

The Post-Quantum Deadlines That Now Bind Federal Contractors and Vendors

The Post-Quantum Deadlines That Now Bind Federal Contractors and Vendors

Adamas Systems · HARDAC-ADV-2026-04 · 27 October 2026 · HARDAC Industries LLC. General guidance, not legal advice or an assessment finding.

HARDAC Industries LLC — Security Advisory HARDAC-ADV-2026-04

Published 27 October 2026 · Version 1.0

Author: HARDAC Industries LLC. Canonical URL: to be assigned on publication. Change log: v1.0, initial release.

Summary

Between November 2025 and October 2026 the federal post-quantum cryptography (PQC) requirements turned from targets into dated obligations with gates. The Department of War (DoW) CIO memorandum of 18 November 2025 made DoW approval a precondition for any component testing, piloting or buying PQC technology, and ended pre-shared-key and symmetric "quantum resistance" on 31 December 2030. Executive Order 14412 (22 June 2026) set 31 December 2030 and 2031 deadlines for the government's most sensitive systems and ordered the FAR Council to propose a rule requiring "covered contractors" to comply with the PQC FIPS by 31 December 2030. OMB M-26-15 (24 June 2026) told civilian agencies to keep an automated cryptographic inventory and to write PQC readiness into vendor requirements. CNSA 2.0 requires new national security system acquisitions to be compliant from 1 January 2027. NIST finalized IR 8547 on 27 October 2026: quantum-vulnerable public-key algorithms are deprecated after 2030 and disallowed after 2035.

This advisory lays those instruments out as one timeline, quotes the operative language, and states what each asks of a contractor and of a vendor selling into DoW. The inventory that NIST SP 800-171 control 3.13.11 and PCI DSS 12.3.3 already require is the inventory every deadline builds on, and the first contractual date, the FAR proposal, is weeks away.

1. One timeline

Date	Instrument	Who it binds	What it requires	Source
13 Aug 2024	FIPS 203, 204, 205	Anyone claiming FIPS PQC	ML-KEM, ML-DSA, SLH-DSA become the approved PQC algorithms	[5][6][7]
18 Nov 2025	DoW CIO memorandum	DoW Components; vendors through them	Intake approval before PQC testing, piloting, investment or acquisition; inventory of all cryptography; migration leads in 20 days; QKD, non-FIPS RNG and commercial PSK "quantum resistance" barred	[1]; (S) [2][3]
23 Jan 2026	CISA PQC product categories	Federal buyers (guidance)	"acquire only PQC-capable products" in listed categories	[12]

22 Jun 2026	Executive Order 14412 (91 FR 38483)	Agencies; FAR Council; "covered contractors"	HVAs and high impact systems on PQC key establishment by 31 Dec 2030, signatures by 31 Dec 2031; FAR proposed rule in 180 days requiring covered contractors to comply with the PQC FIPS by 31 Dec 2030	[8]
23 Jun 2026	DoW PQC Strategy	DoW Components	Support PQC or be phased out by 31 Dec 2030; PQC in use by 31 Dec 2031 (S)	[4][16]
24 Jun 2026	OMB M-26-15	Civilian agencies; vendors through procurement	Plans in 120 days; automated inventory feeding a CBOM; vendor requirements include PQC readiness; TLS 1.3 by 2 Jan 2030	[9]
22 Oct 2026 (derived: 24 Jun + 120 days)	M-26-15 plans due	Civilian agencies	Plans, with "a third-party coordination plan," at OMB and ONCD	[9]
27 Oct 2026	NIST IR 8547 (final)	NIST-conformant systems	Quantum-vulnerable public-key algorithms "Deprecated after 2030," "Disallowed after 2035"	[13]
19 Dec 2026 (derived: 22 Jun + 180 days)	FAR proposed rule due	Covered contractors (undefined)	Proposed rule; compliance by 31 Dec 2030	[8]
1 Jan 2027	CNSA 2.0	New NSS acquisitions	Must be CNSA 2.0 compliant (S)	[14][15]
19 Mar 2027 (derived: 22 Jun + 270 days)	EO 14412 §5(d), §6(d)	CISA/NIST; FAR Council	CBOM minimum elements; VDP rule covering "lack of encryption and the use of non-FIPS approved algorithms"	[8]
31 Dec 2030	EO 14412; DoW memo; FAR rule; CNSA 2.0; IR 8547	Agencies, DoW, covered contractors, NSS	PQC key establishment on HVAs and high impact systems; DoW PSK and symmetric "quantum resistance" retired; contractor FIPS compliance date; CNSA 2.0 exclusive for software signing and networking; NIST deprecation begins	[8][1][14][13]
31 Dec 2031	EO 14412; DoW memo and strategy	Agencies, DoW	PQC signatures on HVAs and high impact systems; DoW CSfC extension ends; PQC in use across DoW	[8][1][4]
2033 / 2035	CNSA 2.0; IR 8547; M-26-15	NSS; all	CNSA 2.0 exclusive for browsers, servers, cloud, operating systems (S); quantum-vulnerable algorithms disallowed and federal migration complete by	[15][13][9]

			2035	
--	--	--	------	--

Dates marked derived are computed from the instrument's own clock and do not appear in its text. (S) marks figures taken from secondary coverage.

2. DoW CIO memorandum, 18 November 2025

The memorandum is posted at dowcio.war.gov and dodcio.defense.gov [1]. Both hosts refused automated retrieval for this advisory (HTTP 403), so the language below is as reported by secondary coverage [2][3] and should be checked against the memo before use in a proposal.

- Two gates.** Components must obtain "cryptographic intake approval" from the DoW CIO PQC Directorate before testing, evaluating, piloting, investing in, using or acquiring PQC-enabling or PQC-related technology, and "cryptographic deployment approval" before deployment. One summary states the intake scope includes "discovery, inventory, migration, and enablement activities." If the Directorate finds security issues, tests and pilots stop.
- Inventory and leads.** Components inventory "any type of cryptography used" across NSS, business and weapons systems, cloud, mobile, physical access control, IoT, unmanned systems and operational technology, "regardless of classification, location, connection, type, purpose, or use." PQC migration leads are named within 20 days, refreshed each 30 September.
- Bars.** Quantum key distribution and related quantum keying, and non-FIPS random number generation, are barred for confidentiality, authenticity or integrity absent an exception. New commercial pre-shared-key (PSK) "quantum resistance" pilots and acquisitions are barred immediately.
- Dates.** PSK solutions not provisioned through NSA's Key Management Infrastructure move to asymmetric PQC key establishment by 31 December 2030. Symmetric key establishment, agreement and distribution used for quantum resistance sunsets 31 December 2030, extended to 31 December 2031 for solutions registered with NSA's Commercial Solutions for Classified (CSfC) program.

Practical obligation. The memo binds DoW Components, not contractors. It reaches a contractor building or operating a DoW system through the Component's inventory and approval process, and a vendor through a buyer that cannot test, pilot or buy without intake approval (Section 8).

3. CNSA 2.0 (NSA)

NSA's advisory Announcing the Commercial National Security Algorithm Suite 2.0 (September 2022) and its FAQ v2.1 (December 2024) are posted on media.defense.gov [14]. Both refused automated retrieval (HTTP 403); figures below are from secondary coverage [15].

Algorithms as reported: AES-256; ML-KEM-1024 (FIPS 203) for key establishment; ML-DSA-87 (FIPS 204) for signatures; SHA-384 or SHA-512; LMS and XMSS (SP 800-208) for software and firmware signing. SLH-DSA and the smaller ML-KEM and ML-DSA parameter sets are not CNSA 2.0. Transition dates as reported (support and prefer / exclusive use): software and firmware signing 2025 / 2030; web browsers, servers and cloud 2025 / 2033; traditional networking equipment 2026 / 2030; operating systems 2027 / 2033; niche equipment 2030 / 2033; custom and legacy equipment, update or replace by 2033. From 1 January 2027, new NSS acquisitions must be CNSA 2.0 compliant unless an exception is noted.

Practical obligation. A contractor supplying or operating NSS, or a vendor whose product will be bought for NSS after 1 January 2027, needs the CNSA 2.0 parameter sets, not "FIPS 203 support." ML-KEM-768 is NIST-approved and not CNSA 2.0.

4. Executive Order 14412, 22 June 2026

Signed 22 June 2026, published at 91 FR 38483 on 25 June 2026 [8]. The operative text:

- Policy: "executing the transition of Federal information systems to National Institute of Standards and Technology (NIST)-approved Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography (PQC), and to assist critical infrastructure owners and operators with their transitions." (§1)
- Agencies: OMB guidance requiring each agency to "transition all HVAs and high impact systems to use PQC for key establishment by December 31, 2030" and "to use PQC for digital signatures by December 31, 2031," excluding national security systems. (§4(b))
- Contractors: "Within 180 days of the date of this order, the Federal Acquisition Regulatory Council (FAR Council) ... shall publish a proposed rule amending the Federal Acquisition Regulation (FAR) to require covered contractors to comply by December 31, 2030, with NIST's FIPS, including all applicable FIPS incorporating PQC compliant algorithms." (§6(c))
- Vulnerability disclosure: within 270 days, a proposed rule so that covered contractors' VDPs "incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS approved algorithms." (§6(d))
- CBOM: within 270 days, CISA and NIST publish "the minimum elements for a cryptographic bill of materials," which "shall enable the automated assessment of the cryptographic assets utilized by a hardware or software element." (§5(d)) Within 180 days, NIST revises CMVP processes "to accelerate validations of cryptographic modules." (§6(b))

Practical obligation. The order does not define "covered contractors"; the proposed rule, due 19 December 2026 (derived), will. The obligation is "NIST's FIPS," which includes FIPS 140-3 validation, not PQC alone: a contractor on unvalidated cryptography has the same gap under this rule as under 3.13.11. No proposed rule had been published at this advisory's date.

5. OMB M-26-15, 24 June 2026

M-26-15, Execution of the Migration to Post-Quantum Cryptography, is the §4(b) guidance. It "does not apply to national security systems." [9] The operative text:

- "Agencies must execute a prioritized migration of cryptographic systems used in information systems that they own or operate with the objective of mitigating as much quantum risk as feasible by December 31, 2030."
- Plans to OMB and ONCD "no later than 120 days from the date of this memorandum" (22 October 2026, derived), containing "The methodologies and automated tools used for the cryptographic inventory" and "A third-party coordination plan."
- "The foundation of the migration plan is a dynamic, continuously updated inventory of all cryptographic assets. This inventory should be created and maintained through automated tools wherever possible ... This data should populate a central Cryptographic Bill of Materials (CBOM)."
- Vendors: agencies "should ensure that any requirements for products used by the agency in those categories include PQC integration" (the CISA categories [12]); the program office "Ensures vendor requirements include PQC-readiness and cryptographic agility provisions."

- Phases: discovery 2026–2027; pilots 2027–2028; key-establishment migration 2028–2030; signatures 2031; full migration 2035. TLS 1.3 "not later than January 2, 2030." Plans "must align" with NIST IR 8547. Appendix A: "Symmetric-key-based protocols should also be avoided."

Practical obligation. The inventory covers systems the agency owns "or operate[s]," including contractor-operated systems, and each plan now at OMB contains a third-party coordination plan. Expect the program office to ask for the contractor's inventory and migration dates, and PQC readiness and agility language in new solicitations.

6. NIST: standards, schedule, validated modules

- FIPS 203 (ML-KEM), 204 (ML-DSA) and 205 (SLH-DSA), published 13 August 2024, are the "FIPS incorporating PQC compliant algorithms" that EO 14412 names [5][6][7].
- NIST IR 8547 was finalized 27 October 2026, obsoleting the November 2024 draft [13]: "NIST will deprecate quantum-vulnerable public-key cryptography after 2030 and disallow its use under NIST standards and guidelines after 2035." Its tables list ECDSA, EdDSA and RSA signatures, and finite-field DH/MQV, elliptic-curve DH/MQV and RSA key establishment, each "Deprecated after 2030" and "Disallowed after 2035." The window "does not alter the earlier deadlines that apply to high value assets, high impact systems, and other high-sensitivity federal systems under EO 14412 and OMB M-26-15." SHA-1 "will be disallowed for use in FIPS-validated cryptographic modules after 2030."
- CMVP: AWS-LC 3 Cryptographic Module (static), certificate #5314, validated 5 June 2026, Active, lists ML-KEM KeyGen and EncapDecap as approved [10]. CryptoComply Native Go Module, #5349, validated 23 June 2026, Active, lists the same [11]. Neither lists ML-DSA; a validated PQC signature path is a separate check.

Practical obligation. "Deprecated" means the data owner examines the risk and decides; "Disallowed" means the algorithm may not be used for that purpose. From 2031 a validated module running RSA or ECDH is running a deprecated algorithm, and the system security plan has to say so.

7. What a contractor should have in hand, by when

Now: the inventory. SP 800-171 Rev. 2 requirement 3.13.11: "Employ FIPS-validated cryptography when used to protect the confidentiality of CUI." [17] 32 CFR 170.24: "FIPS-validated encryption (CMMC Level 2 security requirement SC.L2-3.13.11) is required to protect the confidentiality of CUI," 3 points deducted if encryption is not validated, 5 if not employed [18]. PCI DSS v4.0.1 requirement 12.3.3, mandatory since 31 March 2025, requires cipher suites and protocols in use to be documented and reviewed at least every 12 months, including "an up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used" [19] (wording as reproduced by [20]; the standard sits behind a license acceptance). Every instrument above starts from that record: where cryptography protects data, which module and version, which algorithm and parameter set, which certificate and status. Add two columns: algorithm family, so RSA, ECDH and ECDSA uses can be listed, and the year the protected data stops mattering (M-26-15's "data expected to remain mission-sensitive in 2030").

By end of 2026: module status and gap list. For each module: 140-3 status, whether it carries ML-KEM or ML-DSA, and whether the parameter set meets the customer's bar (NIST-approved for civilian and CUI work; ML-KEM-1024 and ML-DSA-87 for NSS). List each quantum-vulnerable item with no validated PQC replacement.

By the FAR proposal (about 19 December 2026): the migration plan. Dated, mirroring M-26-15's phases, key establishment first and signatures second, in a form an agency can drop into its third-party coordination plan. Comment on the proposed rule: "covered contractors" and subcontractor flow-down will be settled there.

Procurement language. Solicitations and subcontracts should carry the algorithm and parameter-set requirement (NIST-approved PQC, or CNSA 2.0 for NSS work); CMVP validation with the PQC algorithm inside the boundary; a cryptographic-agility clause; and a right to the supplier's inventory or CBOM once the minimum elements are published (about 19 March 2027).

8. Vendors selling cryptographic or security products into DoW

Three things changed on 18 November 2025, as reported [2][3]:

1. **The intake gate.** A Component cannot test, pilot, invest in or acquire the product without intake approval from the DoW CIO PQC Directorate, or deploy it without deployment approval, and must submit test and acquisition artifacts for review. A vendor without a package that supports that submission (algorithms and parameter sets, module certificate numbers, interoperability evidence, agility design) is asking a Component to start a process it cannot finish.
2. **The bars.** Commercial PSK "quantum resistance" is barred for new pilots and acquisitions. QKD, quantum networking for keying, and random number generation that is not FIPS-approved are barred for confidentiality, authenticity or integrity absent an exception. A product that markets any of these as its quantum-resistance mechanism is, on the reported text, not buyable by a Component.
3. **The sunset.** Existing PSK and symmetric key-establishment "quantum resistance" ends 31 December 2030 (2031 for CSfC-registered solutions); M-26-15 adds that "Symmetric-key-based protocols should also be avoided." A roadmap that reaches 2030 on symmetric key distribution has no federal buyer at the end of it.

For NSS sales, CNSA 2.0 sits on top: from 1 January 2027, ML-KEM-1024 and ML-DSA-87, and LMS or XMSS for firmware signing (S) [15].

9. Questions

Question	Answer
Does anything bind my company today?	DFARS 252.204-7012 and 3.13.11 have bound defense contractors since 2017; PCI DSS 12.3.3 since March 2025. The PQC instruments bind agencies and DoW Components now and reach contractors through their inventories, plans and solicitations. The first direct contractor rule is the FAR proposal due about 19 December 2026, compliance by 31 December 2030. [8][17][18][19]
Does "comply with NIST's FIPS" mean PQC only?	No. The text reads "NIST's FIPS, including all applicable FIPS incorporating PQC compliant algorithms." FIPS 140-3 is a FIPS; unvalidated cryptography is a gap under this rule regardless of PQC. [8]
Is ML-KEM-768 enough?	For civilian and CUI work, ML-KEM is NIST-approved at all three parameter sets. For NSS, CNSA 2.0 specifies ML-KEM-1024 and ML-DSA-87 only (S). [15]
Is a "PQC-ready" product with no validated module acceptable for CUI?	No. 3.13.11 asks whether the module is validated; an algorithm outside a validated boundary does not satisfy it. Validated modules with ML-KEM inside the boundary exist (#5314, #5349). [10][11][18]
Can I keep using RSA and ECDH through 2030?	Under NIST's schedule, acceptable through 2030, deprecated after, disallowed after 2035. Under EO 14412 and M-26-15, HVAs and high impact systems must be on PQC key establishment by 31 December 2030, so a contractor operating one has the earlier date. [13][8][9]
Is QKD or a pre-shared-key product a path to DoW quantum resistance?	On the reported memo text, no: both are barred, and PSK sunsets 31 December 2030. Coverage of the DoW strategy reports a

	direction to add PQC to CMMC [4]; no rule change has been published. [2][3]
--	---

What this does not cover

The FAR CUI rule re-proposed 23 June 2026 (91 FR 37550), export classification of PQC products, the DoW strategy's High Assurance ECU track and NSA Type 1 certification, state and sector rules (NYDFS, CJIS, HIPAA), and the CMMC Phase 2 suspension, which HARDAC-ADV-2026-01 addresses. The DoW memorandum and the NSA CNSA 2.0 documents were not retrievable by automated means at publication; where quoted, the text is from labeled secondary coverage and should be confirmed against the primary before 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 instrument's current text and their own assessor's and contracting officer's expectations.

Sources

Primary sources are rule text, orders, memoranda and NIST pages; (S) marks secondary. All accessed 27 October 2026.

1. DoW CIO, Preparing for Migration to Post Quantum Cryptography, memorandum, 18 November 2025.
<https://dowcio.war.gov/Portals/0/Documents/Library/PreparingForMigrationPQC.pdf> ;
<https://dodcio.defense.gov/Portals/0/Documents/Library/PreparingForMigrationPQC.pdf> . Not retrievable by automated means (HTTP 403) at publication.
2. (S) PostQuantum.com, Pentagon CIO memo puts post-quantum crypto on a procurement leash.
<https://postquantum.com/security-pqc/pentagon-cio-dow-dod-memo-pqc/>
3. (S) DigiCert, No Time to Wait: PQC Pressure from the Dept. of War, 17 December 2025.
<https://www.digicert.com/blog/no-time-to-wait-pqc-pressure-from-the-dept-of-war>
4. (S) PostQuantum.com, DoW PQC Strategy: The Defense Half of the EO Mandate, covering the DoW PQC Strategy of 23 June 2026 (<https://dowcio.war.gov/Portals/0/Documents/Library/DoW-PQC-Strategy.pdf>).
<https://postquantum.com/security-pqc/dow-pqc-strategy-eo-14412/>
5. NIST, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, 13 August 2024.
<https://csrc.nist.gov/pubs/fips/203/final>
6. NIST, FIPS 204, Module-Lattice-Based Digital Signature Standard, 13 August 2024.
<https://csrc.nist.gov/pubs/fips/204/final>
7. NIST, FIPS 205, Stateless Hash-Based Digital Signature Standard, 13 August 2024.
<https://csrc.nist.gov/pubs/fips/205/final>
8. Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, 22 June 2026; 91 FR 38483, 25 June 2026 (FR Doc. 2026-12909). <https://www.govinfo.gov/content/pkg/DCPD-202600417/pdf/DCPD->

202600417.pdf ; <https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks>

9. OMB, M-26-15, Execution of the Migration to Post-Quantum Cryptography, 24 June 2026.
<https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf>
10. NIST CMVP, certificate #5314, AWS-LC 3 Cryptographic Module (static), validated 5 June 2026.
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5314>
11. NIST CMVP, certificate #5349, CryptoComply Native Go Module, validated 23 June 2026.
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5349>
12. CISA, Product Categories for Technologies That Use Post-Quantum Cryptography Standards, 23 January 2026.
<https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards>
13. NIST, IR 8547, Transition to Post-Quantum Cryptography Standards, final, October 2026 (published 27 October 2026; obsoletes the 12 November 2024 draft). <https://csrc.nist.gov/pubs/ir/8547/final> ;
<https://nvlpubs.nist.gov/nistpubs/ir/2026/NIST.IR.8547.pdf>
14. NSA, Announcing the Commercial National Security Algorithm Suite 2.0, September 2022, and CNSA 2.0 FAQ v2.1, December 2024. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF ; https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF . Not retrievable by automated means (HTTP 403) at publication.
15. (S) PostQuantum.com, CNSA 2.0 Complete Guide, and NSA CNSA 2.0 FAQ v2.1 Update.
<https://postquantum.com/cnsa-2-0/complete-guide/> ; <https://postquantum.com/security-pqc/nsa-cnsa-2-0-faq-v2-1-update/>
16. (S) Quantum Computing Report, Department of War Unveils Enterprise Post-Quantum Cryptography Strategy, 1 July 2026. <https://quantumcomputingreport.com/department-of-war-unveils-enterprise-post-quantum-cryptography-strategy-to-insulate-defense-networks-by-2031/>
17. NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020 (updated 28 January 2021), requirement 3.13.11.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf>
18. 32 CFR 170.24(c)(4)(ii), CMMC Program final rule, 15 October 2024.
<https://www.law.cornell.edu/cfr/text/32/170.24>
19. PCI Security Standards Council, PCI DSS v4.0.1, requirement 12.3.3 (document library; license acceptance required). https://www.pcisecuritystandards.org/document_library/
20. (S) Encryption Consulting, PCI DSS v4 Requirement on CBOM. <https://www.encryptionconsulting.com/pci-dss-v4-requirement-on-cbom/>