NIST Cybersecurity White Paper
NIST CSWP 37 ipd

Automation of the NIST Cryptographic Module Validation Program:

September 2024 Status Report

Initial Public Draft

Chris Celi
Alex Calis
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

William Barker
Dakota Consulting

Karen Scarfone
Scarfone Cybersecurity

Raoul Gabiam
The MITRE Corporation

Stephan Mueller
Yi Mao
atsec information security

Barry Fussell
Andrew Karcher
Cisco

Douglas Boldt
Amazon Web Services

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.37.ipd

October 31, 2024

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Abstract

The Cryptographic Module Validation Program (CMVP) validates third-party assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140-3, Security Requirements for Cryptographic Modules. The NIST National Cybersecurity Center of Excellence (NCCoE) has undertaken the Automated Cryptographic Module Validation Project (ACMVP) to support improvement in the efficiency and timeliness of CMVP operations and processes. The goal is to demonstrate a suite of automated tools that would permit organizations to perform testing of their cryptographic products according to the requirements of FIPS 140-3, then directly report the results to NIST using appropriate protocols. This is a status report of progress made so far with the ACMVP and the planned next steps for the project.

Audience

The primary audience for this report is technology, security, and privacy program managers and architects, and software developers, engineers, and IT professionals.

Keywords

Automated Cryptographic Module Validation Project (ACMVP); Cryptographic Module Validation Program (CMVP); cryptography; cryptographic module; cryptographic module testing; cryptographic module validation.

Acknowledgements

The ACMVP TE Workstream (WS) is led by Yi Mao of atsec and Alex Calis of NIST with contribution from the atsec team, Javier Martel and Michael McCarl of Aegisolve, Ryan Thomas of Lightship Security, James Reardon of Intertek Acumen Security, Barry Fussell and Andrew Karcher of Cisco, Alicia Squires and Courtney Maatta of Amazon, Marc Ireland of NXP, Shawn Geddis formerly of Apple, Mike Grimm of Microsoft, Ivan Teblin and Blaine Stone of SUSE, Michael Dimond of the MITRE Corporation, and Chris Celi and Murugiah Souppaya of NIST.

The ACMVP Protocol Workstream is led by Barry Fussell and Andrew Karcher of Cisco and Chris Celi of NIST with contributions from Panos Kampanakis of Amazon, Michael McCarl and Deborah Harrington of Aegisolve, Alex Thurston of Lightship, Stephan Mueller and Walker Riley of atsec, Mike Grimm of Microsoft, Robert Staples of NIST, and Raoul Gabiam, Michael Dimond, Kyle Vitale, Doris Rui, and Matthew Fortes of the MITRE Corporation.

The ACMVP Research Infrastructure Workstream is led by Raoul Gabiam of The MITRE Corporation and Douglas Boldt of Amazon, with contributions from Courtney Maatta, Annie Cimack, Diana Brooks, Charlotte Fondren, Zhuo-Wei Lee, Keonna Parrish, Abhishek Isireddy, Abi Adenuga, Bradley Wyman, Brittany Robinson, Gina McFarland, Damian Zell, Cavan Slaughter, Rayette Toles-Abdullah, and Natti Swaminathan of Amazon; Robert Staples and Murugiah

Souppaya of NIST; Michael Dimond, Kyle Vitale, and Josh Klosterman of the MITRE Corporation; and John Booton, Aaron Cook, and Jeffrey LaClair of ITC Federal.

Collaborators

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

- Acumen Security
- AEGISOLVE
- Apple
- Atsec
- AWS
- Cisco
- Lightship Security
- Microsoft
- NXP Semiconductors
- SUSE

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Table of Contents

List of Tables

1. Overview

1.1. Challenge

The Cryptographic Module Validation Program (CMVP) validates third-party assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140-3, Security Requirements for Cryptographic Modules. Under the CMVP, cryptographic modules undergo third-party testing by National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories, and the processes and results are validated under a program run by the National Institute of Standards and Technology (NIST) and the Canadian Center for Cyber Security (CCCS). Current industry cryptographic product development, production, and maintenance processes place significant emphasis on time-to-market efficiency. A number of elements of the validation process are manual in nature, and the period required for third-party testing and government validation of cryptographic modules is often incompatible with industry requirements.

1.2. Solution

The NIST National Cybersecurity Center of Excellence (NCCoE) has undertaken a project to demonstrate the value and practicality of automation support to improve the responsiveness of CMVP. The intent of the Automated Cryptographic Module Validation Project (ACMVP) is to support improvement in the efficiency and timeliness of CMVP operations and processes. This NCCoE effort is one of a number of activities focused on the automation of module validation and report review flow, and it follows the successful completion of NIST efforts such as the automation of the Cryptographic Algorithm Validation Program (CAVP); the rollout of Web-Cryptik, an application for submitting test results to the CMVP; and the automation of the processing of entropy data testing evidence for the Entropy Source Validation (ESV) program. The initiative aims to provide mechanisms for structural presentation of testing evidence by NVLAP-accredited parties to facilitate the automation of evidence validation by the CMVP.

The ACMVP's goal is to enable automated test report review where feasible for each of the test requirements found in FIPS 140-3 and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 24759, which FIPS 140-3 incorporates by reference. Because of the wide range of the technologies and corresponding security requirements that the CMVP covers, this effort is being executed in phases. The initial phase of software module validation such as an OpenSSL module is foundational and will determine future phases.

The module testing and reporting aspects of module validation, according to ISO/IEC 24759, combine functional and nonfunctional security requirements. This project attempts to streamline the test methods for the functional tests of specific classes of technologies (e.g., software modules) and corresponding reporting of functional and non-functional security requirements. We are working to demonstrate a suite of tools to modernize and automate manual review processes in support of existing policy and efforts to include technical testing

under the CMVP. These automated tools employ an NVLAP-accredited testing concept that permits organizations to perform the testing of their cryptographic products according to the requirements of FIPS 140-3, then directly report the results to NIST using appropriate protocols.

The accredited parties will have to identify the corresponding personnel and organizational structures needed to perform this testing while complying with the laboratory requirements for testing programs established by NVLAP under NIST Handbook (HB) 150-17. The accreditation requirements in HB 150-17 are both hierarchical and compositional in nature so that organizations can tailor the scope of accreditation according to their specific product/service portfolio.

1.3. Progress to Date

To date, the ACMVP project has:

- Identified and classified categories of test evidence required for CMVP validation that can readily be automated in a reporting format that is consistent with current Web-Cryptik and CMVP; identified the test evidence classes for which manual processes are still needed
- Identified necessary schemas and protocols for evidence submission and validation for a scalable application programming interface (API) based architecture
- Designed and developed a cloud native infrastructure required to support validation program automation

In the initial phase, the project is divided into three workstreams: the Test Evidence (TE) Workstream, the Protocol Workstream, and the Research Infrastructure Workstream. Each is a focused effort in its own right. The combined impact of these workstreams will result in improvements to the overall automation of the CMVP.

Contributors to each workstream are listed in the corresponding sections below. Additionally, the following people and organizations contributed to the project outside of a workstream: Rochelle Casey, Alicia Squires, Margaret Salter, Tim Ness, and David Browning of Amazon; Apostol Vassilev, Dave Hawes, Gavin O'Brien, Tim Hall, Matt Scholl, Cheri Pascoe, Kevin Stine, Ann Rickerds, Jim Simmons, Rob Densock, and Blair Heiserman of NIST; William Barker of Dakota Consulting; Karen Scarfone of Scarfone Cybersecurity; and Heather Flanagan of Spherical Cow Consulting.

2. Test Evidence Workstream

The ACMVP TE Workstream (WS) is led by Yi Mao of atsec and Alex Calis of NIST with contribution from the atsec team, Javier Martel and Michael McCarl of Aegisolve, Ryan Thomas of Lightship Security, James Reardon of Intertek Acumen Security, Barry Fussell and Andrew Karcher of Cisco, Alicia Squires and Courtney Maatta of Amazon, Marc Ireland of NXP, Shawn Geddis formerly of Apple, Mike Grimm of Microsoft, Ivan Teblin and Blaine Stone of SUSE, Micheal Dimond of the MITRE Corporation, and Chris Celi and Murugiah Souppaya of NIST.

The TE WS has identified and sorted categories of test evidence required for CMVP validation that can readily be automated in a reporting format that is consistent with current Web-Cryptik used by CMVP. The TE WS has also identified those test evidence classes for which manual processes are still needed.

To date, the TE WS team has classified test evidence into the following categories, depending on what needs to be checked, inspected, or tested, and how the vendor evidence (VE) is supposed to be provided:

- Assessments based on reviewing the vendor documentation, especially the Security Policy (SP)
- Assessments based on inspecting the module's source code
- Assessments based on exercising/executing the module to cover functional testing.

The team has also described an approach to filtering test requirements to make the report focus only on the relevant requirements. TE WS output to date is presented in Appendix A.

The main accomplishments of the TE WS to date are as follows:

- Classification/categorization of TEs
- AS/TE/VE (Assertions/Requirements for Tester/Requirements for Vendor) filtering
- A well-defined structure for test evidence data represented in JSON. These JSON files are used by other workstreams within the ACMVP to define the schema and provide opportunity for future automation (includes Security Policy JSON file to satisfy SP TEs.)
- Alignment of the CMVP's Documentation TE List with TE classifications

The TE WS team is now working to complete:

- Test methods for functional testing TEs
- Improvement of TE filtering coverage
- Finalizing the JSON structure for the TE catalog

3. Protocol Workstream

The ACMVP Protocol Workstream is led by Barry Fussell and Andrew Karcher of Cisco and Chris Celi of NIST with contributions from Panos Kampanakis of Amazon, Michael McCarl and Deborah Harrington of Aegisolve, Alex Thurston of Lightship, Stephan Mueller and Walker Riley of atsec, Mike Grimm of Microsoft, Robert Staples of NIST, and Raoul Gabiam, Michael Dimond, Kyle Vitale, Doris Rui, and Matthew Fortes of the MITRE Corporation.

The Protocol WS is responsible for defining the interactions between automated CMVP server assets and the NCCoE ACMVP clients supporting a proof-of-concept of automation capabilities. The proof-of-concept server currently implements the following features:

- Two-factor authentication using time-based one-time passwords (TOTPs) and mTLS. This system improves the TOTP from the Automated Cryptographic Validation Protocol (ACVP) by allowing a user to maintain multiple seeds for simultaneous connections.
- Module registration that defines the security levels, embodiments, and other properties of the cryptographic module. This is used to automatically determine which TEs are applicable to the cryptographic module.
- Module evidence catalog submission that prompts a client to provide evidence addressing TEs that are applicable to the cryptographic module. The system will inform you which TEs have not yet been addressed by the submission to ensure completeness.
- Module security policy submission defined entirely in JSON. The system will generate the security policy automatically, allowing the client to retrieve the completed PDF. This ensures that all sections are present and completed.
- Award of a validation certificate once all evidence catalog and security policy information are completed.

The proof-of-concept includes both client and server components.

- The server uses much of the same infrastructure as ACVP and Entropy Source Validation (ESV). This is intentional in order to use the same team to maintain the systems once they are integrated by the CMVP. This is mainly C# applications along with SQL Server databases. The server development team is also using this opportunity to re-evaluate security assurances within NIST to see if any improvements can be brought back into the rest of the CMVP applications.
- Two client examples have been developed:
    - Cisco's Libamvp is C-based and interacts with the server by parsing user-generated JSON. It is intended to be a simple tool to showcase the protocol and assist developers as they create workflows for the generation and submission of AMVP data. Libamvp can create modules and certification requests, submit all required evidence catalog and security policy info, retrieve security policy PDFs, check for the status of a certification request, and more, as development continues. The code is open-source and is available at the public repository https://github.com/cisco/libamvp.

- The atsec ACVP Proxy provides the interface to access the NIST ACVP, Entropy Source Validation Program (ESVP), and AMVP services. The code is open-source and is available at the public repository https://github.com/smuellerDD/acvpproxy. The ACVP Proxy allows a flexible deployment and is extendable to cover an arbitrary number of Implementation Under Test (IUT) definitions. It implements the entire interaction with the NIST servers to obtain the data from the server and upload all required data to the server.

The protocol effort is still in progress. Work planned for the next year includes:

- Demonstrating the ability for the CMVP staff to use an API to handle “comment round” interactions with NVLAP-accredited parties
- Enabling automatic processing of functional test evidence (FE-TEs) based on the test type selected by NVLAP-accredited laboratories
- Enabling acceptance of source code TEs (SC-TEs) and other TEs (OD-TEs) not yet handled by the server

4. Research Infrastructure Workstream

The ACMVP Research Infrastructure Workstream is led by Raoul Gabiam of The MITRE Corporation and Douglas Boldt of Amazon, with contributions from Courtney Maatta, Annie Cimack, Diana Brooks, Charlotte Fondren, Zhuo-Wei Lee, Keonna Parrish, Abhishek Isireddy, Abi Adenuga, Bradley Wyman, Brittany Robinson, Gina McFarland, Damian Zell, Cavan Slaughter, Rayette Toles-Abdullah, and Natti Swaminathan of Amazon; Robert Staples and Murugiah Souppaya of NIST; Michael Dimond, Kyle Vitale, and Josh Klosterman of the MITRE Corporation; and John Booton, Aaron Cook, and Jeffrey LaClair of ITC Federal.

The Workstream's objective is to develop and demonstrate a cloud-native infrastructure that is scalable, efficient, and up to date (supports containers, zero trust principles, etc.).

This infrastructure is an extension of the on-premises private cloud at the NCCoE. The NCCoE on-premises infrastructure consists of a VMware private cloud and a Microsoft Active Directory which serves as the authoritative identity source for the supporting AWS research environment. The on-premises VMware private cloud is connected to the AWS supporting research environment via an AWS Direct Connect through NOAA/N-Wave. The supporting AWS research environment consists of multiple accounts following AWS and Special Publication 800-53 best practices to ensure isolation and segregation of administrative functions and security in each independent research lab.

A summary of steps taken to modernize the research infrastructure include:

1. **Leveraging cloud native technologies and services** - The current production CMVP environment was designed and built on a standard architecture for on-premises services. The project team is taking this opportunity to refactor the CMVP infrastructure to leverage cloud-native technologies and services. This will modernize the supporting infrastructure, improve efficiency and scalability, and streamline operations. Technologies and services being piloted include containerization to facilitate portability and scalability, serverless to improve efficiency, and AWS RDS and AWS code builds to streamline and automate operations.
2. **Providing visibility in workloads and resources** - A benefit of leveraging cloud services is the transparency and visibility of workloads and their resources down to the specific services used. This enables the team test and balance efficiencies of cloud-native architectures while remaining cost conscious.
3. **Leveraging AWS cloud-native services for security** - The NCCoE AWS research cloud environment supporting the CMVP Automation project leverages AWS cloud-native technologies and services to secure the environment and ensure best practices are followed. These services include AWS Control Tower, AWS Organization, AWS Security Lake, AWS CloudWatch, AWS CloudTrail, AWS Security Hub, and more. A few mapping documents are being generated to capture how the NCCoE is following NIST best practice documents such as Special Publication 800-92 and 800-53 in their AWS research cloud environment.

4. **Infrastructure as code** - Another benefit of leveraging cloud-native services and tools is the ease of deploying them as code. This facilitates the creation of infrastructure stacks, which facilitates creation and replication of infrastructure from code

Next steps planned for the Research Infrastructure WS include:

- Conducting a security assessment of the underlying infrastructure.
- Deploying, testing, optimizing, and documenting a scalable and modernized CMVP infrastructure
- Replicating the research environment into the NIST staging environment, and updating infrastructure documentation.

5. Conclusion

To date, the project has:

- Identified and sorted categories of test evidence required for CMVP validation that can readily be automated in a reporting format that is consistent with current Web-Cryptik used by CMVP, and identified those test evidence classes for which manual processes are still needed.
- Identified necessary schemas and protocols for report submission and validation for a scalable API-based architecture.
- Designed and developed a cloud-based infrastructure required to support validation program automation.

Moving forward, the project staff plans in FY 2025 to:

- Finalize a coordinated JSON structure for TE catalog
- Refine the research infrastructure to support enabling automated acceptance of test evidence and processing of functional test evidence from NVLAP-accredited parties
- Streamline test methods for functional testing
- Improve test requirement filtering capabilities
- Demonstrate an ability for the CMVP staff to use an API to handle “comment round” interactions with NVLAP-accredited parties.

Appendix A. Technical Details from the Test Evidence (TE) Workstream

The rest of this report provides additional technical details from the Test Evidence (TE) Workstream:

- Appendix A.1, TEs Requiring Vendor Documentation: categories and sub-categories of TEs based on reviewing the Security Policy (SP) or other vendor documentation
- Appendix A.2, TEs Requiring Module Functional Test: TEs based on exercising/executing the module to test its functionality
- Appendix A.3, Complete List of TEs: a complete list of TEs, each tagged by category

A.1. TEs Requiring Vendor Documentation

The required documentation for a Federal Information Processing Standards (FIPS) validation is specified in NIST Special Publication 800-140A, which modifies the vendor documentation requirements of ISO/IEC 19790 Annex A. Hereafter, the vendor-documentation-dependent TEs will be indicated as **140A-TE**s. Those TEs require the tester to verify the presence and accuracy of information within the vendor documentation or to verify statements based on information from the documentation.

The overall category of 140A-TEs, as opposed to the TEs depending on functional tests (hereafter **FT-TE**s), is relatively clear. They are indicated by the keyword “verify” as in the following examples:

- “verify the name and version as indicated in AS04.13” (e.g., TE04.33.01)
- "verify the vendor documentation" (e.g., TE04.05.01)
- "verify that the vendor provided documentation" (e.g., TE05.05.01)
- "verify, by inspection and from the vendor documentation" (e.g., TE05.15.01)
- "verify the vendor documentation, and by inspection" (e.g., TE06.10.01), "verify by inspection, or from the vendor documentation" (e.g., TE07.15.01)
- "verify … as documented" (e.g., TE07.27.01)
- "verify … are documented" (e.g., TE07.33.01)
- "verify the vendor documentation shows … " (e.g., TE10.09.01)
- "verify … through the procedure documented in …" (e.g., TE10.11.01)

The 140A-TEs may or may not depend on the SP. They may depend on source code or other proprietary documentation. So, the **140A-TE**s can be further divided into three sub-categories as they relate to Security Policy (SP), Source Code (SC), and Other Documents (OD):

- **SP-TE**s: TEs depend on the information provided by the public-facing SP. NIST Special Publication 800-140Br1 is to be used in conjunction with ISO/IEC 19790 Annex B and ISO/IEC 24759 section 6.14. It also specifies the order of the SP. Some TEs explicitly

identify the source of the vendor documentation in the SP. Ideally, Special Publication 800-140Br1 should require the SP to include all information to satisfy the SP-dependent TEs.

- **SC-TE**s: TEs require source code review. It may not be intuitive that source code falls under vendor documentation. There are TEs that explicitly require code review or actual source code, verify some statement by (code) inspection, or verify how the specification is implemented. Source code handling often requires special care and attention. Therefore, we separate these SC-TEs from the TEs that depend on other vendor documentation.
- **OD-TE**s: If a 140A-TE is neither an SP-TE nor an SC-TE, we designate it as an OD-TE, meaning the TE depends on an Other Document such as a Finite State Model (FSM), Component List (CL), design document, user guidance, or configuration management manual.

Here are some examples:

- SP-TEs: 140B requires the SP to provide the information
  - TE04.47.01: *The tester shall verify that the security functions used to authenticate operators are all approved security functions.*
  - TE04.48.01: *The tester shall verify that the authentication mechanism used to authenticate operators is an approved one.*
- SC-TEs: TEs that depend on source code inspection
  - TE03.07.05: *The tester shall verify that the vendor documentation specifies how the cryptographic module ensures that all data output via the data output interface is to be inhibited during error states or self-test conditions. The tester shall also verify, by inspection of the design of the cryptographic module, that the data output interface is, in fact, logically or physically inhibited under these conditions.*
  - TE03.15.05: *The tester shall examine the applicable source code(s) to ensure that the identified component is actually validating the documented format.*
- OD-TEs: requires rationale of correctness, FSM or SW/FW CL
  - TE03.19.03: *The tester shall verify the correctness of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.*
  - TE11.08.01: *The tester shall verify that the vendor has provided a description of the finite state model. This description shall contain the identification and description of all states of the module and a description of all corresponding state transitions. The tester shall verify that the descriptions of the state transitions include the internal module conditions, data inputs and control inputs that cause*

transitions from one state to another, data outputs and status outputs resulting from transitions from one state to another.

- TE11.16.01: *The tester shall use the list supplied by the vendor to verify that a source listing for each software or firmware component is contained in the module.*

Let us look at an example TE that is assessed by reviewing the vendor documentation, and this TE's associated AS and VE.

AS05.02 states, "The documentation requirements specified in {ISO/IEC 19790:2012} A.2.5 shall be provided." Following that, **VE05.02.01** states, "The vendor shall provide documentation as specified in ISO/IEC 19790:2012, A.2.5." Lastly, the **TE05.02.01** for this section states, "The tester shall verify completeness of the documentation specified in ISO/IEC 19790:2012, A.2.5."

To fulfill **TE05.02.01**, the tester needs to check the documentation provided by the vendor and verify that it is present and complete. The example illustrates a documentation-type TE (i.e. 140A-TE). TEs of this type are ripe for automation because they only rely on checking for the presence of appropriate texts. The accuracy of the information provided for these TEs is later verified by subsequent tests and documentation reviews done during Functional Testing, Source Code Review, and Module Inspection.

By exploring the relationship between VEs and TEs, it becomes apparent that if some VEs were in the form of a standardized SP, their corresponding TEs could be verified through automation. The NIST CMVP updated Special Publication 800-140B to specify the expected content of the SP and provide an SP template for all vendors and labs to use; Revision 1 was published in November 2023.

The current NIST Web-Cryptik Br1 v1.0.3 has built-in Module Information Structure (MIS) Tables and a search capability to look up and select Cryptographic Algorithm Validation Program (CAVP) certificates. The completed MIS Tables can be saved as a JSON file and be combined with other information in an SP Microsoft Word template to build the final SP.

This TE WS is exploring an alternative method to generate the SP purely via JSON rather than implementing a hybrid approach that requires an SP Microsoft Word template to build the final SP. Following the CMVP's current SP Template v5.8, the NCCoE TE WS has developed an SP-evidence JSON file to satisfy all SP-TEs. The NCCoE Research Infrastructure WS is implementing the functionality on the ACMVP server for generating an SP in a PDF file based on the input SP-evidence JSON file. This functionality will be demoed at the ICMC24.

Under the assumptions that the SP strictly follows Special Publication 800-140Br1 and that the required SP content is captured in MIS Tables or the other data entries in the SP-evidence JSON file, all SP-TEs can reference the relevant data points in the SP-evidence JSON file. The existence of the reference can be automatically checked. If the reference exists, the corresponding TE passes.

SP-TEs must be satisfied by the information provided by the SP as specified in NIST Special Publication 800-140Br1, which we denote as **140B-TEs**. 140B-TEs is a subset of SP-TEs because a

vendor may choose to include more information in the SP as required by Special Publication 800-140Br1.

Furthermore, to maximize automation, all data points necessary to satisfy 140A-TEs should be captured in a standardized documentation-evidence JSON. This work needs to be incorporated and elaborated in the TE catalog.

Table 1 lists all of the TEs depending on the SP, regardless of whether the TE explicitly indicates the source of the vendor document to be the SP or whether Special Publication 800-140Br1 requires it, in column **SP-TEs**. The **non-140B-but-140A-TEs** column is not intended to duplicate the TEs from the SP-TEs column, but instead to capture all other TEs that depend on vendor documentation, which could be SP, source code, FSM, CL, design document, or other vendor proprietary documentation. For cases where the information needs to be in the SP and verified by (code) inspection or design document, the TEs (e.g., TE02.07.02) are listed under both columns, despite the duplication.

TEs depending on source code review or inspection are a subset of the non-140B-but-140A-TEs column in the table. Some TEs have the explicit wording of “code” or “source code,” while others imply it via the phrase “by inspection” or “inspecting the module.” TEs requiring source code review are tagged as SC-TE in Appendix A.3, Complete List of TEs.

TEs requiring other documents are tagged as OD-TE in Appendix A.3, Complete List of TEs.

Table 1 - Dividing 140A-TEs into non-140B-TEs and SP-TEs

FIPS 140-3 Section Title	140A-TEs: non-140B-but-140A-TEs	140A-TEs: SP-TEs
General	None	None
Cryptographic Module Specification	TE02.03.02, TE02.07.01, TE02.07.02 (also SP-TE), TE02.10.01 (also SP-TE), TE02.10.02, TE02.13.02, TE02.17.09	TE02.03.01, TE02.07.02, TE02.09.01, TE02.10.01, TE02.11.01, TE02.11.02, TE02.12.01, TE02.13.01, TE02.14.01, TE02.15.01, TE02.15.02, TE02.15.04, TE02.15.06, TE02.15.07, TE02.15.08, TE02.15.09, TE02.15.10, TE02.15.11, TE02.15.12, TE02.15.13, TE02.15.14, TE02.16.01, TE02.16.02, TE02.16.03, TE02.16.05, TE02.17.01, TE02.17.02, TE02.17.03, TE02.17.05, TE02.17.06, TE02.17.07, TE02.17.08, TE02.17.10, TE02.18.01, TE02.19.01, TE02.20.01, TE02.20.02, TE02.20.03, TE02.20.04, TE02.21.01, TE02.21.02, TE02.22.01, TE02.24.01, TE02.26.01, TE02.26.02, TE02.30.01
Cryptographic Module Interfaces	TE03.01.02 (also SP-TE), TE03.02.01, TE03.05.02, TE03.06.02, TE03.07.01, TE03.07.03, TE03.07.05, TE03.07.06, TE03.07.07, TE03.08.02, TE03.09.01, TE03.10.01, TE03.10.03, TE03.10.05,	TE03.01.01, TE03.01.02, TE03.01.03, TE03.02.02, TE03.03,01, TE03.04.01

FIPS 140-3 Section Title	140A-TEs: non-140B-but-140A-TEs	140A-TEs: SP-TEs
	TE03.11.02, TE03.13.01, TE03.14.01, TE03.14.02, TE03.14.03, TE03.15.01, TE03.15.02, TE03.15.05, TE03.16.01, TE03.18.01, TE03.19.01, TE03.19.03	
Roles, Services, and Authentication	TE04.02.01, TE04.03.01, TE04.07.01, TE04.07.02, TE04.19.01, TE04.20.01, TE04.20.02, TE04.21.01, TE04.22.01, TE04.25.01, TE04.33.01, TE04.35.01, TE04.38.01, TE04.39.01, TE04.42.01, TE04.42.02, TE04.43.01, TE04.44.01, TE04.45.01, TE04.51.02, TE04.53.01, TE04.54.01, TE04.55.01	TE04.05.01, TE04.06.01, TE04.11.01, TE04.13.02, TE04.14.01, TE04.18.01, TE04.37.01, TE04.47.01, TE04.48.01, TE04.50.01, TE04.50.02, TE04.51.01, TE04.56.01, TE04.56.02, TE04.59.01
Software/Firmware Security	TE05.02.01, TE05.04.01, TE05.05.01, TE05.05.03, TE05.05.04, TE05.05.06, TE05.06.01, TE05.06.05, TE05.07.01, TE05.08.02, TE05.11.01, TE05.12.01, TE05.12.02, TE05.13.01, TE05.13.02, TE05.13.04, TE05.13.06, TE05.13.07, TE05.15.01, TE05.15.02, TE05.16.01, TE05.16.02, TE05.20.01, TE05.23.01	TE05.05.02, TE05.17.01
Operational Environment	TE06.03.01, TE06.05.01, TE06.05.02, TE06.06.01, TE06.08.01, TE06.08.02, TE06.10.01, TE06.11.01, TE06.12.01, TE06.13.01, TE06.14.01, TE06.15.01, TE06.17.01, TE06.18.01, TE06.19.01, TE06.24.01, TE06.25.01, TE06.26.01, TE06.27.01, TE06.28.01	TE06.07.01, TE06.09.01, TE06.20.01
Physical Security	TE07.10.01, TE07.11.01, TE07.12.01, TE07.15.01, TE07.15.02, TE07.19.01, TE07.20.01, TE07.25.01, TE07.26.01, TE07.33.01, TE07.35.01, TE07.37.01, TE07.37.02, TE07.39.01, TE07.39.02, TE07.39.03, TE07.39.04, TE07.41.01, TE07.42.01, TE07.43.01, TE07.44.01, TE07.45.01, TE07.46.01, TE07.47.01, TE07.48.01, TE07.50.01, TE07.50.02, TE07.50.03, TE07.51.01, TE07.51.02, TE07.51.03, TE07.51.04, TE07.51.05, TE07.51.07, TE07.53.01, TE07.55.01, TE07.57.01, TE07.60.01, TE07.65.01, TE07.65.02, TE07.65.03, TE07.65.04, TE07.65.05, TE07.65.06, TE07.65.07, TE07.67.01, TE07.71.01, TE07.73.01	TE07.01.01, TE07.09.01, TE07.09.02, TE07.19.01, TE07.26.02, TE07.77.04, TE07.81.03
Non-Invasive Security	Not yet enforced by the CMVP	Not yet enforced by the CMVP
Sensitive Security Parameter Management	TE09.01.01, TE09.02.01, TE09.03.01, TE09.05.01, TE09.08.02, TE09.14.01, TE09.16.01, TE09.16.02, TE09.21.01,	TE09.04.01, TE09.04.02, TE09.06.01, TE09.06.02, TE09.06.03, TE09.07.01, TE09.08.01, TE09.09.01, TE09.09.02,

FIPS 140-3 Section Title	140A-TEs: non-140B-but-140A-TEs	140A-TEs: SP-TEs
	TE09.23.01, TE09.23.02, TE09.23.04, TE09.24.01, TE09.25.01, TE09.27.01, TE09.28.06, TE09.29.01, TE09.29.02, TE09.31.01, TE09.32.01, TE09.36.01	TE09.10.01, TE09.10.02, TE09.13.01, TE09.13.02, TE09.19.01, TE09.22.01, TE09.28.01, TE09.28.05, TE09.33.01, TE09.37.01
Self-Tests	TE10.12.01, TE10.12.02, TE10.15.01, TE10.15.02, TE10.20.01, TE10.21.01, TE10.21.02, TE10.22.02, TE10.22.03, TE10.22.05, TE10.27.01, TE10.28.01, TE10.29.01, TE10.33.02, TE10.34.02, TE10.35.01, TE10.35.02, TE10.35.03, TE10.37.03, TE10.37.04, TE10.37.07, TE10.37.08, TE10.46.01, TE10.46.02, TE10.48.02, TE10.49.02, TE10.51.01, TE10.51.02, TE10.51.03	TE10.07.01, TE10.07.02, TE10.08.01, TE10.08.02, TE10.09.01, TE10.09.02, TE10.24.01, TE10.25.01, TE10.33.01, TE10.34.01, TE10.37.01, TE10.37.02, TE10.53.01
Life-Cycle Assurance	TE11.01.01, TE11.03.01, TE11.04.01, TE11.04.02, TE11.04.03, TE11.04.04, TE11.05.01, TE11.06.01, TE11.08.01, TE11.08.02, TE11.08.03, TE11.08.04, TE11.08.05, TE11.08.07, TE11.08.08, TE11.08.10, TE11.08.11, TE11.08.12, TE11.13.01, TE11.15.01, TE11.15.02, TE11.16.01, TE11.17.01, TE11.18.01, TE11.19.01, TE11.21.01, TE11.23.01, TE11.24.01, TE11.25.01, TE11.26.01, TE11.28.01, TE11.28.02, TE11.28.03, TE11.29.01, TE11.29.02, TE11.30.01, TE11.31.01, TE11.33.01, TE11.34.01, TE11.38.03	TE11.32.01, TE11.35.01, TE11.36.01, TE11.37.01, TE11.38.01, TE11.39.01
Mitigation of Other Attacks	TE12.01.01, TE12.04.02	TE12.02.01, TE12.04.01, TE12.04.03
NIST Special Publication 800-140A	TEA01.01	
NIST Special Publication 800-140B (Cryptographic module security policy)		TEB.01.01, TEB.02.01, TEB.03.01, TEB.03.02

A.2. TEs Requiring Module Functional Test

TEs in this category require the tester to exercise and manipulate the module to test its functionality. To do this, testers rely on various pieces of evidence that include log file names, screenshots, or remote testing/video observation. In essence: the tester must directly see and interact with the module to ensure that it functions in the way specified by the vendor.

TE09.03.02 is an example of this category. It states: “For each Sensitive Security Parameter (SSP) that can be entered, the tester shall first enter the SSP while assuming the correct entity. The tester shall then verify that entry is not possible when assuming an incorrect entity.” To fulfill this TE, the tester must assume specific entities and use the module as those assumed

roles, testing that the module correctly identifies roles and grants only the appropriate SSP entry service to each entity.

This category of TEs is the hardest to automate; however, we may address the work surrounding functional testing. Automation opportunities may be found in how the lab collects and prepares the test evidence (e.g., log files) from functional testing.

Table 2 lists all TEs that require functional testing at specific Security Levels (SLs).

Table 2 - TEs Requiring Functional Testing

FIPS 140-3 Section Name	TEs for SL 1-4	TEs for SL 2-4	TEs for SL 3-4	TEs for SL 4
General	N/A			
Module Specification	TE02.10.01 (or SC-TE), TE02.12.01, TE02.13.03, TE02.15.03, TE02.15.05, TE02.16.04, TE02.17.02, TE02.17.04, TE02.19.02, TE02.22.02, TE02.24.02, TE02.26.03, TE02.26.04, TE02.26.05, TE02.28.01, TE02.28.02, TE02.30.02	None	None	None
Module Interfaces	TE03.01.04, TE03.02.01, TE03.05.01, TE03.05.02, TE03.06.01, TE03.06.02, TE03.07.02, TE03.07.04, TE03.07.08, TE03.08.01, TE03.08.02, TE03.09.02, TE03.10.02, TE03.10.04, TE03.11.01, TE03.11.03, TE03.13.02, TE03.14.03, TE03.15.02, TE03.15.03, TE03.15.04, TE03.15.06	None	TE03.16.01 (or SC-TE), TE03.18.01, TE03.18.02, TE03.19.02, TE03.19.04, TE03.20.01, TE03.21.01	TE03.22.01
Roles, Services, and Authentication	TE04.02.02, TE04.02.03, TE04.07.03, TE04.11.02, TE04.13.01, TE04.13.03, TE04.14.02, TE04.15.01, TE04.19.02, TE04.19.03, TE04.20.01, TE04.20.03, TE04.21.02, TE04.22.02, TE04.23.01, TE04.25.02, TE04.25.03, TE04.28.01, TE04.29.01, TE04.32.01, TE04.33.01, TE04.34.01, TE04.35.02, TE04.37.02, TE04.38.02, TE04.39.02, TE04.39.03, TE04.39.04, TE04.43.02, TE04.44.02, TE04.56.02 (L1 only)	TE04.37.02, TE04.38.02, TE04.45.02, TE04.45.02, TE04.45.03, TE04.52.01, TE04.53.01 (L2 only), TE04.54.02, TE04.54.03, TE04.55.02	TE04.39.02, TE04.39.03, TE04.39.04, TE04.42.03, TE04.42.04	TE04.59.01

FIPS 140-3 Section Name	TEs for SL 1-4	TEs for SL 2-4	TEs for SL 3-4	TEs for SL 4
Software/ Firmware Security	TE05.05.05, TE05.05.07, TE05.06.02, TE05.06.03, TE05.06.04, TE05.06.06, TE05.07.01, TE05.08.01, TE05.08.02, TE05.11.01, TE05.11.02, TE05.12.02, TE05.13.01, TE05.13.02, TE05.13.03, TE05.13.04, TE05.13.05, TE05.13.06, TE05.13.08	TE05.15.01, TE05.15.02, TE05.16.03, TE05.17.02	TE05.20.01, TE05.23.01	none
Operational Environment	TE06.05.01, TE06.05.02, TE06.05.03, TE06.06.01, TE06.06.02, TE06.08.01, TE06.08.02, TE06.08.03	The following TEs are for L2 only: TE06.09.02, TE06.09.03, TE06.10.01, TE06.10.02, TE06.10.03, TE06.11.01, TE06.11.02, TE06.11.03, TE06.12.01, TE06.12.02, TE06.12.03, TE06.13.01, TE06.13.02, TE06.13.03, TE06.14.01, TE06.14.02, TE06.14.03, TE06.15.01, TE06.15.02, TE06.15.03, TE06.17.01, TE06.17.02, TE06.17.03, TE06.18.01, TE06.18.02, TE06.18.03, TE06.24.01, TE06.25.01, TE06.25.02, TE06.26.01, TE06.26.02, TE06.27.01, TE06.27.02, TE06.28.01, TE06.28.02, TE06.28.03, TE06.28.04	None	None
Physical Security	TE07.01.02, TE07.10.02, TE07.11.02, TE07.13.01, TE07.15.01, TE07.37.01, TE07.43.01, TE07.60.01	TE07.19.01, TE07.20.01, TE07.35.01, TE07.44.01, TE07.45.01, TE07.45.02, TE07.46.01, TE07.47.01, TE07.47.02, TE07.48.01, TE07.48.02, TE07.62.01, TE07.63.01	TE07.25.01, TE07.26.01, TE07.27.01, TE07.37.03, TE07.39.03, TE07.39.04, TE07.39.05, TE07.39.06, TE07.50.02, TE07.50.03, TE07.51.04, TE07.51.05, TE07.51.06, TE07.51.08, TE07.51.09, TE07.65.04, TE07.65.05, TE07.65.06,	TE07.32.01, TE07.41.01, TE07.41.02, TE07.42.02, TE07.53.01, TE07.55.01, TE07.58.01, TE07.67.01, TE07.71.02

FIPS 140-3 Section Name	TEs for SL 1-4	TEs for SL 2-4	TEs for SL 3-4	TEs for SL 4
			TE07.65.08, TE07.65.09, TE07.77.01, TE07.77.02, TE07.77.03, TE07.81.01, TE07.81.02	
Non-Invasive Security	N/A			
SSP Management	TE09.01.02, TE09.01.03, TE09.02.02, TE09.03.02, TE09.03.03, TE09.13.03, TE09.14.02, TE09.16.03, TE09.18.01, TE09.18.02, TE09.21.02, TE09.21.03, TE09.21.04, TE09.22.01, TE09.24.02, TE09.25.02, TE09.27.02, TE09.28.02, TE09.28.03, TE09.28.04, TE09.33.02, TE09.36.02, TE09.37.02	None	None	None
Self-Tests	TE10.07.03, TE10.07.04, TE10.07.05, TE10.08.03, TE10.09.03, TE10.10.01, TE10.10.02, TE10.11.01, TE10.15.01, TE10.15.02, TE10.21.01, TE10.21.02, TE10.21.03, TE10.21.04, TE10.22.01, TE10.22.04, TE10.25.02, TE10.27.01, TE10.28.02, TE10.34.03, TE10.35.04, TE10.37.05, TE10.37.06, TE10.37.09, TE10.46.03, TE10.46.04, TE10.48.01, TE10.48.03, TE10.49.01, TE10.49.03, TE10.53.02, TE10.53.03		TE10.12.03, TE10.12.04, TE10.12.05, TE10.54.01	
Life-Cycle Assurance	TE11.08.06, TE11.08.09, TE11.11.01, TE11.13.02, TE11.32.02			TE11.28.02, TE11.28.03, TE11.28.04
Mitigation of Other Attacks	N/A			

A.2.1. TE Filters

Table 3 can be used to filter TEs based on module characteristics ("TE Filter Types" in the first column). This table is not an exhaustive list, and more filters could be discovered through use and further feedback.

Table 3 - TE Filter Types and Example TEs within those Filters

TE Filter Types	Sampling of TEs within Filters: Filter Sub-Categories	Sampling of TEs within Filters: Sample TEs within Sub-Categories
Module Type	Hardware	TE11.17.01
	Software	TE11.15.01
	Firmware	TE11.16.01
	Hybrid	TE02.18.01
Security Level	SL 1	TE05.13.01
	SL 2	TE05.17.01
	SL 3	TE03.21.01
	SL 4	TE07.41.01
Embodiment Type		TE07.09.01
Capabilities	Bypass	TE10.22.01
	Self-Initiated Cryptographic	TE04.23.01
SSP	Manual Establishment	TE10.07.01
	Automated Establishment	TE09.10.02
	Wireless Manual Entry/Output	TE09.18.01
	Automated Entry/Output	TE09.03.01
Self-Tests	Comparison Self-Test	TE10.27.01
	Cryptographic Algorithm Self-Tests	TE10.25.01
	Pre-Operational Self-Tests	TE10.53.01
	Comparison Self-Test	TE10.33.01
	Critical Functions	TE10.24.01
Operational Environment Type	Limited	TE06.03.01
	Non-Modifiable	TE06.03.01
	Modifiable	TE06.03.01
Excluded Components		TE02.13.01
Modes of Operation	Approved	TE02.10.01
	Non-Approved	TE02.20.01
	Degraded	TE02.26.01
Interfaces	Data Input	TE03.05.01
	Data Output	TE03.06.01
	Control Input	TE03.08.01

TE Filter Types	Sampling of TEs within Filters: Filter Sub-Categories	Sampling of TEs within Filters: Sample TEs within Sub-Categories
	Control Output	TE03.09.01
	Status Output	TE03.10.01
	Power Input	TE03.13.01
Software/Firmware Loading		TE10.37.01
Complete Image Replacement		TE04.33.01

The CMVP provided Module Supplemental Information (V3.0.0 as of 2024-09-04). While this does capture many filterable items, it is not currently used to filter the set of TEs for the module under test.

The TE WS produces the TETables.json file to reflect the TE classification documented in this paper. The ACMVP server will incorporate the TETables.json file to generate a fitting set of TEs for a given module specification.

The TE WS will work on completing the filter/mapping of TE Filter Types to their respective TEs.

A.2.2. Removing Assertions Not Separately Tested

Some assertions are not separately tested, nor do they depend on the completion of other assertions and their TEs. For example: **AS05.22** is not separately tested, but is instead tested as part of **AS05.05**. Table 4 highlights some assertions which are not separately tested. Since testing these assertions are dependent on testing the assertion(s) that it points to, an approach is to use these assertions to further automate the report writing process. In this instance, the AS that is not separately tested could be marked as completed once the appropriate associated AS, VE, and TE are completed. This automation could take the form of a simple checking mechanic akin to the SP dependent TEs referenced in Table 1.

Table 4 - Assertions not separately tested

FIPS 140-3 Section Title	Assertions Not Separately Tested
General	N/A
Cryptographic Module Specification	AS02.01, AS02.02, AS02.04, AS02.05, AS02.06, AS02.08, AS02.25, AS02.26, AS02.29, AS02.31, AS02.32
Cryptographic Module Interfaces	AS03.12, AS03.17
Roles, Services, and Authentication	AS04.01, AS04.05, AS04.08, AS04.09, AS04.10, AS04.12, AS04.16, AS04.17, AS04.24, AS04.26, AS04.27, AS04.30, AS04.31, AS04.36, AS04.40, AS04.41, AS04.46, AS04.49, AS04.57, AS04.58
Software/Firmware Security	AS05.01, AS05.03, AS05.09, AS05.10, AS05.14, AS05.18, AS05.19, AS05.21, AS05.22
Operational Environment	AS06.01, AS06.02, AS06.04, AS06.09, AS06.16, AS06.21, AS06.22, AS06.23, AS06.29
Physical Security	AS07.02, AS07.03, AS07.04, AS07.05, AS07.06, AS07.07, AS07.08, AS07.14, AS07.16, AS07.17, AS07.18, AS07.21, AS07.22, AS07.23, AS07.24, AS07.28,

FIPS 140-3 Section Title	Assertions Not Separately Tested
	AS07.29, AS07.30, AS07.31, AS07.34, AS07.36, AS07.38, AS07.40, AS07.49, AS07.52, AS07.54, AS07.56, AS07.59, AS07.61, AS07.64, AS07.66, AS07.68, AS07.69, AS07.70, AS07.72, AS07.74, AS07.75, AS07.76, AS07.78, AS07.79, AS07.80, AS07.81, AS07.82, AS07.83, AS07.84, AS07.85, AS07.86
Non-Invasive Security	N/A
Sensitive Security Parameter Management	AS09.11, AS09.12, AS09.15, AS09.17, AS09.20, AS09.26, AS09.30, AS09.34, AS09.35
Self-Tests	AS10.01, AS10.02, AS10.03, AS10.04, AS10.05, AS10.06, AS10.13, AS10.14, AS10.16, AS10.17, AS10.18, AS10.19, AS10.23, AS10.26, AS10.30, AS10.31, AS10.32, AS10.32, AS10.36, AS10.38, AS10.39, AS10.40, AS10.41, AS10.42, AS10.43, AS10.44, AS10.45, AS10.47, AS10.50, AS10.52, AS10.55
Life-Cycle Assurance	AS11.02, AS11.07, AS11.09, AS11.10, AS11.12, AS11.14, AS11.20, AS11.22, AS11.27
Mitigation of Other Attacks	None

A.3. Complete List of TEs

Table 5 provides a complete list of TEs, classified into four categories (i.e., SP-TE, OD-TE, SC-TC, FT-TE) and their potential combinations:

- **SP-TE:** TEs depending on the SP
- **SC-TE:** TEs depending on source code review or inspection
- **OD-TE:** TEs depending on other vendor documentation
- **FT-TE:** TEs depending on functional testing
- **SP-TE/OD-TE:** TEs depending on vendor documentation, regardless whether it is SP or not
- **SC-TE/SP-TE:** TEs depending on source code review or on the SP
- **SP-TE, FT-TE:** TE depending on the SP and on functional testing
- **SC-TE, FT-TE:** TE depending on source code review and on functional testing

Greyed-out TEs marked with an asterisk are those not currently required by the CMVP.

The OD-TEs depend on proprietary vendor documentation. Therefore, they do not belong to the SP-TE category.

Examples:

- FT-TE:
    - The tester shall verify, by exercising the module, that the status indicator is provided when the trusted channel is in use. (e.g., TE03.21.01)
    - The tester shall verify that an identity-based authentication mechanism is employed for all services utilizing the trusted channel. (e.g., TE03.20.01)

- SP-TE, FT-TE or SP-TE/OD-TE, FT-TE:
    - The tester shall use the vendor documentation to assess multi-factor identity-based authentication. (e.g., TE04.59.01)
    - The tester shall verify from the vendor documentation and by inspection that the approved authentication mechanism implemented in the operating system meets the applicable requirements. (TE04.53.01)
- FT-TE, SP-TE or FT-TE, SP-TE/ OD-TE:
    - The tester shall invoke the approved mode of operation using the vendor provided instructions found in the non-proprietary security policy. (e.g., TE02.19.02)
    - The tester shall verify that the module implements a bypass capability as specified in the vendor documentation. (e.g., TE04.18.01)

Table 5 - A complete list of TEs

TE02.03.01	**SP-TE**	**TE02.15.12**	SP-TE	**TE02.21.01**	SP-TE
TE02.03.02	SP-TE/OD-TE	**TE02.15.13**	SP-TE	**TE02.21.02**	SP-TE
TE02.07.01	SC-TE, SP-TE	**TE02.15.14**	SP-TE	**TE02.22.01**	SP-TE
TE02.07.02	SC-TE, SP-TE	**TE02.16.01**	SP-TE	**TE02.22.02**	FT-TE
TE02.09.01	SP-TE	**TE02.16.02**	SP-TE	**TE02.24.01**	SP-TE
TE02.10.01	SP-TE, SC-TE/FT-TE	**TE02.16.03**	SP-TE	**TE02.24.02**	FT-TE
TE02.10.02	SP-TE/OD-TE	**TE02.16.04**	FT-TE	**TE02.26.01**	SP-TE
TE02.11.01	SP-TE	**TE02.16.05**	SP-TE	**TE02.26.02**	SP-TE
TE02.11.02	SP-TE	**TE02.17.01**	SP-TE	**TE02.26.03**	FT-TE
TE02.12.01	SP-TE, FT-TE	**TE02.17.02**	SP-TE, FT-TE	**TE02.26.04**	FT-TE
TE02.13.01	SP-TE	**TE02.17.03**	SP-TE	**TE02.26.05**	FT-TE
TE02.13.02	SP-TE/OD-TE	**TE02.17.04**	FT-TE	**TE02.28.01**	FT-TE
TE02.13.03	FT-TE	**TE02.17.05**	SP-TE	**TE02.28.02**	FT-TE
TE02.14.01	SP-TE	**TE02.17.06**	SP-TE	**TE02.30.01**	SP-TE
TE02.15.01	SP-TE	**TE02.17.07**	SP-TE	**TE02.30.02**	FT-TE
TE02.15.02	SP-TE	**TE02.17.08**	SP-TE	**TE03.01.01**	SP-TE
TE02.15.03	FT-TE	**TE02.17.09**	SP-TE/OD-TE	**TE03.01.02**	SP-TE, SC-TE
TE02.15.04	SP-TE	**TE02.17.10**	SP-TE	**TE03.01.03**	SP-TE
TE02.15.05	FT-TE	**TE02.18.01**	SP-TE	**TE03.01.04**	FT-TE
TE02.15.06	SP-TE	**TE02.19.01**	SP-TE	**TE03.02.01**	SC-TE, FT-TE
TE02.15.07	SP-TE	**TE02.19.02**	FT-TE, SP-TE	**TE03.02.02**	SP-TE
TE02.15.08	SP-TE	**TE02.20.01**	SP-TE	**TE03.03.01**	SP-TE
TE02.15.09	SP-TE	**TE02.20.02**	SP-TE	**TE03.04.01**	SP-TE
TE02.15.10	SP-TE	**TE02.20.03**	SP-TE	**TE03.05.01**	FT-TE
TE02.15.11	SP-TE	**TE02.20.04**	SP-TE	**TE03.05.02**	SP-TE/OD-TE, FT-TE

TE03.06.01	FT-TE
TE03.06.02	SP-TE/OD-TE, FT-TE
TE03.07.01	SP-TE/OD-TE
TE03.07.02	FT-TE
TE03.07.03	SP-TE/OD-TE
TE03.07.04	FT-TE
TE03.07.05	SP-TE/OD-TE, SC-TE
TE03.07.06	SP-TE/OD-TE
TE03.07.07	SP-TE/OD-TE
TE03.07.08	FT-TE
TE03.08.01	FT-TE
TE03.08.02	FT-TE, SP-TE/OD-TE
TE03.09.01	SP-TE/OD-TE
TE03.09.02	FT-TE
TE03.10.01	SP-TE/OD-TE
TE03.10.02	FT-TE
TE03.10.03	SP-TE/OD-TE
TE03.10.04	FT-TE
TE03.10.05	SC-TE/OD-TE
TE03.11.01	FT-TE
TE03.11.02	SP-TE/OD-TE
TE03.11.03	FT-TE
TE03.13.01	SP-TE/OD-TE
TE03.13.02	FT-TE
TE03.14.01	SC-TE/OD-TE
TE03.14.02	SC-TE/OD-TE
TE03.14.03	FT-TE, SC-TE
TE03.15.01	SP-TE/OD-TE
TE03.15.02	FT-TE, SC-TE
TE03.15.03	FT-TE
TE03.15.04	FT-TE
TE03.15.05	SC-TE
TE03.15.06	FT-TE
TE03.16.01	SP-TE/OD-TE, SC-TE/FT-TE
TE03.18.01	SP-TE/OD-TE, FT-TE
TE03.18.02	FT-TE
TE03.19.01	SP-TE/OD-TE, SC-TE
TE03.19.02	FT-TE
TE03.19.03	SP-TE/OD-TE
TE03.19.04	FT-TE
TE03.20.01	FT-TE
TE03.21.01	FT-TE
TE03.22.01	FT-TE
TE04.02.01	SP-TE/OD-TE
TE04.02.02	FT-TE
TE04.02.03	FT-TE
TE04.03.01	SP-TE/OD-TE
TE04.05.01	SP-TE
TE04.06.01	SP-TE
TE04.07.01	SP-TE/OD-TE
TE04.07.02	SP-TE/OD-TE
TE04.07.03	FT-TE
TE04.11.01	SP-TE
TE04.11.02	FT-TE
TE04.13.01	FT-TE
TE04.13.02	SP-TE
TE04.13.03	FT-TE
TE04.14.01	SP-TE
TE04.14.02	FT-TE
TE04.15.01	FT-TE
TE04.18.01	FT-TE, SP-TE/OD-TE
TE04.19.01	SP-TE/OD-TE
TE04.19.02	FT-TE
TE04.19.03	FT-TE
TE04.20.01	FT-TE, SP-TE/OD-TE
TE04.20.02	OD-TE
TE04.20.03	FT-TE
TE04.21.01	SP-TE/OD-TE
TE04.21.02	FT-TE
TE04.22.01	SP-TE/OD-TE
TE04.22.02	FT-TE
TE04.23.01	FT-TE
TE04.25.01	SP-TE/OD-TE
TE04.25.02	FT-TE
TE04.25.03	FT-TE
TE04.28.01	FT-TE
TE04.29.01	FT-TE
TE04.32.01	FT-TE
TE04.33.01	FT-TE, SP-TE/OD-TE
TE04.34.01	FT-TE
TE04.35.01	SP-TE/OD-TE
TE04.35.02	FT-TE
TE04.37.01	SP-TE
TE04.37.02	FT-TE
TE04.38.01	SP-TE/OD-TE
TE04.38.02	FT-TE
TE04.39.01	SP-TE/OD-TE
TE04.39.02	FT-TE
TE04.39.03	FT-TE
TE04.39.04	FT-TE
TE04.42.01	SP-TE/OD-TE
TE04.42.02	SP-TE/OD-TE
TE04.42.03	FT-TE
TE04.42.04	FT-TE
TE04.43.01	SP-TE/OD-TE
TE04.43.02	FT-TE
TE04.44.01	SP-TE/OD-TE
TE04.44.02	FT-TE
TE04.45.01	SP-TE/OD-TE
TE04.45.02	FT-TE
TE04.45.03	FT-TE
TE04.47.01	SP-TE
TE04.48.01	SP-TE
TE04.50.01	SP-TE
TE04.50.02	SP-TE
TE04.51.01	SP-TE
TE04.51.02	SP-TE
TE04.52.01	SP-TE/OD-TE, FT-TE
TE04.53.01	SP-TE/OD-TE, FT-TE
TE04.54.01	SP-TE/OD-TE
TE04.54.02	FT-TE
TE04.54.03	FT-TE
TE04.55.01	SP-TE/OD-TE
TE04.55.02	FT-TE
TE04.56.01	SP-TE
TE04.56.02	FT-TE
TE04.59.01	SP-TE, FT-TE

TE05.02.01	SP-TE/OD-TE
TE05.04.01	SC-TE
TE05.05.01	SC-TE
TE05.05.02	SP-TE
TE05.05.03	SP-TE/OD-TE
TE05.05.04	SP-TE/OD-TE
TE05.05.05	FT-TE
TE05.05.06	SC-TE/OD-TE
TE05.05.07	FT-TE
TE05.06.01	SC-TE
TE05.06.02	FT-TE
TE05.06.03	FT-TE
TE05.06.04	FT-TE
TE05.06.05	SC-TE
TE05.06.06	FT-TE
TE05.07.01	SP-TE/OD-TE, FT-TE
TE05.08.01	FT-TE
TE05.08.02	FT-TE, SC-TE
TE05.11.01	FT-TE
TE05.11.02	FT-TE
TE05.12.01	SP-TE/OD-TE
TE05.12.02	FT-TE, SP-TE/OD-TE
TE05.13.01	FT-TE, SP-TE/OD-TE
TE05.13.02	FT-TE, SP-TE/OD-TE
TE05.13.03	FT-TE
TE05.13.04	FT-TE, SP-TE/OD-TE
TE05.13.05	FT-TE
TE05.13.06	FT-TE, SP-TE/OD-TE
TE05.13.07	SC-TE/OD-TE
TE05.13.08	FT-TE
TE05.15.01	FT-TE, SP-TE/OD-TE
TE05.15.02	FT-TE, SP-TE/OD-TE
TE05.16.01	SP-TE/OD-TE
TE05.16.02	SP-TE/OD-TE
TE05.16.03	FT-TE
TE05.17.01	SP-TE
TE05.17.02	FT-TE
TE05.20.01	SC-TE, FT-TE
TE05.23.01	FT-TE, SP-TE/OD-TE
TE06.03.01	SP-TE/OD-TE
TE06.05.01	SP-TE/OD-TE, FT-TE
TE06.05.02	SP-TE/OD-TE, FT-TE
TE06.05.03	FT-TE
TE06.06.01	SP-TE/OD-TE, FT-TE
TE06.06.02	FT-TE
TE06.07.01	SP-TE
TE06.08.01	SP-TE/OD-TE, FT-TE
TE06.08.02	SP-TE/OD-TE, FT-TE
TE06.08.03	FT-TE
TE06.09.01	SP-TE
TE06.09.02	FT-TE
TE06.09.03	FT-TE
TE06.10.01	SP-TE/OD-TE, FT-TE
TE06.10.02	FT-TE
TE06.10.03	FT-TE
TE06.11.01	SP-TE/OD-TE, FT-TE
TE06.11.02	FT-TE
TE06.11.03	FT-TE
TE06.12.01	SP-TE/OD-TE, FT-TE
TE06.12.02	FT-TE
TE06.12.03	FT-TE
TE06.13.01	SP-TE/OD-TE, FT-TE
TE06.13.02	FT-TE
TE06.13.03	FT-TE
TE06.14.01	SP-TE/OD-TE, FT-TE
TE06.14.02	FT-TE
TE06.14.03	FT-TE
TE06.15.01	SP-TE/OD-TE, FT-TE
TE06.15.02	FT-TE
TE06.15.03	FT-TE
TE06.17.01	SP-TE/OD-TE, FT-TE
TE06.17.02	FT-TE
TE06.17.03	FT-TE
TE06.18.01	SP-TE/OD-TE, FT-TE
TE06.18.02	FT-TE
TE06.18.03	FT-TE
TE06.19.01	SP-TE/OD-TE
TE06.20.01	SP-TE
TE06.24.01	SP-TE/OD-TE, FT-TE
TE06.25.01	SP-TE/OD-TE, FT-TE
TE06.25.02	FT-TE
TE06.26.01	SP-TE/OD-TE, FT-TE
TE06.26.02	FT-TE
TE06.27.01	SP-TE/OD-TE, FT-TE
TE06.27.02	FT-TE
TE06.28.01	SP-TE/OD-TE, FT-TE
TE06.28.02	FT-TE
TE06.28.03	FT-TE
TE06.28.04	FT-TE
TE07.01.01	SP-TE
TE07.01.02	FT-TE
TE07.09.01	SP-TE
TE07.09.02	SP-TE
TE07.10.01	SP-TE/OD-TE
TE07.10.02	FT-TE
TE07.11.01	SP-TE/OD-TE
TE07.11.02	FT-TE
TE07.12.01	SP-TE/OD-TE
TE07.13.01	FT-TE
TE07.15.01	FT-TE, SP-TE/OD-TE
TE07.15.02	SP-TE/OD-TE
TE07.19.01	FT-TE, SP-TE/OD-TE
TE07.20.01	FT-TE, SP-TE/OD-TE
TE07.25.01	FT-TE, SP-TE/OD-TE
TE07.26.01	SP-TE/OD-TE FT-TE
TE07.26.02	SP-TE
TE07.27.01	FT-TE
TE07.32.01	SP-TE/OD-TE, FT-TE
TE07.33.01	SP-TE/OD-TE
TE07.35.01	FT-TE, SP-TE/OD-TE
TE07.37.01	FT-TE, SP-TE/OD-TE
TE07.37.02	SP-TE/OD-TE
TE07.37.03	FT-TE
TE07.39.01	SP-TE/OD-TE
TE07.39.02	SP-TE/OD-TE
TE07.39.03	FT-TE, SP-TE/OD-TE
TE07.39.04	FT-TE, SP-TE/OD-TE

TE07.39.05	FT-TE
TE07.39.06	FT-TE
TE07.41.01	FT-TE, SP-TE/OD-TE
TE07.41.02	FT-TE
TE07.42.01	SP-TE/OD-TE
TE07.42.02	FT-TE
TE07.43.01	FT-TE, SP-TE/OD-TE
TE07.44.01	FT-TE, SP-TE/OD-TE
TE07.45.01	FT-TE, SP-TE/OD-TE
TE07.45.02	FT-TE
TE07.46.01	FT-TE, SP-TE/OD-TE
TE07.47.01	FT-TE, SP-TE/OD-TE
TE07.47.02	FT-TE
TE07.48.01	FT-TE, SP-TE/OD-TE
TE07.48.02	FT-TE
TE07.50.01	SP-TE/OD-TE
TE07.50.02	FT-TE, SP-TE/OD-TE
TE07.50.03	FT-TE, SP-TE/OD-TE
TE07.51.01	SP-TE/OD-TE
TE07.51.02	SP-TE/OD-TE
TE07.51.03	SP-TE/OD-TE
TE07.51.04	FT-TE, SP-TE/OD-TE
TE07.51.05	FT-TE, SP-TE/OD-TE
TE07.51.06	FT-TE
TE07.51.07	SP-TE/OD-TE
TE07.51.08	FT-TE
TE07.51.09	FT-TE
TE07.53.01	SP-TE/OD-TE, FT-TE
TE07.55.01	SP-TE/OD-TE, FT-TE
TE07.57.01	SP-TE/OD-TE
TE07.58.01	FT-TE
TE07.60.01	FT-TE, SP-TE/OD-TE
TE07.62.01	FT-TE
TE07.63.01	FT-TE
TE07.65.01	SP-TE/OD-TE
TE07.65.02	SP-TE/OD-TE
TE07.65.03	SP-TE/OD-TE
TE07.65.04	FT-TE, SP-TE/OD-TE
TE07.65.05	FT-TE, SP-TE/OD-TE
TE07.65.06	FT-TE, SP-TE/OD-TE
TE07.65.07	SP-TE/OD-TE
TE07.65.08	FT-TE
TE07.65.09	FT-TE
TE07.67.01	SP-TE/OD-TE, FT-TE
TE07.71.01	SP-TE/OD-TE
TE07.71.02	FT-TE
TE07.73.01	SP-TE/OD-TE
TE07.77.01	FT-TE
TE07.77.02	FT-TE
TE07.77.03	FT-TE
TE07.77.04	SP-TE
TE07.81.01	FT-TE
TE07.81.02	FT-TE
TE07.81.03	SP-TE
TE08.03.01	SP-TE/OD-TE*
TE08.04.01	SP-TE/OD-TE*
TE08.05.01	SP-TE/OD-TE*
TE08.06.01	SP-TE/OD-TE*
TE08.07.01	SP-TE/OD-TE*
TE09.01.01	SP-TE/OD-TE
TE09.01.02	FT-TE
TE09.01.03	FT-TE
TE09.02.01	SP-TE/OD-TE
TE09.02.02	FT-TE
TE09.03.01	SP-TE/OD-TE
TE09.03.02	FT-TE
TE09.03.03	FT-TE
TE09.04.01	SP-TE
TE09.04.02	SP-TE
TE09.05.01	SP-TE/OD-TE
TE09.06.01	SP-TE
TE09.06.02	SP-TE
TE09.06.03	SP-TE
TE09.07.01	SP-TE
TE09.08.01	SP-TE
TE09.08.02	SP-TE/OD-TE
TE09.09.01	SP-TE
TE09.09.02	SP-TE
TE09.10.01	SP-TE
TE09.10.02	SP-TE
TE09.13.01	SP-TE
TE09.13.02	SP-TE
TE09.13.03	FT-TE
TE09.14.01	SP-TE/OD-TE
TE09.14.02	FT-TE
TE09.16.01	SP-TE/OD-TE
TE09.16.02	SP-TE/OD-TE
TE09.16.03	FT-TE
TE09.18.01	FT-TE
TE09.18.02	FT-TE
TE09.19.01	SP-TE
TE09.21.01	SP-TE/OD-TE
TE09.21.02	FT-TE
TE09.21.03	FT-TE
TE09.21.04	FT-TE
TE09.22.01	FT-TE
TE09.23.01	SP-TE/OD-TE
TE09.23.02	SP-TE/OD-TE
TE09.23.04	SP-TE/OD-TE
TE09.24.01	SP-TE/OD-TE
TE09.24.02	FT-TE
TE09.25.01	SP-TE/OD-TE
TE09.25.02	FT-TE
TE09.27.01	SP-TE/OD-TE
TE09.27.02	FT-TE
TE09.28.01	SP-TE
TE09.28.02	FT-TE
TE09.28.03	FT-TE
TE09.28.04	FT-TE
TE09.28.05	SP-TE
TE09.28.06	SP-TE/OD-TE
TE09.29.01	SP-TE/OD-TE
TE09.29.02	SP-TE/OD-TE
TE09.31.01	SP-TE/OD-TE
TE09.32.01	SP-TE/OD-TE
TE09.33.01	SP-TE
TE09.33.02	FT-TE

TE09.36.01	SP-TE/OD-TE
TE09.36.02	FT-TE
TE09.37.01	SP-TE
TE09.37.02	FT-TE
TE10.07.01	SP-TE
TE10.07.02	SP-TE
TE10.07.03	FT-TE
TE10.07.04	FT-TE
TE10.07.05	FT-TE/SC-TE
TE10.08.01	SP-TE
TE10.08.02	SP-TE
TE10.08.03	FT-TE
TE10.09.01	SP-TE
TE10.09.02	SP-TE
TE10.09.03	FT-TE
TE10.10.01	FT-TE
TE10.10.02	FT-TE
TE10.11.01	FT-TE
TE10.12.01	SP-TE/OD-TE
TE10.12.02	SP-TE/OD-TE
TE10.12.03	FT-TE
TE10.12.04	FT-TE
TE10.12.05	FT-TE
TE10.15.01	SP-TE/OD-TE, FT-TE
TE10.15.02	SC-TE/OD-TE, FT-TE
TE10.20.01	SC-TE/OD-TE
TE10.21.01	SP-TE/OD-TE, FT-TE
TE10.21.02	FT-TE, SP-TE/OD-TE
TE10.21.03	FT-TE
TE10.21.04	FT-TE
TE10.22.01	FT-TE
TE10.22.02	SC-TE/OD-TE
TE10.22.03	SC-TE/OD-TE
TE10.22.04	FT-TE
TE10.22.05	SC-TE/OD-TE
TE10.24.01	SP-TE
TE10.24.02	SC-TE/OD-TE
TE10.25.01	SP-TE
TE10.25.02	FT-TE
TE10.27.01	FT-TE, SP-TE/OD-TE
TE10.28.01	SP-TE/OD-TE, SC-TE
TE10.28.02	FT-TE
TE10.29.01	SC-TE, SP-TE/OD-TE
TE10.33.01	SP-TE
TE10.33.02	SC-TE/OD-TE
TE10.34.01	SP-TE
TE10.34.02	SP-TE/OD-TE, SC-TE
TE10.34.03	FT-TE
TE10.35.01	SP-TE/OD-TE, SC-TE
TE10.35.02	SP-TE/OD-TE, SC-TE
TE10.35.03	SP-TE/OD-TE, SC-TE
TE10.35.04	FT-TE
TE10.37.01	SP-TE
TE10.37.02	SP-TE
TE10.37.03	SP-TE/OD-TE
TE10.37.04	SC-TE/OD-TE
TE10.37.05	FT-TE
TE10.37.06	FT-TE
TE10.37.07	SC-TE/OD-TE
TE10.37.08	SC-TE/OD-TE
TE10.37.09	FT-TE
TE10.46.01	SP-TE/OD-TE
TE10.46.02	SC-TE, SP-TE/OD-TE
TE10.46.03	FT-TE
TE10.46.04	FT-TE
TE10.48.01	FT-TE
TE10.48.02	SC-TE, SP-TE/OD-TE
TE10.48.03	FT-TE
TE10.49.01	FT-TE
TE10.49.02	SC-TE, SP-TE/OD-TE
TE10.49.03	FT-TE
TE10.51.01	SC-TE, SP-TE/OD-TE
TE10.51.02	SC-TE, SP-TE/OD-TE
TE10.51.03	SC-TE, SP-TE/OD-TE
TE10.53.01	SP-TE
TE10.53.02	FT-TE
TE10.53.03	FT-TE
TE10.54.01	FT-TE, SC-TE
TE11.01.01	SP-TE/OD-TE
TE11.03.01	SP-TE/OD-TE
TE11.04.01	SP-TE/OD-TE
TE11.04.02	SP-TE/OD-TE
TE11.04.03	SP-TE/OD-TE
TE11.04.04	SP-TE/OD-TE
TE11.05.01	SP-TE/OD-TE
TE11.06.01	SP-TE/OD-TE
TE11.08.01	OD(FSM)-TE
TE11.08.02	OD(FSM)-TE
TE11.08.03	OD(FSM)-TE
TE11.08.04	OD(FSM)-TE
TE11.08.05	OD(FSM)-TE
TE11.08.06	FT-TE
TE11.08.07	OD(FSM)-TE
TE11.08.08	OD(FSM)-TE
TE11.08.09	FT-TE
TE11.08.10	OD(FSM)-TE
TE11.08.11	OD(FSM)-TE
TE11.08.12	OD(FSM)-TE
TE11.11.01	FT-TE
TE11.13.01	OD(FSM)-TE
TE11.13.02	FT-TE
TE11.15.01	SP-TE/OD-TE
TE11.15.02	SP-TE/OD-TE
TE11.16.01	SC-TE/OD-TE
TE11.17.01	SC-TE/OD-TE
TE11.18.01	SC-TE/OD-TE
TE11.19.01	SP-TE/OD-TE
TE11.21.01	SP-TE/OD-TE
TE11.23.01	SP-TE/OD-TE
TE11.24.01	SC-TE
TE11.25.01	SP-TE/OD-TE
TE11.26.01	SP-TE/OD-TE
TE11.28.01	SC-TE
TE11.28.02	FT-TE, SC-TE
TE11.28.03	FT-TE, SC-TE
TE11.28.04	FT-TE
TE11.29.01	SP-TE/OD-TE

TE11.29.02	SP-TE/OD-TE	**TE11.36.01**	SP-TE	**TE12.04.02**	SP-TE/OD-TE		
TE11.30.01	SP-TE/OD-TE	**TE11.37.01**	SP-TE	**TE12.04.03**	SP-TE		
TE11.31.01	SP-TE/OD-TE	**TE11.38.01**	SP-TE	**TEA01.01**	SP-TE/OD-TE		
TE11.32.01	SP-TE	**TE11.38.03**	SP-TE/OD-TE	**TEB01.01**	SP-TE		
TE11.32.02	FT-TE	**TE11.39.01**	SP-TE	**TEB02.01**	SP-TE		
TE11.33.01	SP-TE/OD-TE	**TE12.01.01**	SP-TE/OD-TE	**TEB03.01**	SP-TE		
TE11.34.01	SP-TE/OD-TE	**TE12.02.01**	SP-TE	**TEB03.02**	SP-TE		
TE11.35.01	SP-TE	**TE12.04.01**	SP-TE				

The CMVP currently does not enforce the grayed-out TEs in area eight (see TEs below).

- TE08.03.01 SP-TE/OD-TE*
- TE08.04.01 SP-TE/OD-TE*
- TE08.05.01 SP-TE/OD-TE*
- TE08.06.01 SP-TE/OD-TE*
- TE08.07.01 SP-TE/OD-TE*

Appendix B. List of Symbols, Abbreviations, and Acronyms

140A-TE
Vendor-documentation-dependent Test Evidence

ACMVP/ACVP
Automated Cryptographic Module Validation Project

AS
Assertion

CAVP
Cryptographic Algorithm Validation Program

CL
Component List

CMVP
Cryptographic Module Validation Program

CRADA
Cooperative Research and Development Agreement

ESV
Entropy Source Validation

ESVP
Entropy Source Validation Program

FIPS
Federal Information Processing Standards

FSM
Finite State Model

FT
Functional Test

IUT
Implementation Under Test

MIS
Module Information Structure

NCCoE
National Cybersecurity Center of Excellence

NVLAP
National Voluntary Laboratory Accreditation Program

OD
Other Documents

SC
Source Code

SP
Security Policy

SSP
Sensitive Security Parameter

TE
Test Evidence

VE
Vendor Evidence

WS
Workstream

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:
Celi C, Calis A, Souppaya M, Barker W, Scarfone K, Gabiam R, Mao Y, Fussel B, Karcher A, Boldt D (2024) Automation of the NIST Cryptographic Module Validation Program: September 2024 Status Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 37 ipd. https://doi.org/10.6028/NIST.CSWP.37.ipd

Author ORCID iDs
Chris Celi: 0000-0001-9979-6819
Alex Calis: 0000-0003-1937-8129
Murugiah Souppaya: 0000-0002-8055-8527
William Barker: 0000-0002-4113-8861
Karen Scarfone: 0000-0001-6334-9486

Public Comment Period
October 31, 2024 - December 2, 2024

Submit Comments
applied-crypto-testing@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at Automation of the NCCoE's NIST Cryptographic Module Validation Program project page, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).