

FIPS 140-2 Certificates Are Now Historical: What Changes for CMMC Control 3.13.11

FIPS 140-2 Certificates Are Now Historical: What Changes for CMMC Control 3.13.11

Adamas Systems · HARDAC-ADV-2026-01 · 27 October 2026 · HARDAC Industries LLC. General guidance, not legal advice or an assessment finding.

HARDAC Industries LLC — Security Advisory HARDAC-ADV-2026-01

Published 27 October 2026 · Version 1.0

Summary

On 21–22 September 2026, NIST's Cryptographic Module Validation Program (CMVP) moved every FIPS 140-2 certificate to its Historical List. The modules did not stop working and existing systems did not become noncompliant: NIST states that CMVP "supports the purchase and use of these modules for existing systems." What changed is the status an assessor sees when they look up each module.

For defense contractors handling Controlled Unclassified Information (CUI), that matters because NIST SP 800-171 control 3.13.11, carried into CMMC as SC.L2-3.13.11, requires FIPS-validated cryptography, and the evidence for it is a list of modules with their certificate numbers and status. Every evidence file built on 140-2 certificates now points at Historical entries. This advisory explains the rule, what the status change does and does not mean, and the steps to bring a 3.13.11 evidence file current.

1. What NIST did

- FIPS 140-2 modules could be used for new systems until 21 September 2026 (NIST's transition page; its schedule table shows 22 September). After that date, all 140-2 certificates moved to the Historical List. [1]
- NIST's position on historical modules: "Even on the historical list, CMVP supports the purchase and use of these modules for existing systems." For new purchases NIST recommends considering all validated modules, FIPS 140-2 or 140-3; the practical reading for a contractor is that new systems should be built on 140-3 certificates, which will not sunset. [1]
- The change reaches ordinary environments. Microsoft's Kernel Mode Cryptographic Primitives Library, FIPS 140-2 certificate #4766, covering Windows 10 20H2/21H1, Windows 11 and Windows Server 2022, is now listed as "Historical ... due to sunseting." [3]
- FIPS 140-3 certificates are unaffected. Validated modules that include post-quantum algorithms now exist, for example AWS-LC 3 (certificate #5314, validated 5 June 2026) and the Go cryptographic module (#5349). [4]

2. What the rule requires

- 32 CFR 170.24(c): "FIPS-validated encryption (CMMC Level 2 security requirement SC.L2-3.13.11) is required to protect the confidentiality of CUI." [5]
- Scoring: if encryption is employed but not FIPS-validated, three points are subtracted from the assessment score; if no encryption is employed, five points. [5]

- POA&M: 3.13.11 is the one multi-point requirement that may sit on a Plan of Action and Milestones, and only when encryption is employed but not FIPS-validated. A Level 2 conditional status must close out within 180 days (32 CFR 170.21). [6]
- DFARS 252.204-7012 has required NIST SP 800-171 since 2017 and continues to apply. CMMC Phase 2 third-party assessments were suspended on 13 July 2026 pending DoD's review; self-assessments, SPRS scores and annual affirmations continue. [7]

3. What the status change means, and what it does not

Question	Answer
Does a Historical certificate make my system noncompliant?	No. NIST supports continued use in existing systems, and the control asks whether the cryptography is validated, which a Historical certificate still records. [1]
Does my evidence file need to change?	Yes. Any evidence that cites a 140-2 certificate now cites a Historical entry. The system security plan (SSP) should state the module's current status and the organization's position on it, rather than leave an assessor to discover the change.
Can I keep buying or deploying 140-2 modules?	For existing systems, yes; NIST supports it. For new systems, build on FIPS 140-3 certificates: a Historical certificate will never return to Active, so a new deployment on one starts with evidence that is already dated. [1]
Is "FIPS mode enabled" enough?	No. Validation is specific to a module, a version and an operational environment. A product can run in FIPS mode on an environment that is not in the certificate's scope. The evidence must match all three.
What if I have no validated module for a function?	Record it. If encryption is employed but not validated, the gap can go on a POA&M for up to 180 days; if no encryption protects CUI in transit or at rest, there is no POA&M path for that item. [5][6]

4. Steps to bring 3.13.11 evidence current

1. **Inventory the cryptography that protects CUI.** For each system in the CUI boundary, record where CUI is encrypted at rest and in transit: operating-system modules, TLS libraries, VPNs, backup and email gateways, mobile device management, file-sharing services and cloud services.
2. **Identify the module behind each item**, not the product name: the library or hardware module, its version and the operating environment it runs on.
3. **Look up each module on the CMVP list** and record the certificate number, the standard (140-2 or 140-3), the status (Active, Historical or Revoked), the sunset date, and the operational environments the certificate covers. Confirm the version in use is the version the certificate names.
4. **Read the security policy's approved-mode conditions** for each certificate. A module is validated only when configured and used as its security policy states.
5. **Write the SSP position.** For each Historical module: that it remains in use in an existing system, that NIST supports that use, and the plan and date for moving to a 140-3 module. For each unvalidated item: the POA&M entry and its 180-day close date.
6. **Date and sign the evidence**, keep the lookups, and set a recurrence. Certificate status changes without notice to the contractor; a refresh at least annually, and before each affirmation, keeps the evidence true.

5. Why this is worth doing now

Three things make 2026 different from a routine refresh. The status of every 140-2 module changed on one day, so almost every existing evidence file is now out of date at once. Enforcement of NIST SP 800-171 continues through self-assessment, SPRS scoring and the annual affirmation even while third-party assessments are suspended, and a false affirmation carries False Claims Act exposure. And the post-quantum transition has begun: new 140-3 modules carry the NIST post-quantum algorithms, and federal deadlines for that transition run from 2027 to 2035, so a module inventory built now is the starting point for the migration plan that will follow.

What this advisory does not cover

- Whether a specific assessor will accept a Historical certificate in a given system: that is the assessor's call, informed by the SSP position described above.
- NIST SP 800-171 Revision 3 (control 03.13.11), which DoD has not yet adopted into CMMC.
- Cryptography outside the CUI boundary, and encryption of FCI, which 3.13.11 does not govern.

About HARDAC

HARDAC Industries LLC is a managed security services provider and compliance consultancy, in business ten years, delivering ISO/IEC 27001 and NIST Risk Management Framework consulting and managed security operations to defense contractors and commercial clients. This advisory is general guidance, not legal advice or an assessment finding; contractors should confirm each module's status against the CMVP list and their own assessor's expectations.

Sources

1. NIST, FIPS 140-3 Transition Effort (updated 13 April 2026). <https://csrc.nist.gov/projects/fips-140-3-transition-effort>
2. NIST, Cryptographic Module Validation Program. <https://csrc.nist.gov/projects/cryptographic-module-validation-program>
3. NIST CMVP, certificate #4766, Microsoft Kernel Mode Cryptographic Primitives Library. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4766>
4. NIST CMVP, validated modules list: certificate #5314 (AWS-LC 3) and #5349 (Go cryptographic module). <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>
5. 32 CFR Part 170, CMMC Program final rule, 15 October 2024, §170.24. <https://www.govinfo.gov/content/pkg/FR-2024-10-15/html/2024-22905.htm>
6. 32 CFR §170.21, Plan of Action and Milestones requirements. Same publication.
7. USD(A&S) memorandum 26-P-1023, Implementing Suspension of CMMC Phase II, 13 July 2026. <https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf>

Change log

- 1.0, 27 October 2026: first publication.