Federal Identity, Credential, and Access Management (FICAM) Testing Program Concept of Operations

Final Draft

July 23, 2012

This page is intentionally left blank.

Table of Contents

This page is intentionally left blank.

List of Figures

This page is intentionally left blank.

1 Introduction

1.1 Background

The General Services Administration (GSA) has the responsibility of supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) Publication 201[1] Approved Products List (APL)[2] Evaluation Program (EP), as well as services for Federal ICAM (FICAM) conformance and compliance. Currently, there is a shortfall between the ICAM business processes and the intended vision of a government-wide ICAM conformance and standards interoperability capability.

Additionally, the landscape for ICAM is changing. Several policy drivers (i.e., Homeland Security Presidential Directive 12 [HSPD-12],[3] Office of Management and Budget [OMB] Policy Memorandum 11-11 [M-11-11],[4] OMB Memorandum 06-24 [M-06-24],[5] and the FICAM Roadmap and Implementation Guidance[6] [FICAM Roadmap]) have required federal agencies to upgrade their ICAM technologies to support new functionality and needs (e.g., modernizing Physical Access Control Systems [PACS] to use Personal Identity Verification [PIV] credentials). 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 access control systems.

There is a clear need to develop the FICAM Testing Program to encompass the broader needs of agencies striving to architect and implement HSPD-12 solutions and develop ICAM systems that are secure, interoperable, and compliant with the FICAM Roadmap.

1.2 Purpose

The purpose of the FICAM Testing Program Concept of Operations is to describe the overarching framework used to support the GSA FICAM Testing Program. It is intended to capture and expand upon the existing FIPS 201 EP and incorporate testing related to the ICAM Trust Framework Solutions to create an updated FICAM Testing Program.

---

[1] FIPS 201, Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. [FIPS 201]

[2] FIPS 201 Evaluation Program Approved Products List (APL), General Services Administration. [APL]

[3] Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, White House, August 2004. [HSPD-12]

[4] Continued Implementation of Homeland Security Presidential Directive (HSPD) -12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

[5] Acquisition of Products and Services for Implementation of HSPD-12, OMB, June 30, 2006. [M-06-18]

[6] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, Federal Chief Information Officers Council, December 2, 2011. [FICAM Roadmap]

1.3 Scope

The scope of the Federal Identity, Credential, and Access Management (FICAM) Testing Program Concept of Operations is limited to testing of requirements found in FIPS 201 Conformance and the FICAM Roadmap. The following areas are not in the scope of the FICAM Testing Concept of Operations:

- GSA Federal Acquisition Schedule 70 Special Item Number (SIN) 132-51, SIN 132-60A-F, SIN 132-61, SIN 132-62, and Schedule 84 SIN 246-35 1-2
- Approved Service Providers and products on the current APL are outside of the scope of this document.

1.4 Assumptions and Dependencies

The updated FICAM Testing Program will take into consideration the following assumptions and dependencies:

- GSA will manage the FICAM Testing Program and will be responsible for formalizing and maintaining the test design, test evaluation, test approval, and program optimization processes and procedures.
- GSA will revise the current testing approach to meet the new FICAM Testing framework outlined in this document
- GSA will work collaboratively with the National Institute of Standards and Technology (NIST), Certified Testing Laboratories (CTLs), and Industry to ensure the FICAM Testing Program is updated to incorporate requirements from relevant technical and policy documentation (e.g., FIPS 201, FICAM Roadmap), as appropriate,
- GSA will work with FICAM Testing Program stakeholders to further define and assign the roles and responsibilities necessary to execute the ConOps.
- GSA will collaborate with CTLs on test requirements development, test development, and test execution for the FICAM Testing Program.
- FICAM Roadmap Testing (Section2.2.2) needs to be further defined with stakeholders to develop test requirements, testing procedures, use cases, and types of testing appropriate for the products and services being tested.
- GSA will determine the appropriate evaluation mode for products and services to meet the requirements of the FICAM Testing Program.
- This document is a living document and stakeholder feedback will continue to drive future revisions of the FICAM Testing Program.

1.5 References

The following documents where leveraged to support development of this document:

- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance[7] [FICAM Roadmap]
- Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, White House, August 2004.[8] [HSPD-12]

[7] FICAM Roadmap.

- FIPS 201, Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.[9] [FIPS 201]
- FIPS 201 Evaluation Program Approved Products List (APL),[10] General Services Administration. [APL]
- FIPS 201 Evaluation Program Development, Laboratory Concept of Operations, Version 1.0.0,[11] February 13, 2006 [FIPS 201 LAB CONOPS]
- FIPS 201 Evaluation Program Laboratory Specification, Version 7.0.0,[12] GSA, May 2010.
- National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150, Procedures and General Requirements, February 2006.[13] [NIST NVLAP HB-150]
- National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150-17, Cryptographic and Security Testing, March 2012[14] [NIST NVLAP HB-150-17]
- 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[15] [OMB M-05-24]
- 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[16] [OMB M-11-11]

---

[8] HSPD-12

[9] FIPS 201

[10] FIPS 201 APL

[11] FIPS 201 Evaluation Program Development, Laboratory Concept of Operations, Version 1.0.0,February 13, 2006 [FIPS 201 LAB CONOPS]

[12] FIPS 201 Evaluation Program Laboratory Specification, Version 7.0.0

[13] National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150, Procedures and General Requirements, February 2006[13] [NIST NVLAP HB-150]

[14] National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook (HB) 150-17, Cryptographic and Security Testing, March 2012. [NIST NVLAP HB-150-17].

[15] 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 [OMB M-05-24]

[16] 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 [OMB M-11-11]

2 FICAM Testing Program Overview

GSA has responsibility both over the Federal ICAM initiative as well as 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. Historically, this capability has been focused on the FIPS 201 program through the authority assigned in OMB M-05-24. Now that the scope of the FICAM testing program is expanding, the conceptualization of the program will be revisited and broadened. This section outlines the goals and objectives for the program and discusses the main elements of the program, including the existing FIPS 201 evaluation and broader testing to support technical interoperability and Trust Framework Solutions testing.

The vision of the FICAM testing program 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.

2.1 Goals and Objectives

The primary goals and objectives of the FICAM testing program are:

- To provide a common government-wide testing capability for ICAM products and services;
- To provide compliance, consistency and alignment of commercially available products and services with the requirements and functional needs of government ICAM implementers;
- To ensure availability and choice among vendor products to support different ICAM components;
- To coordinate interaction and coordination with the ICAM vendor community to improve the inclusion of ICAM requirements into product offerings; and
- To promote cost effective ICAM implementation through qualification of products and services that have been demonstrated to perform successfully.

2.2 Elements of Testing

The elements of testing under the current EP will expand to cover a comprehensive set of policies and technologies that are critical to the implementation of the target-state architecture. The updated FICAM Testing Program is organized into two primary testing capabilities: HSPD-12 and FICAM Roadmap. These capabilities are comprised of different components related to ICAM-specific technologies and solutions. These test elements are described in detail in the following sections and are depicted in the hierarchal graphic below.

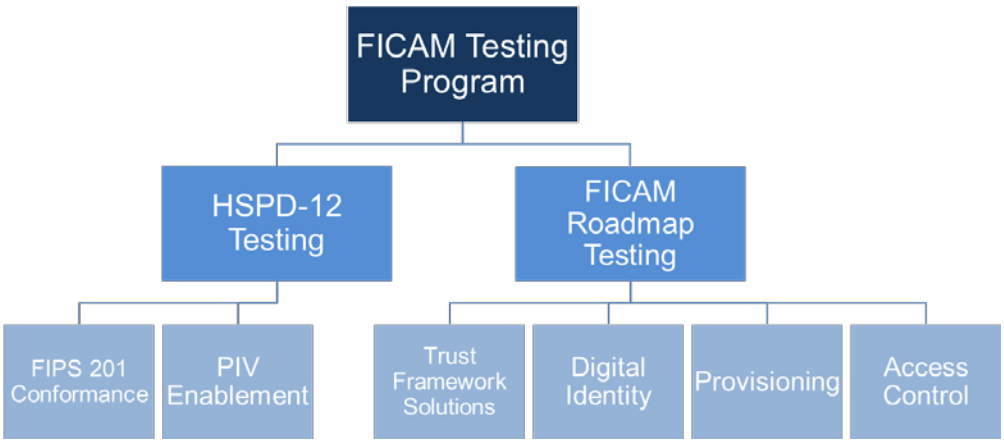

Figure 1: FICAM Testing Program Testing Hierarchy

2.2.1 HSPD-12 Testing

OMB M 11-11 decrees that agencies implement required use of the PIV credentials for physical and logical access to federal facilities and networks, respectively. To implement HSPD-12 and OMB M-11-11, agencies must upgrade their physical and logical access systems to use PIV credentials and to PIV-enable new access systems prior to implementation and operation. HSPD-12 testing will group the existing FIPS 201 Conformance testing activities (Section2.2.1.1) with the broader interoperability and end-to-end functionality testing discussed in PIV Enablement (Section 2.2.1.2).

2.2.1.1 FIPS 201 Conformance

Currently, the FIPS 201APL is the primary tool for determining the conformance of products and services for HSPD-12 needs. The scope of FIPS 201 testing is limited to product categories with explicit requirements identified in FIPS 201 and the supporting NIST Special Publications (i.e., SP 800-73-1, SP 800-76-1, SP 800-78, SP 800-85A, and SP 800-85B). It does not define specific requirements for usage applications of the PIV card, such as logical and physical access, and in particular, does not take into account for the testing needed to verify compatibility and interoperability. As a result, agencies face a challenge with identifying and procuring products and services to modernize their ICAM infrastructure. This document seeks to close that gap and offers a framework under which ICAM products and services can be tested to determine suitability for use in agency ICAM implementations.

2.2.1.2 PIV Enablement

As the government-wide push to align with FICAM continues, there is a need to develop testing around HSPD-12 systems conformance and interoperability, focusing on logical and physical access and alignment with the ICAM segment architecture. To ensure proper usage of PIV cards, interoperability and HSPD-12 compliance testing should be performed on both logical access control systems (LACS) and physical access control systems (PACS). As usage of the PIV Card continues to be extended to physical and logical access and as the process of federation is adopted more frequently across the government, testing will need to be updated to ensure compliance with FICAM.

2.2.2 FICAM Roadmap Testing

FICAM Roadmap testing will cover areas that enable agencies to implement systems and solutions to help them align with the FICAM Roadmap and Implementation Guidance and to meet the objectives of the ICAM target-state architecture. These areas include Trust Framework Solutions, Digital Identity Data Collection and Attribute Solutions, Provisioning, and Access Control and are described in the following sections.

2.2.2.1 Trust Framework Solutions

The ICAM Trust Framework was created and adopted to support E-Government activities and for agencies to interact with the public through logical means at the first, second, and non-Public Key Infrastructure (PKI) third levels of assurance (LOA 1, LOA 2, non-PKI LOA 3). The goals and objectives of Trust Framework Solutions testing are to test for the level of trust and interoperability for PKI and non-PKI credentials and for inclusion of these services under the revamped EP.

2.2.2.2 Digital Identity Data Collection and Attribute Solutions

As part of agency efforts to align with FICAM Initiative 5 (Streamline Collection and Sharing of Digital Identity Data), solutions are required to eliminate redundancies in the collection and maintenance of identity data and mitigate the inefficiencies and security and privacy risks associated with current identity data management processes. There are several solutions that deal with the variety of activities under the digital identity data and attribute umbrella including: managing digital identity at the enterprise level, authoritative data source identification, and attribute exchange. Testing for digital identity data collection and attribute solutions will examine how specific solutions, such as the Authoritative Attribute Exchange Service (AAES) or Back-End Attribute Exchange (BAE), collect digital identity data and share attributes.

2.2.2.3 Provisioning

Currently, automated provisioning capabilities that are integrated with PACS and LACS solutions typically provision user identity data for the purpose of establishing a user account, while entitlement privileges (e.g., access to specific sites or doors) are managed and controlled within the PACS and LACS solution itself. In the ICAM target state, however, agencies should develop automated provisioning capabilities that enable the provisioning of desired baseline physical and logical access privileges (e.g., access to building common areas for all agency cardholders or default access to an agency application) as part of the initial account creation process. The goals and objectives of Provisioning testing are to test the automated provisioning capabilities of provisioning solutions for compliance with the FICAM Roadmap.

2.2.2.4 Access Control

As agencies move toward enterprise approaches to access control in the ICAM target state, many ICAM implementers are looking for more flexible, granular approaches for managing access. Several additional access control models are available that automate access based upon user attributes and contextual resource information, including Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Risk-Adaptable Access Control (RAdAC). The goals and objectives of Access Control testing are to test the access control solutions for compliance with the FICAM Roadmap.

3 Test Framework

As GSA revises and transforms the current FIPS 201 EP, the need has arisen to incorporate a holistic perspective which encompasses the broader FICAM environment. The objective of the FICAM Testing Program is to provide federal agencies a list of approved products and services to assist with ICAM implementation. The updated FICAM Testing Program should be viewed as a continuously improving process with the ability to adapt to new products developed by vendors. Providing a feedback loop for vendors, who undergo the evaluation program, and agencies, who are the end customers of the APL, will help GSA achieve a high level of active maintenance and improvement of the entire FICAM Testing Program. As ICAM evolves, new product categories and test procedures are introduced and incorporated into the evaluation program. This will allow GSA to meet the needs and challenges of its customers and stakeholders as requirements and technology evolve.

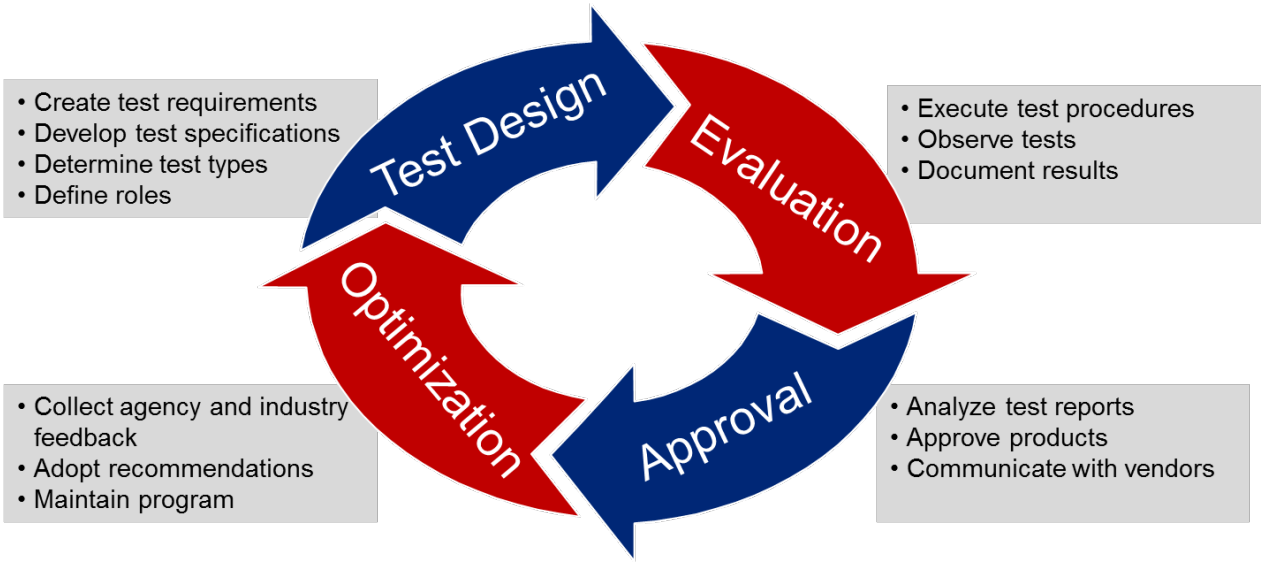

Figure 2: FICAM Testing Framework

The framework for FICAM testing is a four-phase cyclical process that possesses 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 FICAM 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 testing program. Test processes and procedures will be developed by leveraging existing and creating new requirements from federal standards, policy, and guidelines.
- **Evaluation.** Once the objectives are defined and established, the processes and procedures can be executed. In evaluation, the testing artifacts developed in test design are used to evaluate products/services. The test results will indicate whether a product or service is conformant with FIPS 201 and/or FICAM.
- **Approval.** Observations made during the evaluation phase will be analyzed and a decision will be made to approve the product/service.
- **Optimization.** GSA will gather input from vendors, agencies, and test labs to maximize the efficiency and keep the FICAM Testing Program current. A continuously improving

program will enhance GSA's ability to serve its customers at both ends of the program 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. Actions from the feedback in the optimization phase are executed and incorporated back into the test design phase.

4 Test Design

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 execute 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. For the GSA FICAM Testing Program, test requirements will be collected from known and trusted sources, including:

- FIPS 201 and associated NIST Special Publications
- FICAM Roadmap and Implementation Guidance
- Agency-specific requests
- Results from testing feedback processes

Where new requirements need to be isolated and developed, it is expected that this process would include an integrated team within the GSA FICAM Testing Program that bring points of view from system functionality, product knowledge, and includes developers and testers.

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 testing labs 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 Section 4.3 for more details).

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

Test Specification Output	Description
Test Procedures	Standardized, executable instructions for testing requirements.
Approval Procedures	Standardized process for analyzing test evaluation 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.

Figure 3: GSA FICAM Test Specification Components

4.3 Testing Types

A sub-element of the test specification development is 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 and Trust Framework Solutions.

The types of testing that will be performed under the FICAM Testing 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 and the Trust Framework Solution. 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 stakeholders of the FICAM Testing Program will be the customers, approval authority, applicants, certified testing lab staff, and the approving authority. The roles may, and in some cases are required to, be filled by more than one individual.

- **Approval Authority.** The Approval Authority is established by GSA Office of Governmentwide Policy (OGP) and is responsible for reviewing final test reports, approving or rejecting products and services for the FIPS 201 APL, and communicating approval decisions with the Applicant in conjunction with the Certified Testing Labs. 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 FICAM Testing Program website.
- **Applicant.** The Applicant submits a product or service to Certified Testing Laboratories (CTL) 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 FICAM Testing Program website or contact the FICAM Testing Program Approval Authority for questions and detailed information on the importance of the FICAM Testing 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, or components on the APL and have passed security testing according industry standards.
- **Certified Test Lab Staff.** The Certified Test Laboratories are responsible for the overall operation of the lab, product evaluation and evaluation oversight, quality assurance, and managing relationships with the applicants and the approval authority. The Certified Testing Laboratories must be compliant with GSA FIPS 201 Laboratory Specification Version 7.0.0 and the FIPS 201 Evaluation Program Development Laboratory Concept of Operations, which specify the minimum number of staff required for a Certified Testing Lab.
- **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 Evaluation

The evaluation phase is where the testing execution is performed. Inputs to this phase include the test procedures which will test products and services against the requirements developed in the test design phase. The output from this phase is the test/evaluation report which includes in detail the 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 Approved Products List. Section 5 (Evaluation) provides a more detailed overview and explanation of the evaluation phase.

5.1 Testing Process

The testing process occurs in four phases, which are detailed below. The main method of communication between all primary actors (i.e., Applicants, Labs, and the 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 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.

- **Application submission.** The applicant submits a complete application package (see section 4.3 for more information) to the CTL. 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. If the application is incomplete, the application is returned to the Applicant.
- **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.
- **Reporting.** The CTL summarizes the evaluation process and submits a Final Test Report. If the Final Test Report indicates a product or service passed the testing, the report is sent to the Approval Authority. If the Final 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.
- **Approval.** If a product or service has passed the evaluation testing, then the Approval Authority will write a letter of approval for the Applicant and send the letter to the CTL which conducted the testing. The CTL notifies the Applicant by sending the approval letter and adds the product or service to the APL.

The following figure graphically represents the testing process.

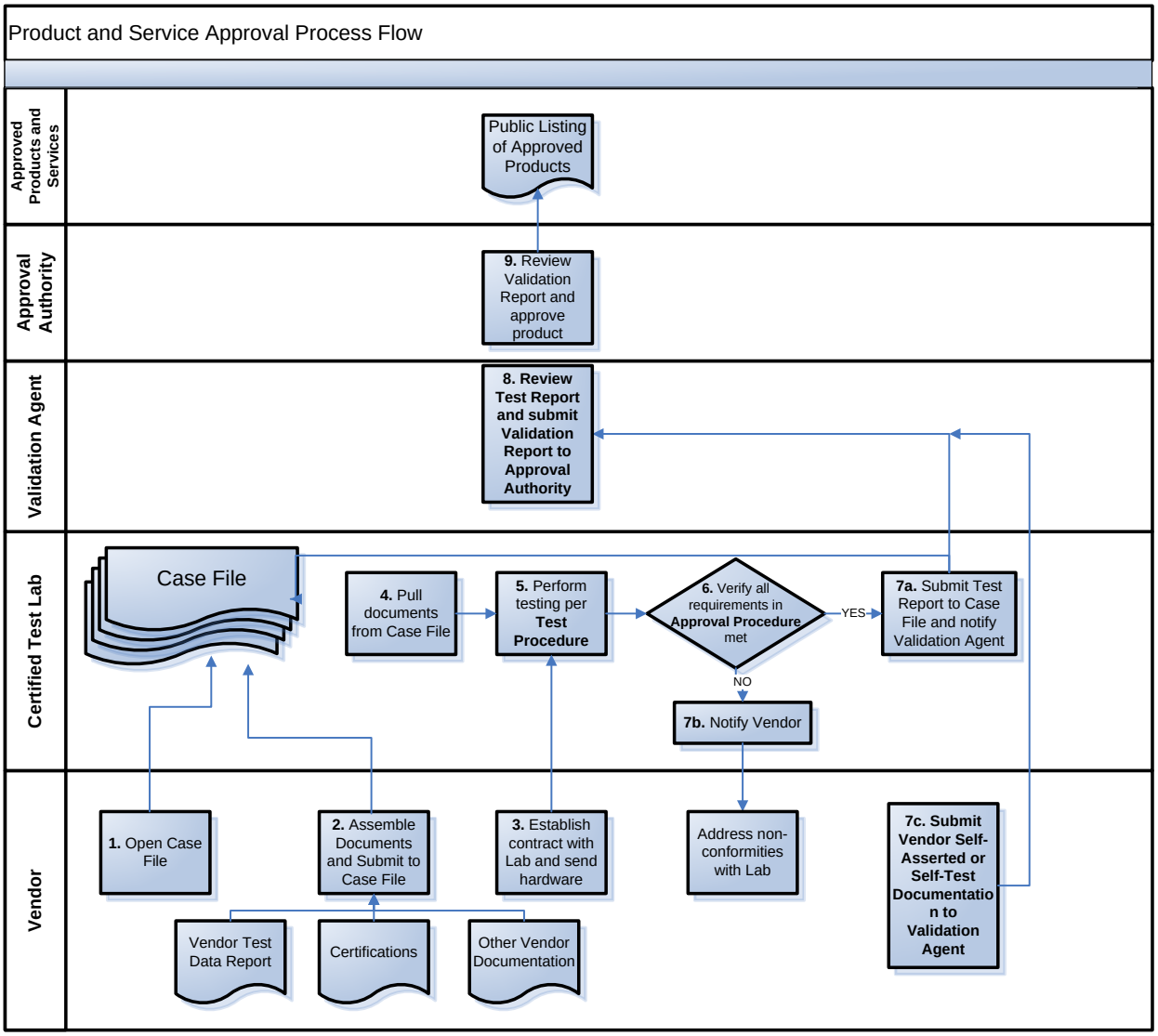

Figure 4: FICAM Testing Program Approval Process Flow

5.2 Evaluation Modes

There are several methods for evaluating vendor products: 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 vendors to provide documentation packages stating how their product passes a test for conformance and interoperability with FICAM requirements. This package may include a summary of functionality and implementation approaches for meeting the FICAM requirements and the basis for stating compliance. Additionally, the documentation package may include product test evaluation results from evaluation or testing entities

independent of FICAM Testing Program CTLs. Depending on the product test evaluation results, GSA would have the discretion to accept the results without requiring the product to undergo repetitive testing under the FICAM Testing Program. Testers will in turn inspect the product 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
• Low level of effort for GSA • Provides references to existing published documentation, such as certifications, to reduce testing redundancy	• Accuracy relies on vendor claims about their own product

Figure 5: Benefits and Limitations of Vendor Assertion Testing

5.2.2 Vendor Self-testing

Vendor self-testing enables product vendors to execute GSA- 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 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 for evaluation. For example, a vendor may self-test pre-requisite requirements before submitting for independent testing.

Benefits	Limitations
• Low level of effort for GSA • Enables vendor to perform integration of their own product • Enables vendor to perform initial testing of low risk requirements and resolve issues during product development	• 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 • Accuracy relies on vendor expertise with FICAM testing

Figure 6: 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 the GSA and NIST specifications. This method of evaluation may be appropriate for tests that are medium priority to GSA and products that are too large to transport or are integrated systems.

Benefits	Limitations
• Low level of effort for GSA • Enables vendor to perform integration of their own product	• Requires vendors to have the tools and data necessary to execute the test procedures • Requires travel for testers of certified labs

Benefits	Limitations
• Enables independent oversight of testing activities and results • Provides technical expertise in executing the tests and analyzing the results	• Test results may be specific to vendor configuration • Test environment may not be controlled

Figure 7: Benefits and Limitations of Witness Testing

5.2.4 Independent Verification

Independent verification enables testers to integrate and test vendor products in a CTL. The testers will follow vendor documentation to install and configure the product for testing and then execute the GSA- 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
• 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	• High level of effort for GSA • Requires testers to determine how to integrate and configure vendor products

Figure 8: Benefits and Limitations of Independent Verification

6 Approval

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 Approved Product List. Historically, the approval phase has only been performed within the realm of FIPS 201 testing. The resulting approval decision was the placement of a product or service on the FIPS 201 APL, which agencies are required to use when purchasing products and services when implementing HSPD-12. In the broader framework for the FICAM Testing Program, the approval process needs to be expanded to encompass the new testing areas referenced in Section 2 and to reflect a more diverse set of possible test results. Simple placement on the APL is no longer sufficient to meet the broader testing and usage needs by agency ICAM implementers. The existing APL will either need to be expanded or additional approval lists or results will need to be communicated to agency customers that capture the types of testing and requirements used to qualify a particular product or service.

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 GSA's Validation Agent, which is the point of exit for the evaluation phase (see Section 5). The following figure illustrates the key steps in the approval process.

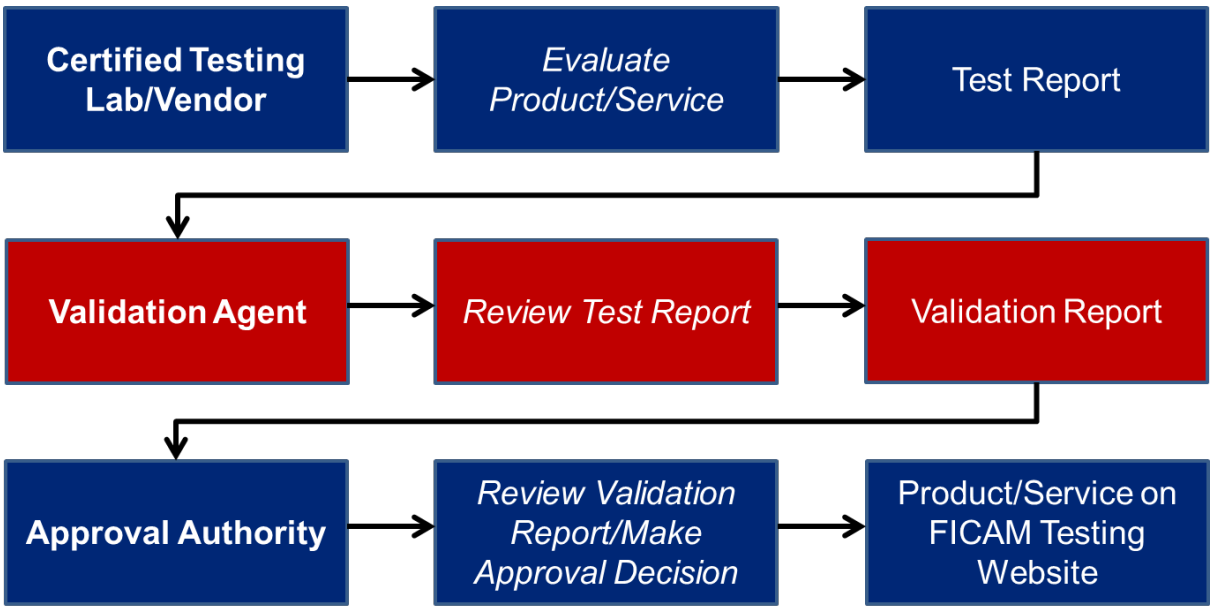

Figure 9: FICAM Testing Approval Process

The following steps detail the approval process:

1. The CTL or the Vendor 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 FICAM Testing Program webpage.

The approval process detailed above expands the existing FIPS 201 EP approval process to address the changing scope and objective of the FICAM Testing Program. The envisioned target approval process provides greater details around the testing being conducted and for the results to provide more meaningful information to the users and customers. 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. The following table lists in detail 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.

Figure 10: GSA ICAM Testing Approval Documentation

The information captured and distributed via the approval documentation achieves the objective of the GSA FICAM Testing Program 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.

7 Optimization

Optimization is a new phase which has been added to the FICAM testing process in order to create 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 to evaluate and analyze the strengths and development areas of the FICAM Testing Program and to incorporate any changes that may make the program more efficient or more responsive to stakeholders and customers. This section provides a more detailed overview and explanation of the optimization phase.

7.1 Program Review

A core component for optimizing the FICAM Testing Program is a periodic program review. The program review is a meeting held by the GSA OGP leadership to evaluate the program as a whole and 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, etc.) are being applied appropriately to the products and services and that the testing being performed is adequate (i.e., if there are areas where testing is being done that is not necessary or more testing is necessary).
- **Evaluation modes.** Ensure the methods for evaluating vendor products 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 the GSA OGP leadership to identify the aspects of the program that are successful and the areas that could use some additional attention. The feedback provided by the stakeholders would be used in the program review to improve upon the design process and the testing program.

The stakeholders for the program are some of the primary players in the testing process and as such, have first-hand knowledge about gaps, inefficiencies and opportunities for improvement. The stakeholders for the testing program 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.

The following table provides an overview of the different ways the 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.

Figure 11: Stakeholder Feedback Mechanisms

Appendix A Acronym List

Acronym	Description
AAES	Authoritative Attribute Exchange Service
ABAC	Attribute-Based Access Control
APL	Approved Products List
BAE	Back-end Attribute Exchange
CTL	Certified Testing Laboratory
EP	Evaluation Program
FICAM	Federal Identity, Credential & Access Management
FIPS 201	Federal Information Processing Standard Publication 201
GSA	General Services Administration
HB	Handbook
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity, Credential & Access Management
ICAMSC	Identity, Credential and Access Management Subcommittee
LACS	Logical Access Control Systems
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OGP	Office of Governmentwide Policy
OMB	Office of Management and Budget
PACS	Physical Access Control Systems
PBAC	Policy-Based Access Control
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RAdAC	Risk-Adaptable Access Control
RBAC	Role-Based Access Control
RTM	Requirements Traceability Matrix
SP	Special Publication