U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

EAC Decision on Request for Interpretation 2026-01 Federal Information Processing Standard (FIPS) Cryptographic Modules

Sections of Voluntary Voting System Guidelines 2.0:

13.3-A –Cryptographic Module Validation

Cryptographic functionality must be implemented in a cryptographic module that meets current FIPS 140 validation, operating in FIPS mode. This applies to:

1. software cryptographic modules, and
2. hardware cryptographic modules.

Date:

June 23, 2026

Question(s):

1. Does the term "current" in Requirement 13.3-A refer exclusively to cryptographic modules designated as "Active" by the CMVP?
2. Do cryptographic modules designated as "Historical" by the CMVP satisfy the "current FIPS 140 validation" requirement of 13.3-A?

Discussion:

The Cryptographic Module Validation Program (CMVP) is a joint effort between the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security. Cryptographic and Security Testing Laboratories (CSTLs) verify cryptographic modules to ensure they meet a set of testable cryptographic and security criteria. Upon completion of testing the CMVP identifies validation status for each cryptographic module as “Active”, “Historical”, or “Revoked”. “Active” modules meet the requirements of either the FIPS 140-2 or FIPS 140-3 standard as annotated on the CMVP validation entry. This is the default status for all newly validated modules. A “Historical” status indicates that the certificate and the documentation posted with it is more than 5 years old. In this case, the certificates have not been updated to reflect latest guidance or transitions and may not accurately reflect how the module can be used in a FIPS-approved mode. Modules that have been noted as “Historical” are not to be included in new systems but may still be procured and used in legacy systems. If a validation certificate is marked as “Revoked” the module validation is no longer valid and may not be referenced to demonstrate compliance with the FIPS 140 standards.

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

The term "current" used in requirement 13.3-A is not defined by NIST, CMVP, the Voluntary Voting System Guidelines (VVSG) nor the Voting System Testing and Certification Program Manual. The EAC, in collaboration with NIST technical experts, has determined that the intent of the term "current" refers only to modules designated as "Active" by CMVP, given these modules are supported and maintained. Modules with an "Active" status have recently undergone review ensuring their integrity and ability to perform cryptography in line with current FIPS requirements. Modules that have not received recent review are moved to a "Historical" status given that they may still perform at the necessary level, but without being submitted for review there is not a guarantee. Requiring an "Active" module status for cryptography used in a voting system ensures that modules are receiving regular review and voting systems meet all federal standards. In addition, modules must be valid at the time of U.S. Election Assistance Commission (EAC) certification to satisfy the applicable federal standards rather than modules whose validation has transitioned to a "Historical" status.

Under the sunset policy established by CMVP in 2017, a module's validation remains in an "Active" status for 5 years. After its initial validation, the certificate is moved to "Historical" status. As a result, all remaining FIPS 140-2 module validations will transition to the "Historical" status by September 21, 2026. To ensure testing and certification of voting systems to VVSG 2.0 proceeds during this period without unnecessary delay, separate temporary guidance addressing the sunset period has been issued by the EAC in the Policy Memorandum "Use of Historical Federal Information Processing Standard (FIPS) 140-2 Cryptographic Modules."

Conclusion:

The term "current" for FIPS 140 validation is defined as modules listed as "Active." Cryptographic modules designated as "Historical" or "Revoked" do not meet requirement 13.3-A for current FIPS 140 validation. Separate guidance addressing the transition period issued by the EAC can be found in the Policy Memorandum "Use of Historical Federal Information Processing Standard (FIPS) 140-2 Cryptographic Modules."

Effective Date:

As of the date this document is published.