggest “areas of improvement” of the Program, and to incorporate changes that may make the Program more efficient or more responsive to stakeholders and customers.

7.1 Program Review

A core component for optimizing the Program is a periodic program review. The Program review is a meeting held by GSA OGP leadership to evaluate the Program as a whole and to determine what is working well and where there are opportunities for improvement. The findings of this review would inform the modifications that are made to the design process of the testing capability. The Program review would minimally include the following areas:

- **Testing scope.** Ensure the Program is testing the appropriate capabilities, functions, products, and services, and if there are new areas or tests that need to be included in the Program.
- **Testing types.** Ensure the different testing types (e.g., conformance, functional, interoperability) are being applied appropriately to the products and services, and that the testing being performed is adequate (i.e., identify areas where testing is being done that is not necessary or more testing is necessary).
- **Evaluation modes.** Ensure the methods for evaluating vendor products and services include the appropriate level of rigor and if there are items that would be better addressed by a different evaluation mode (i.e., an item that currently needs to be verified could be evaluated by vendor testing instead).
- **Testing process.** Ensure that the testing process is working efficiently and meeting the needs of the program and identify opportunities to streamline or automate processes and procedures.
- **Approval results.** Ensure that the APL and associated materials are effective in supplying relevant information for implementers and that they are successful in supporting the decision of which products and services to employ in their programs.
- **Lab performance.** Ensure that the current Labs are meeting expectations and maintaining a high level of quality and performance in both their staff and tools and that the number of Labs supporting the Program is sufficient.

7.2 Stakeholder Feedback

In addition to conducting an internal review of the Program, obtaining feedback from stakeholders is key to successful Program optimization. Receiving comments, questions, and concerns will allow GSA OGP leadership to identify the aspects of the Program that are successful and the areas that could use some additional attention. Stakeholder feedback would be used in the Program review to improve upon the design process and the Program.

Program stakeholders are some of the primary players in the testing process and therefore have first-hand knowledge about gaps, inefficiencies and opportunities for improvement. Program stakeholders include:

- **Agencies.** Use the APL to inform purchasing decisions and will be able to comment on the usefulness and user-friendliness of the APL in a production environment.
- **Industry.** Uses the testing process to get their products and services approved and will be able to provide feedback around improvements to the application and testing process and the requirements as well as the relative ease of working with particular Labs.
- **Labs.** Execute the testing process, work with the vendors and will be able to provide insights around the level of awareness vendors have of the testing process, the usability and gaps of the testing procedures and tools, and Lab environment requirements.

Table 7 provides an overview of the different ways GSA OGP leadership could capture both formal and informal feedback from its stakeholders.

Feedback Mechanism	Description
Open Meeting	An annual session where stakeholders across the program could attend and discuss their questions and concerns.
Email Communications	A mechanism on the APL site for collecting communications via email. This would allow those who interact with the APL to provide their input.
Lab Escalation	An established process for the Labs to communicate frequently asked questions or commonly received feedback for review by GSA OGP leadership.
ICAM Subcommittee (ICAMSC)	Aggregated comments provided by implementers to the ICAMSC and its working groups for review by GSA OGP leadership.

Table 7: Stakeholder Feedback Mechanisms

7.3 Special Review Team

Program issues may arise from time to time. Examples of issues include but are not limited to an ambiguous or unclear test requirement (which could result in a Lab or vendor incorrectly interpreting the requirement), and the need to improve testing methods. At the sole discretion of the Program Manager, a review team may be convened to analyze the issues presented and to determine the appropriate course of action (e.g., further research, seek external input, revise existing test requirements). The Program Manager is the final approval authority for all review actions and decisions.

Appendix A Acronym List

Acronym	Description
APL	Approved Products List
CTL	Certified Testing Laboratory
EP	Evaluation Program
EPD	Evaluation Program Development
FAC	Federal Acquisition Circular
FAR	Federal Acquisition Regulation
FICAM	Federal Identity, Credential & Access Management
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
ISO	International Organization for Standardization
LACS	Logical Access Control Systems
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
NPIVP	Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OGP	Office of Government-wide Policy
OMB	Office of Management and Budget
PACS	Physical Access Control Systems
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comment
RTM	Requirements Traceability Matrix
SP	Special Publication
TFS	Trust Framework Solutions

Appendix B References

- [APL] *FIPS 201 Evaluation Program Approved Products List (APL), General Services Administration.*
<http://fips201ep.cio.gov/>
- [Credentialing Memo] *Office of Management and Budget (OMB) Memorandum date October 6, 2011; Requirements for Accepting Externally-Issued Identity Credentials*
http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/ombreqfora_cceptingexternally_issuedidcred10-6-2011.pdf
- [FAC 2005-19] *Federal Acquisition Circular 2005-19 Sub part 4.13*
http://www.acquisition.gov/far/fac/FAC_2005-19_Looseleaf_pgs.pdf
- [FAR Case 2005-017] *Federal Acquisition Regulation; FAR Case 2005-017; Requirement to Purchase Approved Authentication Products and Services*
<https://www.federalregister.gov/articles/2006/08/23/06-7088/federal-acquisition-regulation-far-case-2005-017-requirement-to-purchase-approved-authentication>
- [FICAM Roadmap] *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*
http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf
- [HSPD-12] *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, White House, August 2004.*
<http://www.dhs.gov/homeland-security-presidential-directive-12>
- [FIPS 201] *FIPS 201, Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.*
<http://csrc.nist.gov/publications/PubsFIPS.html>
- [Lab ConOps] *FIPS 201 Evaluation Program Development Laboratory Concept of Operation; Version 1.0.0; February 2006*
<http://fips201ep.cio.gov/documents/FIPS201epdCONOPS.pdf>
- [Lab Spec] *GSA FIPS 201 Evaluation Program Laboratory Specification, Version 7.0.0, GSA, May 2010.*
http://fips201ep.cio.gov/documents/Lab_Specification_v7.0.0.pdf
- [NVLAP HB 150] *National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150, Procedures and General Requirements, February 2006.*
<http://www.nist.gov/nvlap/upload/nist-handbook-150.pdf>

- [NVLAP HB 150-17] *National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150-17, Cryptographic and Security Testing, March 2012*
<http://www.nist.gov/nvlap/upload/NIST-HB-150-17-2012.pdf>
- [NISTSP 800-53] *National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for federal Information Systems and Organizations; April 2013.*
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- [OMB M-05-24] *Office of Management and Budget (OMB) Memorandum (M)-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005*
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>
- [OMB M-06-18] *Office of Management and Budget (OMB) Memorandum (M)-06-18, Acquisition of Products and Services for implementation of HSPD-12, June 2006*
<http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2006/m06-18.pdf>
- [OMB M-11-11] *Office of Management and Budget (OMB) Memorandum (M)-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011*
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>