

What a Cryptographic Inventory for CMMC Control 3.13.11 Actually Costs

What a Cryptographic Inventory for CMMC Control 3.13.11 Actually Costs

Adamas Systems · HARDAC-ADV-2026-02 · 27 October 2026 · HARDAC Industries LLC. General guidance, not legal advice or an assessment finding.

HARDAC Industries LLC — Security Advisory HARDAC-ADV-2026-02

Published 27 October 2026 · Version 1.0

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

Summary

CMMC control SC.L2-3.13.11 requires FIPS-validated cryptography wherever cryptography protects the confidentiality of CUI. The only evidence that proves it is an item-by-item list of the cryptographic modules in the CUI boundary, each matched to a CMVP certificate, a version, an operational environment and an approved-mode configuration. No consultancy we could find publishes a price for building that list, and the cryptography share of a standard gap assessment (about 3 to 9 percent of the work, derived below) is enough to mark the control "not met" but not enough to build the inventory behind it.

This advisory sets out the tasks, the hours per unit and the arithmetic. For a contractor under 50 employees the initial inventory and mapping is about 80 hours, or \$12,000 to \$32,000 at market consulting rates; for 50 to 250 employees, about 180 hours, or \$27,000 to \$72,000. A yearly refresh runs about 37 percent of the initial effort. Every figure is cited or derived from arithmetic shown here. The model is a planning estimate, not a quote.

1. The rule and the score

- 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. 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." [1]
- 32 CFR 170.21 governs POA&Ms. The rule states that 3.13.11 "may be included on a POA&M if encryption is employed and is not FIPS-validated," and that POA&M items "must be remedied within 180 days." DoD adds that "FIPS module validation can exceed the 180-day CMMC assessment POA&M threshold" and that vendor limitations "could be considered enduring exceptions or temporary deficiencies." [1]
- The DoD Assessment Methodology sets the evidentiary standard: "Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140." [2]
- Since 21 September 2026 every FIPS 140-2 certificate is on the CMVP Historical List, including Microsoft's Kernel Mode Cryptographic Primitives Library (#4766). NIST supports continued use in existing systems; the evidence file still has to record the new status (see HARDAC-ADV-2026-01). [3][4][5]

The control cannot be proven from a policy or a screenshot of "FIPS mode enabled." It is proven module by module.

2. Why gap assessments undercount cryptography

No published source breaks out the cryptography share of a CMMC engagement. It can be derived from the scoring weights [Derived, from source 2]:

Basis	Cryptography controls	Share
SPRS points, six core controls (3.1.13, 3.5.10, 3.13.8, 3.13.10, 3.13.11, 3.13.16: 5+5+3+1+5+1, with 3.13.11 at its 5-point value)	20 of 313	6.4%
SPRS points, adding 3.1.17, 3.1.19, 3.8.6 (5+3+1)	29 of 313	9.3%
NIST SP 800-171A assessment objectives (our parse)	11 or 16 of 320	3.4% to 5.0%

The 313 total is the sum of point values across the 110 requirements in the DoD methodology, whose scores run from 110 down to -203 [2]. The range is about 3 to 9 percent. Applied to what the market sells [Derived]:

- DoD's cost model for a small entity's Level 2 self-assessment budgets 88 external service provider hours at \$260.28 (32 planning, 48 conducting, 8 reporting), assuming the controls are already implemented [1]. A 3.4 to 9.3 percent share is 3.0 to 8.2 hours, or \$790 to \$2,120.
- Market gap assessments run from about \$3,500 to \$20,000 (vendor claim) [6]; one RPO publishes a Level 2 gap assessment at \$21,200 [7]. The cryptography share is about \$120 to \$1,970.

Three to eight hours is enough to ask whether FIPS mode is on and record "not met," not to enumerate every module and look each one up. That is consistent with DIBCAC's report at the September 2022 CyberAB town hall that 3.13.11 was the most common "other than satisfied" practice, failed by half of the companies with any top-ten finding (secondary source) [8].

3. The task list and the arithmetic

An inventory for 3.13.11 is a sequence of manual tasks. Tools shorten the first two; they do not shorten the rest. OMB describes the federal manual inventory as "researching each piece of hardware and software to discover the type of cryptography used," and notes that automated tools "may not identify all instances." [9]

Hours per unit [Derived; our estimates, calibrated in Section 5]

Task	Unit	Hours per unit (low-high)
Scoping: CUI boundary, data flows, interviews	engagement	4-8 (under 50); 8-12 (50-250); 16-24 (250-1,000); 32-48 (over 1,000)
Discovery: RMM/EDR/MDM exports, TLS and SSH scans, certificate discovery, cloud key-store listings	engagement	4-8; 8-16; 16-32; 40-80 by band
OS/firmware build review: FIPS policy, disk encryption, module versions	distinct build	1.0
Appliance review: firewall, VPN, Wi-Fi, NAS, backup; FIPS mode and ciphers	model/firmware	1.0-1.5
TLS/SSH service triage	listening service	0.1
Certificate review, grouped by issuer and template	certificate	0.05 for the first 300, then 0.02
CUI application and SaaS review: vendor documentation, FIPS letters, library identification	application	0.75-1.25
Cloud tenant and key management review	tenant	2-4

CMVP lookup: find the certificate; match version and operational environment; record Active, Historical or Revoked and sunset date; read the security policy's approved-mode conditions	distinct module	0.75–1.0
Deliverables: inventory, SSP narrative, POA&M and operational plan entries, evidence package	engagement	10–16; 16–28; 28–48; 60–100 by band
Project management and QA		+10%

Scope assumptions by band [Derived]

	Under 50	50–250	250–1,000	Over 1,000
Distinct OS/firmware builds	3–6	6–12	12–25	25–60
Appliance models	3–8	8–20	20–60	60–200
TLS/SSH services	10–40	40–150	150–600	600–3,000
Certificates	10–50	50–300	300–2,000	2,000–20,000
CUI applications and SaaS	8–20	20–50	50–120	120–400
Cloud tenants	1–3	2–5	4–10	10–40
Distinct modules to map	12–25	25–50	50–100	100–250

Worked example, under 50 employees. Typical uses the scope midpoint and the per-unit midpoint: scoping 6 + discovery 6 + builds $4.5 \times 1.0 = 4.5$ + appliances $5.5 \times 1.25 = 6.9$ + services $25 \times 0.1 = 2.5$ + certificates $30 \times 0.05 = 1.5$ + applications $14 \times 1.0 = 14$ + cloud $2 \times 3 = 6$ + CMVP $18.5 \times 0.875 = 16.2$ + deliverables 13 = 76.6 hours; plus 10 percent = 84.3, rounded to 80. The low case (every count and rate at its low end) is $42.5 \times 1.1 = 47$ hours; the high case is $118.5 \times 1.1 = 130$.

Band	Scope	Disc.	OS	Appl.	TLS/SSH	Certs	Apps	Cloud	CMVP	Deliv.	+10%	Total → typical
Under 50	6	6	4.5	6.9	2.5	1.5	14	6	16.2	13	7.7	84 → 80
50–250	10	12	9	17.5	9.5	8.8	35	10.5	32.8	22	16.7	184 → 180
250–1,000	20	24	18.5	50	37.5	32	85	21	65.6	38	39.2	431 → 430
Over 1,000	40	60	42.5	162.5	180	229	260	75	153.1	80	128.2	1,410 → 1,400

Certificate hours in the larger bands use the stepped rate ($1,150$ certificates = $300 \times 0.05 + 850 \times 0.02 = 32$). The two largest lines in every band are application review and CMVP mapping, the two that tooling does not remove.

4. The cost by size band

Rate tiers [Derived from sources 1, 6, 7, 10, 11]

Tier	Rate	Anchors
In-house	\$81–\$97/hr	BLS May 2025 median for information security analysts, \$62.11, $\times 1.30$ (DoD's fringe and G&A factor) = \$80.74 [10][1];

		DoD's in-house staff IT specialist, \$97.49 [1]
Low	\$150/hr	MSP project engineers \$135–\$195 (vendor claim) [11]; DoD's external service provider rate is the next tier up [1]
Mid	\$250/hr	DoD's external service provider rate, \$260.28, an "Information Assurance Specialist Level 7," which "includes the labor rate, overhead expense, G&A expense, and profit" [1]; bottom of the \$250–\$400 CMMC consultant band (vendor claim) [6]
High	\$400/hr	Top of that band [6]; one RPO's published full day at \$3,600, about \$450 an hour [7]

Initial inventory and CMVP mapping [Derived: Section 3 hours × rate]

	Under 50	50–250	250–1,000	Over 1,000
Typical hours	80	180	430	1,400
Hours range (low–high case)	47–130	99–287	226–680	562–2,428
Low, \$150	\$12,000	\$27,000	\$64,500	\$210,000
Central, \$250	\$20,000	\$45,000	\$107,500	\$350,000
High, \$400	\$32,000	\$72,000	\$172,000	\$560,000
Full range (low hours × \$150 to high hours × \$400)	\$7,000–\$52,000	\$14,900–\$115,000	\$33,900–\$272,000	\$84,000–\$971,000
In-house labor at \$81/hr, typical hours	\$6,480	\$14,580	\$34,830	\$113,400
Central cost per endpoint (75 / 300 / 1,250 / 5,000 endpoints)	\$267	\$150	\$86	\$70

For scale, DoD's model prices an entire small-entity Level 2 self-assessment with its initial affirmation at \$34,277 [1], and SBA puts total compliance cost per certification for self-assessing small firms at \$388,600, with no breakdown [12]. A real 3.13.11 inventory for an under-50 contractor is close to DoD's whole assessment budget, which is why it is seldom built in full.

5. Cross-checks against published prices

Published offerings are post-quantum readiness assessments, not 3.13.11 packages, and none includes per-module CMVP mapping or SSP evidence. Converted to hours at the central and low rates [Derived]:

Published anchor	Implied hours	Comparison
PQC Consultancy Tier 1: up to 100 assets, 2–3 weeks, \$6,500, CBOM plus algorithm and certificate inventory [13]	26–43	Under-50 low case is 47; the gap is CMVP mapping (9–25 hours) and evidence, which the tier excludes
PQC Consultancy Tier 2: up to 500 assets, 2–4 weeks, \$27,500 [13]	110–183	Matches the 50–250 typical of 180
Axis12 one-time Silver: 3 sensors, under 10,000 assets, £15,000, about \$20,000 (UK, ex VAT) [14]	80–133	Between the 50–250 low and typical; sensor-driven, no FIPS mapping
DigiCert packaged PKI services: 12 / 24 / 40 / 100 fixed hours by company size [15]	PKI scope only	Close to the model's certificate and deliverable lines per band
QRAMM: under 500 employees 2–4 weeks; 500–5,000 1–3 months, with the warning	80–160; 160–480 at one consultant full time	Consistent with the first three bands

that inventory "always takes longer than expected" [16]		
---	--	--

6. The yearly refresh

Certificate status changes without notice to the contractor: CMVP keeps modules Active for five years (two for interim validations) [3], OS patches move systems off the validated version, and the 140-2 sunset changed every 140-2 status on one day. The refresh model [Derived]: 25 percent of scoping; 50 percent of discovery, service and certificate work; 25 percent of OS, appliance, application and cloud review; 0.25 hour per module to re-verify status; full remapping for 20 percent module churn; 40 percent of deliverables; plus 10 percent.

	Under 50	50–250	250–1,000	Over 1,000
Refresh hours (range; typical)	18–45; 30	39–100; 65	88–239; 160	220–895; 540
At \$150 / \$250 / \$400	\$4,500 / \$7,500 / \$12,000	\$9,750 / \$16,250 / \$26,000	\$24,000 / \$40,000 / \$64,000	\$81,000 / \$135,000 / \$216,000

That is 36 to 39 percent of the initial hours. The first refresh after September 2026 is heavier: if every module needs remapping rather than 20 percent, the under-50 refresh rises from 30 to about 44 hours ($27.4 - 3.2 + 16.2 = 40.4$, plus 10 percent).

7. What makes the number move

- **Module count.** Each additional ten distinct modules adds 7.5 to 10 hours, \$1,900 to \$2,500 at the central rate. Consolidating OS builds and appliance models is the cheapest lever.
- **Application count.** Application review is the largest line in every band (14 of 84 hours under 50; 260 of 1,410 over 1,000). Each CUI application removed from the boundary saves about an hour.
- **Enclave scoping.** Holding the fixed lines (scoping, discovery, deliverables: 25 hours under 50) and halving every count-driven line gives $50.8 \times 1.1 = 56$ hours, 30 percent less [Derived].
- **Existing tooling.** Discovery, service triage and certificate review are 10 of 84 hours under 50 but 469 of 1,410 over 1,000. Tooling matters at scale and barely at all for small firms.
- **Rate tier.** \$150 to \$400 is a factor of 2.67 on the same hours; the hours range within a band is a factor of about 2.8. Scope uncertainty moves the number as much as the rate does.
- **In-house staffing.** In-house labor is \$81 to \$97 an hour, but GAO found 18 of 24 federal agencies "reported a lack of expertise in cryptography and developing related inventories," 19 used no automated tools and 23 had no documented maintenance process [17]. The model applies no expertise penalty, so in-house hours are likely understated.

8. Questions and answers

Question	Answer
Is a product list with "FIPS 140-2 compliant" claims an inventory?	No. The evidence is a certificate number, the version it names, the operational environment it covers and the approved-mode configuration. [2][3]
Can the whole inventory go on a POA&M?	Only "encryption employed but not FIPS-validated" items, for 180 days. Items with no encryption cannot. [1]
Our 140-2 certificates are Historical. Do we fail?	No. NIST supports use in existing systems; the SSP should state the status and the plan for 140-3 modules. [3][4]
Why does a gap assessment not produce this?	Its cryptography share is about three to eight hours (Section 2);

	the list takes 47 to 130 hours for the smallest band.
Does tooling remove the manual work?	It shortens discovery, not module identification, CMVP lookup or evidence writing. [9]
How often is the refresh needed?	At least annually and before each affirmation. [3]

9. Steps

1. Count distinct modules, not devices; the module count drives the mapping cost. Get it before asking for quotes.
2. Ask any bidder for hours by task against Section 3. A fixed price that cannot be decomposed this way is a readiness scan, not a 3.13.11 inventory.
3. Budget the yearly refresh as a line at roughly 37 percent of the initial effort.
4. Record the 140-2 Historical position in the SSP now; it is the part an assessor looks at first.

10. What this does not cover

Remediation costs (enclaves, GCC High licensing, replacing unvalidated products), discovery tool licenses, C3PAO fees, a vendor's own FIPS validation, post-quantum migration beyond the inventory, and legal exposure under the annual affirmation. The hours model is our estimate, calibrated against Section 5, not measured from a published dataset, because none exists. UK prices are comparators, not US market prices. Vendor-claimed rates are marked as such; the government figures and published price lists are the hard data.

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. 32 CFR Part 170, CMMC Program final rule, 89 FR 83092, 15 October 2024: §170.21, §170.24(c), preamble responses on FIPS scoring, and the regulatory impact analysis (labor rates, hours, 30 percent fringe and G&A factor). <https://www.govinfo.gov/content/pkg/FR-2024-10-15/html/2024-22905.htm> (accessed 27 October 2026)
2. DoD, NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, 24 June 2020, §5 and Annex A. <https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf> (accessed 27 October 2026)
3. NIST, Cryptographic Module Validation Program (updated 21 August 2026). <https://csrc.nist.gov/projects/cryptographic-module-validation-program> (accessed 27 October 2026)
4. NIST, FIPS 140-3 Transition Effort (updated 13 April 2026). <https://csrc.nist.gov/projects/fips-140-3-transition-effort> (accessed 27 October 2026)
5. NIST CMVP, certificate #4766, status Historical. <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4766> (accessed 27 October 2026)

6. Secureframe, CMMC certification cost (editor's note 13 July 2026). Secondary, vendor claim.
<https://secureframe.com/hub/cmmc/certification-cost.md> (accessed 27 October 2026)
7. Totem Technologies, compliance pricing (© 2026). Published price list. <https://www.totem.tech/cybersecurity-compliance-pricing/> (accessed 27 October 2026)
8. Etactics, summary of the CyberAB town hall of 27 September 2022 (14 October 2022). Secondary.
<https://etactics.com/blog/cyberab-september-town-hall> (accessed 27 October 2026)
9. OMB, Report on Post-Quantum Cryptography, July 2024, pp. 5–6 and 12. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf (accessed 27 October 2026)
10. BLS, Occupational Outlook Handbook, Information Security Analysts, May 2025 median \$62.11 per hour (modified 27 August 2026). <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> (accessed 27 October 2026)
11. Makologics, IT buyer's guide (21 April 2026). Secondary, vendor claim. <https://makologics.com/resources/it-buyers-guide>
12. SBA, News Release 26-73, 13 July 2026. <https://legacy.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors> (accessed 27 October 2026)
13. PQC Consultancy, pricing (© 2026). Published price list. <https://pqcconsultancy.com/pricing.html> (accessed 27 October 2026)
14. Axis12, G-Cloud 15 pricing document, 29 January 2026. Published price list, UK.
<https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-15/documents/92214/380441517909314-pricing-document-2026-01-29-1702.pdf> (accessed 27 October 2026)
15. DigiCert, Professional Services packaged services overview (2026). Vendor-published effort.
<https://www.digicert.com/content/dam/digicert/pdfs/datasheet/digicert-ps-packaged-services-overview-en.pdf> (accessed 27 October 2026)
16. QRAMM, Quantum readiness assessment guidance (December 2024). Secondary, nonprofit.
<https://qramm.org/learn/quantum-readiness-assessment.html> (accessed 27 October 2026)
17. GAO-27-108740, Quantum Computing: Federal Actions Needed to Prepare for Emerging Cyber Threat, 6 October 2026. <https://files.gao.gov/reports/GAO-27-108740/index.html> (accessed 27 October 2026)

Change log

- 1.0, 27 October 2026: first publication.