

Why "FIPS Mode Enabled" Is Not 3.13.11 Evidence: How FIPS Validation Status Gets Reported Wrongly

Why "FIPS Mode Enabled" Is Not 3.13.11 Evidence: How FIPS Validation Status Gets Reported Wrongly

Adamas Systems · HARDAC-ADV-2026-03 · 27 October 2026 · HARDAC Industries LLC. General guidance, not legal advice or an assessment finding.

HARDAC Industries LLC — Security Advisory HARDAC-ADV-2026-03

Published 27 October 2026 · Version 1.0

Author: HARDAC Industries LLC. Canonical URL: assigned on publication.

Summary

NIST SP 800-171 control 3.13.11, carried into CMMC as SC.L2-3.13.11, asks whether FIPS-validated cryptography is employed to protect the confidentiality of CUI. [8] The evidence is a set of Cryptographic Module Validation Program (CMVP) certificates matched to the systems in the CUI boundary. A certificate is narrow: it names one module, specific versions, and the operational environments a laboratory tested, and it holds only while the module runs in the approved mode its security policy describes. [1][5][6]

In our assessment experience, most 3.13.11 evidence files break at least one of those links: a product named instead of a module, a version other than the one installed, an operating system the certificate does not list, the Windows "FIPS mode" policy offered as proof of validation, or a certificate that has moved to the Historical list. This advisory, for defense contractors, managed service providers and CMMC consultants, reads one certificate page, lists the error classes with the fix for each, and gives the record to keep per item. Encryption that is not FIPS-validated costs three points, none costs five, and only the first has a 180-day POA&M path. [9][10]

1. The rule in brief

- 32 CFR 170.24(c)(4)(ii): "FIPS-validated encryption (CMMC Level 2 security requirement SC.L2-3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not FIPS-validated, three (3) points are subtracted from the maximum score; if encryption is not employed; five (5) points are subtracted from the maximum score." [9]
- 32 CFR 170.21(a)(2)(ii): a Level 2 POA&M may hold no requirement worth more than one point, "except SC.L2-3.13.11 CUI Encryption may be included on a POA&M if encryption is employed but it is not FIPS-validated." Closeout must be confirmed within 180 days of the Conditional CMMC Status Date (170.21(b)). [10]
- NIST SP 800-171A (June 2018), the procedure CMMC uses for Rev. 2: "Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI." Objects to examine include "cryptographic module validation certificates; list of FIPS-validated cryptographic modules." [8]
- NIST on terms: "The correct term is validated." A "compliant" claim means the vendor believes its product meets the requirements without CMVP validation; a validated module "will have a CMVP issued certificate number." [2]
- For CUI in an external cloud service, DFARS 252.204-7012(b)(2)(ii)(D) requires security equivalent to the FedRAMP Moderate baseline. That is a separate requirement, not a substitute for the 3.13.11 record. [11]

2. What a certificate covers: a worked reading

Microsoft's Kernel Mode Cryptographic Primitives Library (cng.sys), CMVP certificate #4766, records: [5]

- **Standard and status.** FIPS 140-2; Historical, "Moved to historical list due to sunseting"; the module "should not be included by Federal Agencies in new procurements."
- **Overall level.** 1. Validated 19 August 2024 by Leidos.
- **Software versions.** 10.0.19042, 10.0.19043, 10.0.20348, 10.0.22000: the builds of Windows 10 20H2 and 21H1, Windows Server 2022 and Windows 11 21H2.
- **Tested configurations.** Sixteen lines, each an operating system edition on named hardware, for example "Windows 10 version 20H2 Enterprise (64-bit) running on a Dell Latitude 7420 with an Intel i7-1185G7 with PAA" and "Windows Server 2022 Core Datacenter (64-bit) running on an HPE ProLiant E910."
- **Caveat.** "When operated in FIPS mode with modules Windows OS Loader validated to FIPS 140-2 under Cert. #4339" and related boot-chain certificates. This module's validation depends on others.
- **Security policy** (version 1.1, 24 June 2024). Section 1.3: FIPS-Approved mode is entered by the Group Policy setting "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" or a registry value under FIPSAAlgorithmPolicy, then a reboot. Section 2: third-party applications and drivers "must not use any of the non-Approved algorithms implemented by this module," and booting in Debug mode, booting with driver signing disabled, or entering the S4 power state puts the module in a non-Approved mode. [6]

Read together: this binary, in these four builds, on this hardware, with FIPS mode set, the boot chain validated, and no caller using a non-approved algorithm. It does not say "Windows is FIPS validated." Microsoft: "Microsoft validates the cryptographic modules used in Windows and other products, not individual Windows services or applications." [3]

The FIPS 140-3 successor, certificate #5408 (Active, validated 31 August 2026, sunset 30 August 2031), presents the same facts in the 140-3 layout. Its security policy (version 1.0, 4 May 2026) names Windows 11 22H2 build 10.0.22621.30001 and Windows Server 2022 build 10.0.20348.30000, lists the tested hardware, and adds a vendor-affirmed table (relabeled versions of those operating systems on "Any UEFI-based x64 computer") followed by the required sentence that "The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated sensitive security parameters (SSPs or keys) when so ported." Section 11.2 tells the administrator to check the installed Windows version and the CNG.SYS file version against the listed builds. [7]

3. The error classes

3.1 Wrong module named

Assessor sees. "Windows 11 (FIPS validated)," "VPN client (FIPS compliant)," "BitLocker, FIPS 140-2," with no certificate number or with a number for a different module than the one doing the work.

Why it fails. Certificates are issued to modules. NIST: "A product which uses an embedded validated cryptographic module cannot claim itself to be validated," and "There is no assurance that a product is correctly utilizing an embedded validated cryptographic module." [2]

Fix. Name the module. For Windows that is the Cryptographic Primitives Library, the Kernel Mode Cryptographic Primitives Library and the boot-chain modules, each with its own certificate on Microsoft's per-release list. [4] For third-party products, obtain a signed vendor letter citing the certificate number; if the letter and the CMVP entry do not match, "the vendor is not offering a validated solution." [1]

3.2 Version drift

Assessor sees. OpenSSL FIPS Provider certificate #4282 cited for a 3.0 release other than 3.0.8 or 3.0.9; #4766 cited for a Windows 11 build later than 10.0.22000.

Why it fails. The CMVP entry states "what version/part number/release is validated." [1] #4282 lists 3.0.8 and 3.0.9 only. [12] The 140-3 OpenSSL certificate #4985 covers 3.1.2; OpenSSL records that 3.5.8 "has been submitted for FIPS 140-3 validation and is in the CMVP review process," so it is not validated today. [13][14]

Fix. Record the installed version from the system (file version, package version, build) beside the certificate's version string. Where they differ, the item is not covered by that certificate.

3.3 Untested operational environment

Assessor sees. A certificate listing Windows 10 20H2 and Windows 11 21H2 cited for Windows 11 24H2 endpoints; #4282 (tested on Ubuntu 22.04.1, Debian 11.5, FreeBSD 13.1, macOS 11.5.2 and Windows 10) cited for a container on another Linux distribution.

Why it fails. The certificate "serves as the benchmark for the module-compliant configuration." Porting to an unlisted environment is allowed under the porting rules, and the vendor or user "may affirm that the module works correctly in the new OE. However, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported." Vendor-affirmed configurations "may be considered by the user at their risk." [15] FIPS 140-2 IG G.5 said the same. [16] Microsoft's Windows 11 validation list names 21H2 and 22H2 only, as of 2 September 2026. [4]

Fix. Record the tested configuration matched, or the vendor-affirmed entry (as in #5408 Table 8 [7]), or the organization's own user affirmation under Management Manual 7.9.2. Say which.

3.4 FIPS mode flag mistaken for validation

Assessor sees. A Group Policy report showing "System cryptography: Use FIPS compliant algorithms" enabled, offered as the 3.13.11 evidence for the Windows estate.

Why it fails. The policy is one approved-mode condition for 140-2 Windows modules, not the validation. [6] For Windows 11 and Server 2022 and later, Microsoft states that since the April 2024 updates the modules run their self-tests automatically and "Configuring the legacy FIPS policy is no longer needed unless the BitLocker scenario described in BitLocker and the FIPS policy is still in use." [3] The flag on a Windows 11 24H2 machine does not put that build on #4766 or #5408.

Fix. Keep the policy evidence where a security policy calls for it, including BitLocker PIN protectors, where it switches key derivation to PBKDF2. [3] File it under approved-mode conditions. The validation evidence is the certificate match in Section 4.

3.5 Approved-mode conditions not met

Assessor sees. Right module, right version, listed environment, and a configuration the security policy excludes: driver signing disabled, an application set to a non-approved algorithm, a BitLocker PIN created before the policy was set.

Why it fails. Certificate caveats read "When operated in FIPS mode" or "When operated in approved mode," often with "When installed, initialized and configured as specified in Section 11.1 of the Security Policy." [5][7][17] Microsoft: where that note appears, "specific configuration and security rules outlined in the Security Policy must be followed." [3]

Fix. Turn each security policy's operator rules into a per-module checklist with configuration evidence per line. Where a condition cannot be met, record the item as not validated.

3.6 Historical or Revoked status unnoticed

Assessor sees. A 2025 evidence file listing every Windows and OpenSSL certificate as Active. On 22 September 2026 every FIPS 140-2 certificate moved to the Historical list. [18] OpenSSL's FIPS page still showed #4282 and #4811 as Active with a 21 September 2026 end date when we read it; the CMVP pages now read Historical. [12][13]

Why it matters. Historical is not revocation: NIST supports "the purchase and use of these modules for existing systems." [18] Revoked means "the module validation is no longer valid and may not be referenced." [1] NIST also warns a historical certificate "may not accurately reflect how the module can be used in FIPS/approved mode." [2] A record that reports a status the CMVP page no longer shows is wrong on its face.

Fix. Record status and date read for every certificate; state the position on each Historical module (existing system, migration target and date); treat Revoked as no validation. HARDAC Advisory 2026-01 covers the transition.

3.7 Cloud or SaaS asserted without the provider's certificate

Assessor sees. "Microsoft 365 GCC High: FIPS validated" or "FedRAMP, therefore FIPS," with no module or certificate.

Why it fails. FedRAMP equivalence is a DFARS requirement on the provider [11]; it does not identify the module that encrypts this contractor's CUI in that service. The service "utilizes" validated modules; it is not itself validated. [2] AWS-LC 3 (#5314, FIPS 140-3, Active, sunset 4 June 2031) and SafeLogic's CryptoComply Native Go Module (#5349, Active, sunset 26 April 2031) show what a current cloud-side certificate looks like, each listing ML-KEM. [17][19]

Fix. Capture the provider's published, dated statement of the modules and certificates protecting customer data for the service in use, and the contractor-side module (the endpoint's TLS client is in scope).

3.8 VPN, backup and email gateways omitted

Assessor sees. An inventory of endpoints and file servers; the VPN concentrator, backup appliance, email gateway and MDM agent encrypt CUI and none appear.

Why it fails. The objective covers all cryptography "employed to protect the confidentiality of CUI." [8] Each of those devices runs its own module, often firmware with its own version and tested configuration.

Fix. Inventory by CUI data path: wherever CUI is stored or crosses a network, name the module at each end.

4. The correct matching record

One row per item, kept with the SSP:

Field	Record
CUI data path	System, store or link; at rest or in transit
Product	Commercial name
Module	Name as the certificate states it [1]
Certificate and standard	Number; FIPS 140-2 or 140-3
Status and date read	Active / Historical / Revoked; sunset date; date the CMVP page was read
Validated version	Version string on the certificate or in security policy §2.2
Installed version	File, package or build version taken from the host [7]
Operational environment	Tested configuration matched, vendor-affirmed entry, or user affirmation on file [15]
Approved-mode conditions	Security policy rules and the configuration evidence for each

Dependencies	Other certificates the caveat requires [5]
Vendor statement	Signed letter naming module and certificate (third-party and cloud) [1]
Result	Matched; vendor- or user-affirmed; not validated (POA&M); no encryption

5. Questions and answers

Question	Answer
The vendor says "FIPS 140-2 compliant." Enough?	No. Only a module with a CMVP certificate number is validated. Ask which module the product uses and for a letter citing the certificate. [1][2]
Our Windows build is newer than any on the certificate.	Not covered by the tested configurations. Look for a vendor-affirmed entry in the security policy; otherwise the basis is user affirmation, which the CMVP does not stand behind. Record which. [7][15]
Does enabling the FIPS policy make Windows validated?	No. It is one approved-mode condition for some modules, and Microsoft says it is no longer needed on Windows 11 and Server 2022 outside the BitLocker PIN case. [3][6]
A certificate is Historical. NOT MET?	NIST supports continued use in existing systems. The record must show current status and the organization's position. [1][18]
A certificate is Revoked.	It "may not be referenced." Treat as not FIPS-validated: three points, POA&M for 180 days. [1][9][10]
No validated module for one data path.	Encryption without validation: three points, POA&M. No encryption: five points, no POA&M. [9][10]
One certificate, several operating systems?	Only the tested configurations plus the security policy's vendor-affirmed table; each row needs its own match. [5][7]

6. Action steps

1. Rebuild the 3.13.11 inventory by CUI data path, including VPN, backup, email, MDM, removable media and cloud services.
2. Replace each product name with the module name and certificate number; read the CMVP page on a recorded date. [1]
3. Capture the installed version from the system and compare it with the certificate.
4. Match the operating system and hardware to a tested configuration, or document the vendor- or user-affirmed basis. [15]
5. Extract each security policy's operator rules and keep configuration evidence per rule; file the Windows FIPS policy there, not as validation. [3][6]
6. Mark each Historical certificate with its 140-3 migration plan, and each Revoked or unmatched item as a POA&M entry closing within 180 days. [10][18]
7. Date and sign the record; refresh it before each affirmation and on every operating system or module version change.

7. What this does not cover

This advisory addresses the confidentiality objective of 3.13.11 under NIST SP 800-171 Rev. 2 as assessed by SP 800-171A (June 2018). It does not address Rev. 3, the companion requirements that rely on 3.13.11 (remote access, wireless, portable media, CUI at rest and in transit), key management, the CMMC Phase 2 suspension, or the accuracy of any vendor's claims. Confirm each certificate on the CMVP site at the time of use.

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 CMVP, Validated Modules (Historical and Revoked definitions; vendor letter advice). Updated 21 August 2026. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>
2. NIST CMVP, Frequently Asked Questions (SG-7, SG-8, P-17, P-18, CL-8). Updated 21 August 2026. <https://csrc.nist.gov/Projects/cryptographic-module-validation-program/FAQs>
3. Microsoft, Windows FIPS 140 validation. Page dated 2 September 2026. <https://learn.microsoft.com/en-us/windows/security/security-foundations/certification/fips-140-validation>
4. Microsoft, FIPS 140 validated modules for Windows 11 (22H2: #5404–#5410; 21H2: #4546, #4825, #4766). Page dated 2 September 2026. <https://learn.microsoft.com/en-us/windows/security/security-foundations/certification/validations/fips-140-windows11>
5. NIST CMVP, certificate #4766, Kernel Mode Cryptographic Primitives Library (FIPS 140-2, Historical). Read 27 October 2026. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4766>
6. Microsoft, Kernel Mode Cryptographic Primitives Library Security Policy, version 1.1, 24 June 2024 (certificate #4766). <https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4766.pdf>
7. Microsoft, Kernel Mode Cryptographic Primitives Library FIPS 140-3 Security Policy, version 1.0, 4 May 2026, and NIST CMVP certificate #5408 (Active, validated 31 August 2026, sunset 30 August 2031). <https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp5408.pdf> ; <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5408>
8. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, June 2018, requirement 3.13.11. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>
9. 32 CFR §170.24(c)(4)(ii), CMMC Program final rule, 89 FR 83092, 15 October 2024. <https://www.govinfo.gov/content/pkg/FR-2024-10-15/html/2024-22905.htm> ; codified text at <https://www.law.cornell.edu/cfr/text/32/170.24>
10. 32 CFR §170.21(a)(2) and (b), same publication. <https://www.law.cornell.edu/cfr/text/32/170.21>

11. DFARS 252.204-7012, paragraph (b)(2)(ii)(D), May 2024. <https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>.
12. NIST CMVP, certificate #4282, OpenSSL FIPS Provider (FIPS 140-2, versions 3.0.8 and 3.0.9, Historical). Read 27 October 2026. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4282>
13. OpenSSL, CVEs and the FIPS provider (#4985 for 3.1.2; #4282 and #4811 for 3.0.8 and 3.0.9; 3.5.8 in CMVP review). Undated; read 27 October 2026. <https://openssl-library.org/news/fips-cve/index.html>
14. NIST CMVP, certificate #4985, OpenSSL FIPS Provider (FIPS 140-3, Active, sunset 10 March 2030). <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4985>
15. NIST and CCCS, FIPS 140-3 CMVP Management Manual, version 2.7, 9 April 2026, section 7.9. <https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS-140-3-CMVP%20Management%20Manual.pdf>
16. NIST and CCCS, Implementation Guidance for FIPS 140-2 and the CMVP, last update 30 October 2023, IG G.5. <https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips140-2/FIPS1402IG.pdf>
17. NIST CMVP, certificate #5314, AWS-LC 3 Cryptographic Module (static) (FIPS 140-3, Active, validated 5 June 2026, sunset 4 June 2031). <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5314>
18. NIST, FIPS 140-3 Transition Effort. Updated 13 April 2026. <https://csrc.nist.gov/projects/fips-140-3-transition-effort>
19. NIST CMVP, certificate #5349, CryptoComply Native Go Module, SafeLogic (FIPS 140-3, Active, validated 23 June 2026, sunset 26 April 2031). <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5349>

Change log

- 1.0, 27 October 2026: first publication.