Approved PACS Topology Mapping Document (PACS 13.01)

VERSION 1.3.3 Rev. G

FIPS 201 EVALUATION PROGRAM

February 1, 2019

FINAL

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
First draft	0.0.1	2/6/2014	Mapping for PACS 13.01	Limited
Draft	0.0.2	2/14/2014	Initial edit	Limited
Draft	0.0.3	2/18/2014	Updated definitions, diagrams	Limited
Draft	0.0.4	2/19/2014	Team edits	Limited
Draft	0.0.5	2/20/2014	Team edits	Limited
Draft	0.0.6	2/22/2014	Cleaned up table inconsistencies	Limited
Draft	0.1.0	5/16/2014	Cleaned up grammatical errors.	Public
Draft	0.1.1	7/8/2014	Revised category descriptions and Topology illustration to make it clearer that the configurations are examples, and that other approaches are acceptable. Changed Program name back to FIPS 201 Evaluation Program.	Public
Final	1.3.0	3/2/2015	Revised to be in synch with FRTC v1.3.0	Public
Final	1.3.3	9/8/2017	• Revised to synch with PACS FRTC v1.3.3. • Updated links to online normative references. • Added security classifications, severity level definitions, APL listing requirements. • Reactivated 12 previously deprecated test cases, clarified 16, added 58, and deprecated 14 test cases. • Biometric verification of cardholder is required at time of registration. Security Object verification is mandatory at time of registration.	Public
Final	1.3.3 Rev A	9/18/2017	• Corrected typos. • Re-ordered and renumbered test certificate policy and interoperability test cases so that the same card can be used for multiple tests before switching to the next card. • Added one (1) missing certificate policy test case for PIV Authentication at time of access.	Public
Final	1.3.3 Rev B	11/3/2017	• Updated normative policy references for Federal Common Policy, FBCA, SSP, and PIV-I. • Updated Discovery Object tests to reflect that max retries of test cards are set to 10, not 5. • Added ICAM Test Card 54 (NFI PIV-I).	Public

Status	Version	Date	Comment	Audience
Final	1.3.3 Rev C	1/7/2018	• Replaced all instances of the use of ICAM Test Card #01 with ICAM Test Card 46. • Replaced all instances of the use of ICAM Test Card #02 with ICAM Test Card 54. • Corrected expected Global PIN retry counter, Test Cases 2.18.02 and 5.17.02. • Added ICAM Test Card 55 (Missing Security Object) and Test Case 2.14.03. • Clarified the expected result of Test Cases 2.16.02 and 5.15.02.	Public
Final	1.3.3 Rev. D	4/24/2018	• Deprecated Test Cases 2.06.03, 2.06.04, 5.06.03., 5.06.04, and 5.11.01. (and removed Section 5.11). • For time-of-access fault path testing, included instructions as to which golden card must be registered with the PACS. • Activated ICAM Test Card 48 (PPS with LEN value greater than zero). • Corrected bit ordering of last 5 digits of example FASC-N in Credential Identifier Processing in Section 5. • Corrected card type from Card Authentication Certificate to PIV Authentication Certificate in Test Cases 2.06.07 and 5.06.07. • Added "Valid/Invalid" column to card description table. • Verified and updated links to normative references. • Clarified card type (PIV/PIV-I) for test cases 7.05.01 and 7.05.02	Public
Final	1.3.3 Rev. E	6/21/2018	• Deprecated Test Case 5.12.02 • Clarified that Card 7 must be personalized with the tester's biometric. • Removed Fault Paths 37-40 • Deprecated Test Cases 8.01.01-8.10.04 (Handheld)	Public
Final	1.3.3 Rev. F	8/21/2018	• Deprecated Test Cases 2.17.14 and 5.16.14 because RSA 4096 was deprecated by FIPS 186-3 and subsequently SP 800-78-2. • Changed wording of Test Case 5.02.03 to "With ICAM Test Card 46 registered with the PACS, verify product’s ability to reject a credential when notAfter date of any certificate in the path is sometime in the past." • Deprecated Test Case 5.02.05 because Test Case 5.02.03 was updated to include all certificates in the path.	Public

Status	Version	Date	Comment	Audience
			• Added Test Cases 2.10.8 and 2.10.9 because Paths 3 and 16 can be used to test them.	
Final	1.3.3 Rev. G	2/1//2019	• Changed 5.15.04 to "With ICAM Test Card 46" • Deprecated Test Cases 2.04.05 and 5.04.05 (requires SKID to consist of SHA-1 of public key). Going forward, PACS should not enforce this rule. • Replaced "CHUID signature" with Card Authentication" in the description for Test Case 5.06.13. We are testing for a Card Authentication certificate policy OID. • The description for Test Case 5.15.04 was changed to, "With ICAM Test Card 46...". • Added Test Cards 57, 58, and 59 and Test Cases 2.09.11, 2.10.10, 5.09.11, and 5.10.1 • Changed Test Case 5.12.05 to " With ICAM Test Card 59 registered..." • Added Sections **Error! Reference source not found.** Testing Criteria, **Error! Reference source not found.** Severity Levels.	Public

Table of Contents

1 Background

The General Services Administration (GSA) is responsible for 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) 201 Evaluation Program and its associated Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance.

2 Objectives

The FIPS 201 Evaluation Program's PACS evaluation process is designed to be agnostic to architecture and focuses solely on functional testing using an end-to-end testing methodology. This document facilitates applicant mapping of the functional requirements identified in *Functional Requirements and Test Cases* [FRTC] to the categories identified in the FIPS 201 Evaluation Program's PACS 13.01 topology.

3 Normative References

[BAA] Buy American Act Certification FAR 52.225-2
https://www.law.cornell.edu/cfr/text/48/52.225-2

Common] FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 1.27, June 29, 2017, or as amended
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

[E-PACS] FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), Version 3.0 March 26, 2014
https://www.idmanagement.gov/docs/pacs-piv-epacs.pdf

[FBCA] FBCA X.509 Certificate Policy for Federal Bridge Certification Authority (FBCA), Version 2.31 June 29, 2017, or as amended
https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf

[FIPS 201] Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[FRTC] FIPS 201 Evaluation Program Functional Requirements and Test Cases
https://www.idmanagement.gov/docs/pacsapp-frtcworkbook.xlsx

[HSPD-12] Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

[M-05-24] Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2005/m05-24.pdf

[M-06-18] Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2006/m06-18.pdf

[M-11-11] OMB Memorandum M-11-11, February 3, 2011
https://www.cac.mil/portals/53/documents/m-11-11.pdf

[PIV-I] CIO Council Personal Identity Verification Interoperability for Issuers, Version 2.0.1 July 27, 2017, or as amended
https://www.idmanagement.gov/docs/archived/fpki-pivi-for-issuers.pdf

[PROF] X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program, Version 1.8 June 17, 2017, or as amended
https://www.idmanagement.gov/docs/fpki-x509-cert-profile-common.pdf

[Roadmap] FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
https://www.idmanagement.gov/icamsolutions/

[Sect508] Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998
http://www.section508.gov/section508-laws

[SP800-73] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-73-4, Part 1-3, May 2015
http://dx.doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76-2, July 2013
https://csrc.nist.gov/pubs/sp/800/76/2/final

[SP800-78] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-78-4, May 2015
https://csrc.nist.gov/pubs/sp/800/78/4/final

[SP800-96] NIST SP 800-96, September 2006
http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[SP800-116] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://dx.doi.org/10.6028/NIST.SP.800-116

[SP800-153] NIST SP 800-153, February 2012
http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

[TAA] Trade Agreement Act Certification FAR 52.225-6
https://www.acquisition.gov/far/52.225-6

[UL 294] The Standard of Safety for Access Control System Units, UL Edition Number – 6, Date 05/10/2013, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_294_6

[UL 1076] The Standard of Safety for Proprietary Alarm Units, UL Edition Number – 5, Date 09/29/1995, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1076_5

[UL 1981] The Standard for Central-Station Automation Systems UL Edition Number - 3, Date 10/29/2014, Type ULSTD
https://standardscatalog.ul.com/standards/en/standard_1981_3

4 FIPS 201 Evaluation Program Defined Categories

The PACS 13.01 Topology defines three major categories (4.1 – 4.3 below). Each of these categories is defined as part of a whole PACS solution that can be tested end-to-end using the FRTC. Note that a category is not defined as a single object that is procured as a single SKU. The following definitions define the objects that make up a functional element called a category:

- ***Compatible*** components are proved to work with each other.
- ***Interoperable*** components are tested to determine the set of like and related components with which it can reliably be operated in combinations. Interoperable components must use an industry standard (e.g., ISO, ANSI, IETF RFC) to enable standardized interfaces between components.
- A ***subsystem*** is assembled of compatible components. Hence a subsystem would be tested and acquired as a unit or "configuration item". A subsystem may leverage an interoperable component external to the subsystem.
- A ***category*** is made up of subsystems, compatible and/or interoperable components that meet functional requirements defined in [FRTC].

The three categories defined by this topology are ***PACS Infrastructure, Validation System,*** and ***PIV Reader.*** They are further described in the following sections.

4.1 PACS Infrastructure Category

The PACS Infrastructure is made up of many compatible and interoperable components. Typical components may include:

- PACS application and server (also called the head-end);
- Database and server (often an integral part of the PACS application and server);
- Controllers (also called field panels or door controllers); and
- Workstations (for administration, registration of individuals, help desk, etc.).

Generally, PACS Infrastructure is made up of both software and hardware. PACS application software primarily runs on a physical server, virtual server, server cluster, or in some type of cloud-based architecture. The PACS Infrastructure runs in conjunction with field hardware that provides the door control, I/O, or alarm annunciation back to the PACS head end. Field Hardware can consist of I/O controllers, Alarm Controllers, Door Controllers, and Readers. Each Component performs a certain function and tied together creates a PACs. Some vendors might want to consolidate these components into a single component to increase performance or lower the overall foot print of the field panel, thereby lowering costs. But overall, the functions of PACS Infrastructure are still the same.

Other approaches that meet the functional requirements are also valid.

PACS Infrastructure is a very diverse environment that interoperates with many different subsystems that are outside the scope of the FIPS 201 Evaluation Program. These include:

- Intrusion Detection Systems (IDS);
- Video Management Systems (VMS);
- Visitor Management Systems (also called VMS);
- Enterprise Identity Management Systems (E-IdM); and
- Physical Security Information Management systems (PSIM).

These additional subsystems that are part of a total physical security program may become categories in a future spiral of the FIPS 201 Evaluation Program.

4.2 Validation System Category

A Validation System provides the necessary functions to perform identification and authentication of the bearer of a credential according to a FICAM Authentication Methods. These methods, and the controls necessary to implement them, are defined fully in E-PACS. A Validation System, as defined by the FIPS 201 Evaluation Program, is tightly integrated with the PACS Infrastructure and the PIV Reader. Typically, a Validation System is made up of several compatible and interoperable components that may include:

- SCVP server;
- OCSP responders;
- Caching status proxy server;
- Secure controllers (with or without caching capabilities);
- PKI validation software; and
- PKI registration and management software.

Validation Systems are generally made up of software and hardware. It can run on its own physical, virtual, clustered server, or cloud-based solution. It can run as an integrated solution with another vendor’s hardware such as a PACS vendor’s intelligent controller, or it can be a single proprietary solution of both software and field hardware. In some implementations, the field hardware is a secure controller that performs PKI validation (generally using cached information) and acts as an interface between the reader and the door controller. Any of these components could be integrated with other third-party components or in a completely virtual environment. Many Validation Systems are backed by an enterprise PKI validation solution that determines trust anchors and required constraints on the PKI. These enterprise validation solutions may include high-availability, consolidated OCSP responders or SCVP servers.

Other approaches that meet the functional requirements are also valid.

4.3 PIV Reader Category

A PIV Reader is an accepting device as defined in E-PACS that provides the human interface, the card interface, and the communications[1] to and from the Validation System. It is installed at a door, portal, or gateway. As an accepting device, a PIV Reader may be a wholly-integrated unit, or it may be an assembly of components including:

- Contact smart card reader;
- Contactless smart card reader;
- LCD display;
- LED lights;
- Audio announcers;
- PIN pad;
- Fingerprint sensor;
- Other biometric modalities (e.g., iris); and
- Communications to a validation system (e.g., Wiegand, RS-485, secure wireless, Ethernet).

The PIV Reader is a device that is installed at the door and performs functions to interact with the bearer of the credential, the credential itself. This configuration can vary. The Reader must support a minimum of one FICAM authentication mode as defined in E-PACS but may support multi-factor authentication. The Reader may also support optional legacy technologies and credential formats as defined in [FRTC].

Other approaches that meet the functional requirements are also valid.

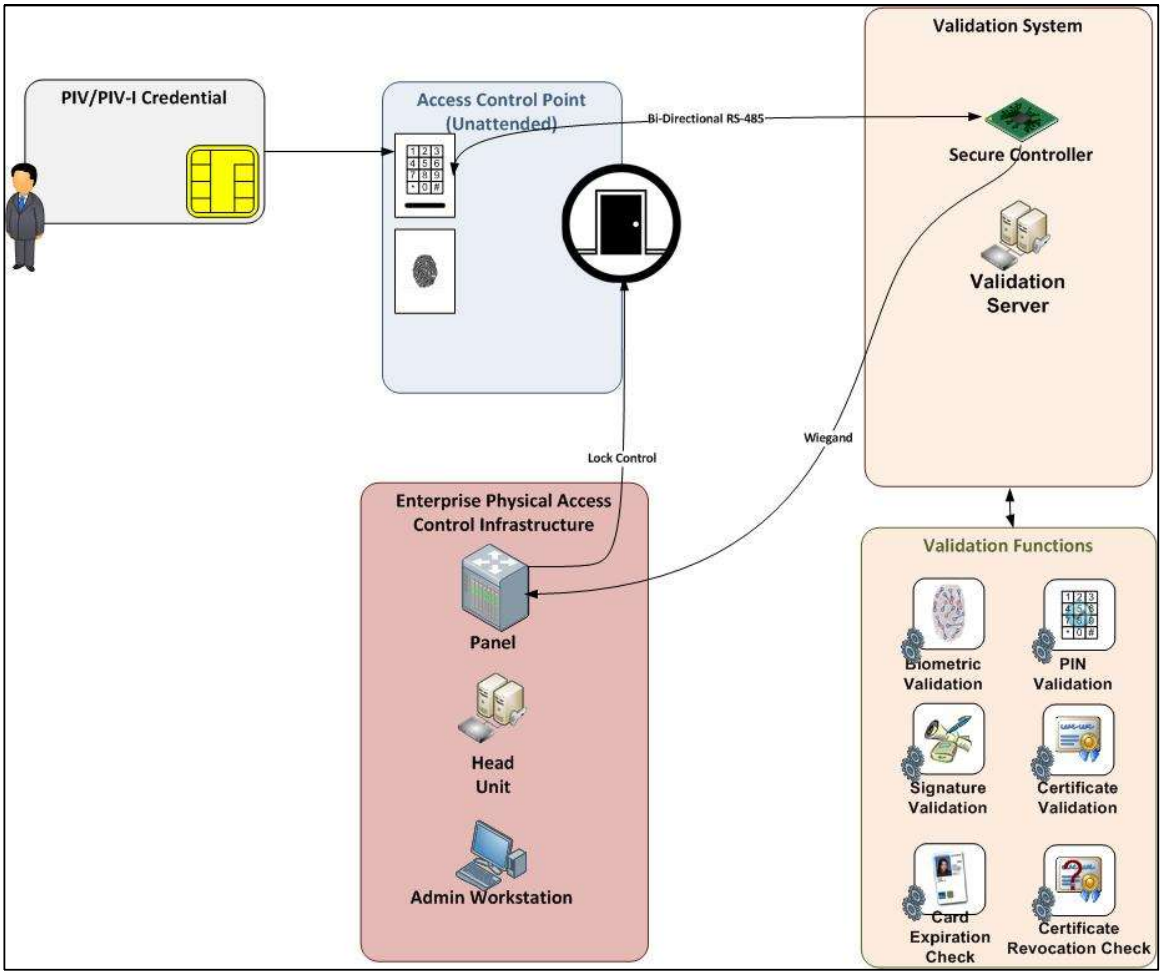
[1] Vendors have the flexibility on how the communication works (i.e., whether communication is direct at run time or other mechanisms are used).

4.4 Topology Diagram

The Applicant must submit a topology diagram to the FIPS 201 Evaluation Program. The diagram must show the architectural linkage of all components that make up an end-to-end system. It must show which components belong to a given category. The diagram facilitates an understanding of how a system is linked together and how it performs the functions required by [FRTC]. In other words, the diagram is a communications tool to enable the FIPS 201 Evaluation Program to understand how a given solution is put together to support end-to-end operational testing.

Figure 1 is a sample topology diagram that portrays one potential approach. Other approaches that meet the functional requirements are also valid.

Figure 1 - Sample Topology for an End-to-End System Using FIPS 201 Evaluation Program Categories



A complete topology diagram identifies every component that makes up an applicant's solution for the FIPS 201 Program categories and provides the specific linkages (communications, internal messaging) that makes up the solution. As new topologies are adopted per [TAP], applicants must map their solution and its components into these new topologies.

4.5 Testing Criteria

4.5.1 Severity Levels

If [FRTC] functional requirements are revised due to time-sensitive security threats, noted technology vulnerabilities, or other critical issues, or alternatively, specific problems are discovered in a vendor's product (or class of products) after it has been listed on the APL, the affected vendor(s) will be notified that the identified product(s) must be improved as necessary in order to remain on the APL. A remediation grace period will be granted commensurate with the severity level of the problem.

4.5.2 APL Listing Requirements

Table 1 defines the APL listing requirements based on classification of the test case and its severity level. The program will not list a product that has a Severity 1 test case that failed (shown RED). ***Table 2*** specifies the remediation timeframes for each severity level. Products not corrected within the given timeframe will be moved to the Removed Products List (RPL).

Table 1 - APL listing based on Test Level and Classification

Test Level / Classification	***Severity 1***	***Listed on APL***	***Severity 2***	***Listed on APL[2]***	***Severity 3***	***Listed on APL***
Security Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✗	Fail	✓
Security Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Security Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓
Usability Required	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓
Usability Optional: Supported by Product	Pass	✓	Pass	✓	Pass	✓
	Uses APL approved product	✓	Uses APL approved product	✓	Uses APL approved product	✓
	Fail	✗	Fail	✓	Fail	✓

[2] No new solution that fails a test case labeled Security/Required Severity Level 2 (SR-2) will be listed on the APL. Existing solutions that initially passed a SR-2 test case, but in subsequent revisions fail a SR-2 test case, are subject to remediation within 90 days as specified in ***Table 2*** below.

Test Level / Classification	*Severity 1*	*Listed on APL*	*Severity 2*	*Listed on APL[2]*	*Severity 3*	*Listed on APL*
Usability Optional: Not Supported	Not Supported	✓	Not Supported	✓	Not Supported	✓

Table 2 - Severity Remediation Timeframes

Severity Level	*Severity Description*	*Remediation Timeframe*
1	The identified problem results in a High impact to any of security, PACS operations, PACS availability, or other area examined.	30 days
2	The identified problem results in a Moderate impact to any of security, PACS operations, PACS availability, or other area examined.	90 days
3	The identified problem results in a Low impact to any of security, PACS operations, PACS availability, or other area examined.	1 year

4.5.3 Classification Codes and Scoring Guidelines

The Topology Mapping form includes a classification code for each test case. The classification code is shorthand that indicates the test type for the requirement is *Security* or *Usability* and whether the requirement is mandatory (*Required*) or *Optional*.

Table 3 - Classification Codes

Classification Code	*Security/Usability*
S[RO]-[123]	**Security** - A control directly impacting security of the system.
U[RO]-[123]	**Usability** - A control impacting end user system usability. Does not directly impact security.
[SU]R-[123]	**Required** - Must be present. Must work correctly: Red/Green.
[SU]O-[123]	**Optional** - May be present. If present, it must work correctly: Red/Green. Not Supported: Yellow.
Example: SR-2	**Security, Required, Severity Level 2**
Example: UO-3	**Usability, Optional, Severity Level 3**

5 Topology Mapping

Mapping is the process of taking the functional requirements defined in [FRTC] and allocating them into the FIPS 201 Evaluation Program categories, and then indicating the specific named components within your solution that perform the operations for that requirement. For example, if the requirement is for a product to validate signatures as defined in [FRTC] §2.1-Test 2.1.1, the Applicant should follow the example given in ***Table 4*** below.

Table 4 - Example Mapping Table for Time of Individual Registration Signature Verification

FRTC Version	Classification	TC #	Card #	Path #	Description/Test Case Procedure	Expected Result	Requirement Source	Category(ies)	Components	Process
		2.0			**Requirements at Time of In-Person Registration in Accordance With [E-PACS] PIA-9**	**All tests use PKI-AUTH unless specifically noted.**	**Note all requirements sourced from [E-PACS] unless otherwise noted.**			`
		2.01			**Signature Verification**					
1.2.0	SR-1	2.01.01	01	00	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential	Registration succeeds.	PIA-2 thru PIA-7	Validation System (13.01), PACS Infrastructure (13.01)	Registration Workstation, PACS application, Path Discovery and Validation engine	EE certificate signature is validated immediately by the Validation System. The CA certificate signatures are evaluated, but may be cached by the path discovery and validation engine if they have been previously seen.

In the example provided in ***Table 4***, the signature verification involves several elements. It is allocated to the PACS Infrastructure and Validation System, as both solutions require information from the credential. The PACS Infrastructure provides the registration workstation. The Validation System is doing the PKI signature verification for the end entity, and the Validation System's PDVAL engine is evaluating signatures and caching status for the CA certificate path. Clearly there are many potential combinations of components within categories that could perform this function and it is up to the applicant to describe the process of how, when, and where [FRTC] requirements are met.

5.1 Topology Mapping Workbook

The PACS FRTC 1.3.3 Topology Mapping Workbook contains a listing of requirements used with the 13.01 topology. Beginning with FRTC 1.3.3, we provide this artifact in the form of a Microsoft Excel workbook which allows you to hide columns as needed and maneuver more easily. You will find the Topology Mapping Workbook included in the evaluation application. Use it to provide the Lab with the PACS 13.01 topology mapping of functional requirements identified in the [FRTC] to the FIPS 201 Evaluation Program categories as defined in this document. The columns for Category(ies), Components and Process are intentionally left blank in this table. These three columns must be completed by the Applicant when submitting a component/solution to the FIPS 201 Evaluation Program for evaluation, testing, and approval.