U.S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
633 3rd Street NW, Suite 200
Washington, DC 20001

Policy Memorandum

Use of Historical Federal Information Processing Standard (FIPS) 140-2 Cryptographic Modules

Issued by Program Director on June 23, 2026

Authority

The U.S. Election Assistance Commission (EAC) is authorized under the Help America Vote Act of 2002 (HAVA), 52 U.S.C. § 20971, to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. Pursuant to this authority, the EAC administers the Voting System Testing and Certification Program and has the responsibility to ensure that voting systems certified under the Voluntary Voting System Guidelines (VVSG) meet applicable federal standards. This authority includes the Program's operations and administrative requirements for voting system testing and certification. This policy memorandum is issued under that authority to provide interim administrative guidance during the ongoing transition from FIPS 140-2 to FIPS 140-3 validation standards.

Purpose

The purpose of this policy memorandum is to provide guidance for voting systems submitted under VVSG 2.0 that include cryptographic modules validated under FIPS 140-2 during the ongoing Cryptographic Module Validation Program (CMVP) transition to FIPS 140-3.

Scope

This policy may be applied to any voting system application submitted to the EAC for evaluation to VVSG 2.0 prior to January 1, 2027, and accepted for testing in accordance with EAC policy, that contains a 140-2 cryptographic module that has transitioned to "Historic" status prior to the completion of testing. Starting January 1, 2027, all systems submitted to the EAC for testing to VVSG 2.0 must utilize a cryptographic module with an "Active" CMVP designation. Modules listed as "Revoked" are expressly prohibited.

U.S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
633 3rd Street NW, Suite 200
Washington, DC 20001

Background

The CMVP, jointly operated by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security, as of September 22, 2020, began validating cryptographic modules to FIPS 140-3 security requirements. In addition, the CMVP stopped accepting cryptographic modules submissions for new validation certificates against FIPS 140-2 security requirements on September 22, 2021. Whether FIPS 140-2 or FIPS 140-3, upon completing cryptographic validation a module remains on the "Active" list for 5 years before automatically moving to the "Historical" list. These events signify that all FIPS 140-2 modules will be moved to the "Historical" list by September 22, 2026.

Discussion

This transition presents a challenge for the EAC's testing and certification program, as the EAC Decision on Request for Interpretation (RFI) 2026-01 requires "Active" FIPS 140 validation cryptographic modules. Manufacturers may have begun development using a cryptographic module that held an "Active" status at the time of development, only for that module to transition to a "Historical" status prior to completion of EAC testing and certification.

Unlike FIPS 140-3, the current standard for security requirements, FIPS 140-2 modules that have transitioned to a "Historical" status are no longer eligible for resubmission or reevaluation under the CMVP. This creates a situation where manufacturers potentially have no available path to restore a module's "Active" status without replacement and further development. The integration of a new cryptographic module into a voting system is costly and time-intensive and cannot be reasonably expected of a manufacturer mid-certification.

While this policy memorandum does not alter the interpretation defined in RFI 2026-01, the EAC recognizes the need to establish a structured review process to determine continued suitability of affected modules for voting system use on a case-by-case basis with the expectation that new voting systems will, in general, strive to move toward adoption of FIPS 140-3.

Evaluation of "Historical" Modules

To support the EAC review of submissions involving "Historical" FIPS 140-2 cryptographic modules, the following manufacturer and VSTL responsibilities apply:

The Manufacturer Responsibilities

Manufacturers choosing to use "Historical" FIPS 140-2 modules must:

- Provide written justification to both the VSTL and EAC at the outset of certification, including rationale and alternatives considered.
- Identify the module's CMVP certificate number and confirmation of its FIPS 140-2 validation and status.
- Provide documentation demonstrating that cryptographic services comply with current NIST cryptographic algorithm standards and guidelines to remain suitable under VVSG.
- Inform the VSTL of planned use and ensure all required testing is completed and documented.
- If applicable, outline and submit a migration plan to FIPS 140-3 modules.
- Clearly identify the "Historical" module in the technical data package (TDP) documentation and include supporting validation and compliance evidence.

The VSTL Responsibilities

Voting System Test Laboratories must:

- Confirm the module was validated under FIPS 140-2 by CMVP.
- Ensure proper integration and operation per the module's security policy.
- Conduct all cryptographic assessments required by VVSG.
- Provide evaluation of documentation received from the manufacturer and recommendation on suitability of use to the EAC.

The EAC Responsibilities

The EAC will evaluate manufacturer submitted documentation and VSTL recommendation in coordination with NIST on a case-by-case basis to determine if the "Historical" module continues to meet all current functional and security requirements necessary for use in voting systems. Factors considered in the EAC's determination will include the nature and scope of the cryptographic module's use within the voting system and whether the module's cryptographic services remain consistent with current NIST guidance. Manufacturers with questions regarding the likely suitability of a specific "Historical" module prior to submission are encouraged to contact the Program Director for pre-submission guidance.

The EAC will notify the VSTL and the manufacturer of the evaluation outcome. Acceptance of the use of a "Historical" module does not indicate that the cryptographic module meets all VVSG requirements. VSTLs remain responsible for evaluating the implementation of the module against all applicable VVSG requirements.

U.S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
633 3rd Street NW, Suite 200
Washington, DC 20001

Conclusion

Due to the ongoing transition from FIPS 140-2 to FIPS 140-3, and consistent with the interpretation established in RFI 2026-01, the EAC will not automatically reject a voting system submission solely on the basis that it utilizes a cryptographic module designated as "Historical" by the CMVP, provided the submission meets the eligibility requirements established in this memorandum. Instead, such submissions will be subject to the additional evaluation process described herein, and acceptance will be determined on a case-by-case basis. The use of an approved "Historical" module does not guarantee certification. Modules listed as "Revoked" are expressly prohibited. Beginning January 1, 2027, following the completion of the FIPS 140-2 transition, the EAC will no longer accept system applications that include cryptographic modules designated as "Historical."