National Institute of Standards and Technology
U.S. Department of Commerce

Cryptographic Module Validation Program (CMVP) Status and Future Plans

21 January 2026

David Hawes, CMVP Program Manager
Security Testing, Validation and Measurements Group
Computer Security Division/Information Technology Lab/NIST

Outline

- FIPS 140 Conformance Validation – Background
- FIPS 140 Conformance Validation – Previous Approach
- Queue Issues Created
- Queue Reducing Projects & Results
- Future CMVP Challenges

Conformance Validation - Background

The FIPS 140 Standard is Large

- ISO 19790 is 85 pages
- ISO 24759 (associated test requirements) has ~650 test/evidence item pairs
- Over 30% is related to correctly describing cryptographic related functionality

The FIPS 140 Standard is Broad - Modules come in many shapes and sizes

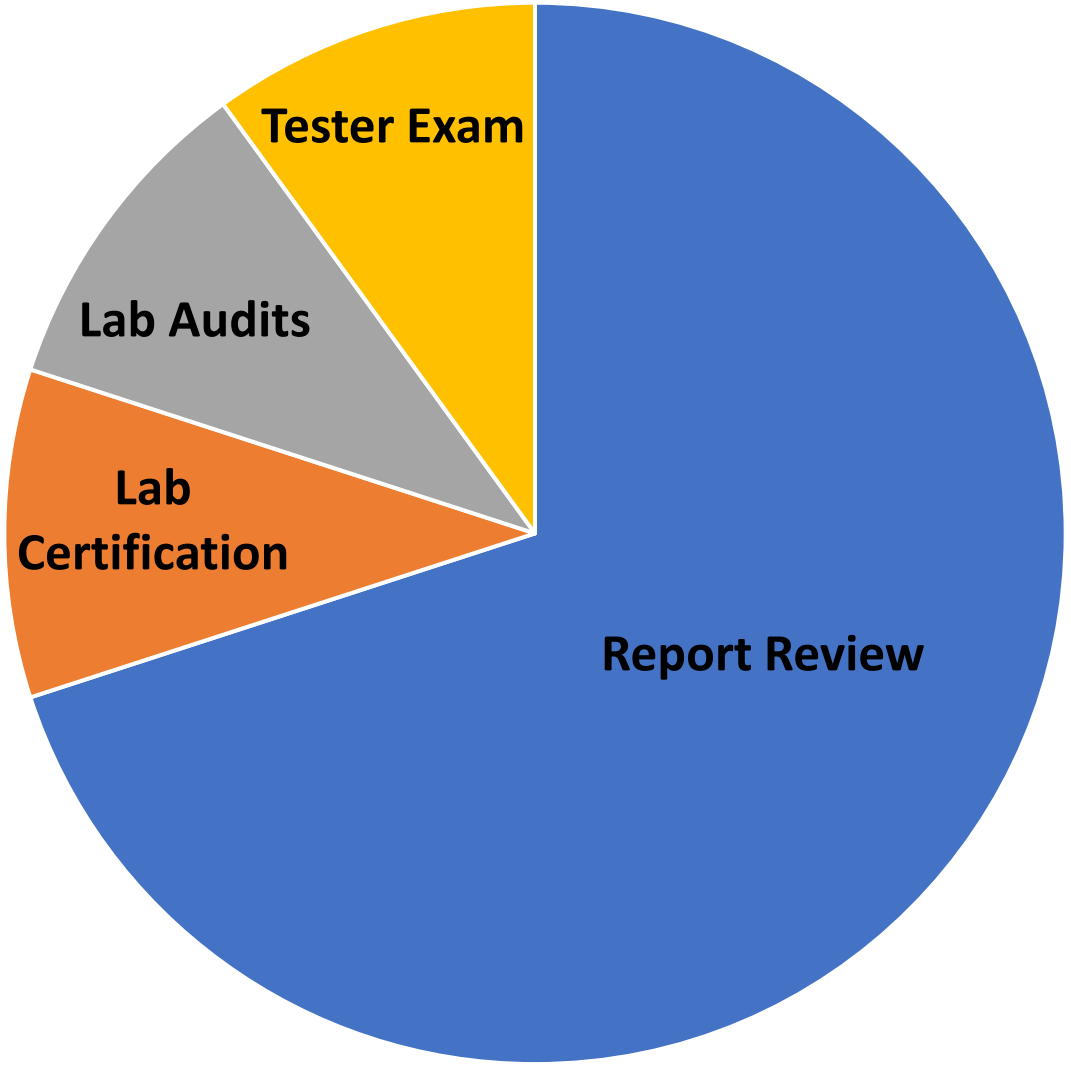
- Types: Hardware, Software, Firmware, Hybrid
- Boundary Definitions: Entire Devices, Cryptographic Components, Libraries, Specific Algorithm Implementations, etc.

- Conformance Testing by Certified Laboratories is Complex
  - CMVP Validation of Conformance Testing is Challenging

Conformance Validation – Previous Approach

How to provide trust that modules conform to the standard?

- Emphasis on Report Review
  - Two Reviews – NIST and CCCS
- Manhours Required to Scale
  - Unstructured information (PDF) led to manual processes
  - Multiple representations of information led to tedious and editorial work
- Report review was performed by junior personnel
  - Inconsistent results



Queue Issues Created

Total Submitted Modules Increased

Algorithm and Entropy Standards Changed – Hard End Dates

- SP800-90B – Entropy (Nov 2020)
- SP800-56Ar3 – Key Agreement (Dec 2020)

FIPS 140-3 (Sep 2021)

- Based on ISO Standards
- New module and report submission system

Queue Time -> Greater than 2 years, after lab testing

Queue Reducing Projects

Separate and Reusable Entropy Validation – 2021

Structured and Reusable Cryptographic Description – 2023/2024

- Reduce editorial errors
- Provide well-defined data descriptions
- Utilizing existing algorithm testing results
- Automate cryptographic configuration conformance
- Automate filtering of requirements to specific implementation

Queue Reducing Projects Continued

Standardize public Security Policy document

Structured and Shared Report Review Checklist

- Filtered related to module type

Report Review Process Changes

- All CMVP personnel involved
- Targeted review areas
  - Initial and POC
  - Security Priority Levels
  - Weekly Meetings

Queue Reducing Results & Future

Results

- As of January 1, 2026, queue backlog is 180 days
- Average of last 30 validations: 348 days
- Near-Zero Backlog Goal: July 1st, 2026

Future

- Expand structure and automated validation
- Create template structure sets for similar cryptographic functionality
- Move trust and assurance activities to certification, audits, etc.

Future CMVP Challenges

Need to move from reactive to proactive

- New version of ISO standards was published in 2025
- Increase participation in ISO standard updates
- Earlier guidance for algorithm transitions
- Greater outreach to customers and vendors to keep up with technology changes

Create personnel and funding stability

- We receive significant funding through validation cost recovery
- Significant decrease of federal employees over the past three years
- Three of those recently from VERA/VSIP actions

Questions and Comments