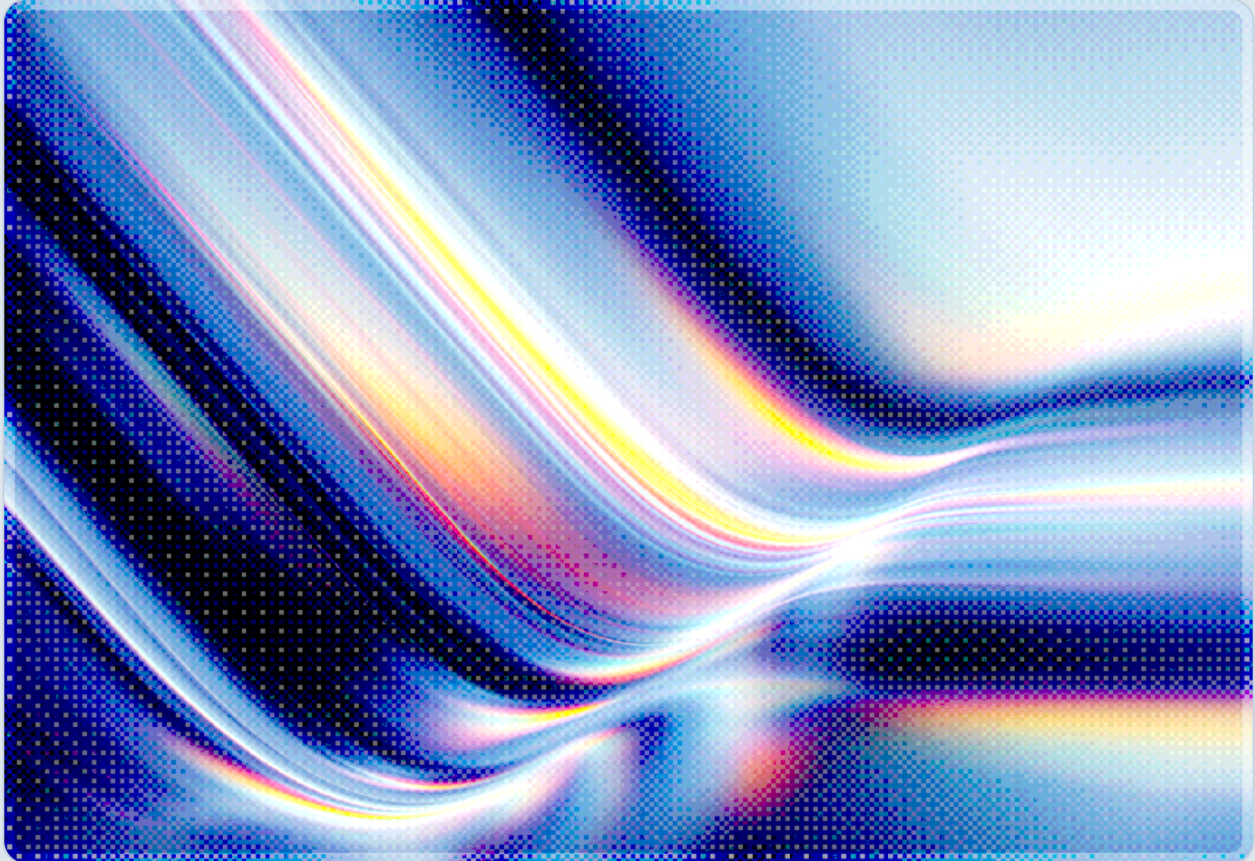


# NIST IR 8547 Final: Post-Quantum Deadlines Become Vendor Requirements

What the 2030 Deprecation and 2035 Disallowance Dates Mean for Products, Contracts, and Cloud Services

2026-10-30

 AI-assisted Rapid Research



CSAI

cloud  
security  
alliance®

**© 2026 Cloud Security Alliance. Some rights reserved.**

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

*This document was generated with AI assistance and has not undergone official CSA review and approval processes.*

---

## Key Takeaways

On October 27, 2026, NIST published the final version of NIST IR 8547, *Transition to Post-Quantum Cryptography Standards*, nearly two years after the initial public draft of November 2024 [1][2]. The final report keeps the draft's headline dates but changes what they apply to. Every approved quantum-vulnerable public-key algorithm is now deprecated after 2030 and disallowed under NIST standards and guidelines after 2035, regardless of key size [1]. The draft deprecated only the 112-bit parameter sets after 2030, so RSA-3072, P-256 ECDSA, and Ed25519 had appeared acceptable until 2035 [2][12]. That distinction no longer exists. Products built on today's most common "strong" classical defaults have just over four years before they become deprecated, and less time for products sold into federal high value assets and high impact systems.

The final report states that it supports the implementation of Executive Order 14412 and OMB Memorandum M-26-15, which in turn require agencies to align their plans with IR 8547 [1][5]. Those instruments require federal high value assets (HVAs) and high impact systems to use post-quantum cryptography (PQC) for key establishment by December 31, 2030, and for digital signatures by December 31, 2031 [1][3][5]. Through federal procurement, these dates become supplier obligations. The order directs the FAR Council to propose a rule requiring covered contractors to comply with NIST's PQC-related FIPS by December 31, 2030 [3]. OMB tells agencies to build PQC integration into product requirements and to settle PQC responsibilities with FedRAMP cloud providers [5].

For cloud providers, software vendors, and the enterprises that buy from them, the most immediate consequence concerns classical-only public-key cryptography. At any key size, it becomes deprecated after 2030. CSA recommends treating it as end-of-life in roadmaps, contracts, and risk registers, because continued use will require documented risk acceptance and is effectively barred earlier for federal HVAs and high impact systems. The path forward is also clearer than it was. Hybrid key establishment, such as ML-KEM combined with ECDH, is explicitly accommodated in FIPS 140 validation provided at least one component is NIST-approved, and NIST's designation of ML-KEM-768 as its recommended default parameter set gives vendors and buyers a common baseline to specify [1].

Two near-term dates deserve attention. The FAR proposed rule is due around December 19, 2026, under the order's 180-day clock, and CISA's minimum elements for a cryptographic bill of materials (CBOM) are due around March 19, 2027, under its 270-day clock [3]. Organizations outside the federal market are not

bound by these deadlines. NIST nonetheless explicitly positions the report as a blueprint for critical infrastructure and other organizations [1]. In CSA's assessment, vendors are unlikely to keep separate federal and commercial cryptographic baselines for long.

## Background

NIST finalized its first three post-quantum standards in August 2024: FIPS 203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA) for digital signatures, and FIPS 205 (SLH-DSA) for stateless hash-based signatures [7][8][9]. In March 2025 it selected HQC as an alternative key-encapsulation mechanism based on different mathematics, and a FIPS for HQC is under development [11][1]. With those standards published, the open question for the industry was no longer *which* algorithms to adopt but *when* classical algorithms would stop being acceptable. NIST IR 8547 answers that question. The November 2024 draft proposed a two-step schedule (deprecation after 2030, disallowance after 2035) and drew 25 written public comments before its January 2025 close [2].

Policy then moved faster than the standards process. Executive Order 14412, *Securing the Nation Against Advanced Cryptographic Attacks*, was signed on June 22, 2026, and published in the Federal Register on June 25 [3][4]. Some early commentary misidentified this order by number; the Federal Register and NIST's final report identify it as EO 14412 [4][1]. The order sets the 2030 and 2031 migration deadlines for HVAs and high impact systems. It also directs NIST to revise Cryptographic Module Validation Program (CMVP) processes to accelerate module validations, directs CISA to publish CBOM minimum elements, and directs the FAR Council to propose contractor rules on both PQC compliance and cryptographic vulnerability disclosure [3].

OMB Memorandum M-26-15, *Execution of the Migration to Post-Quantum Cryptography*, followed on June 24, 2026. It required agencies to submit PQC migration plans within 120 days, which works out to roughly October 22, 2026, and it laid out a five-phase program running from discovery (2026–2027) to full migration (2035) [5]. The memorandum states that agencies "must align their plans with NIST Internal Report (IR) 8547 ... or successor document" [5]. Because the final report arrived about five days after the derived plan deadline, plans submitted on time were presumably written against the 2024 draft. Agencies may therefore need to revisit them now that the stricter deprecation scope is final. M-26-15 does not apply to national security systems, which follow a separate governance track [5].

# Security Analysis

## What Changed Between Draft and Final

The most consequential change is the scope of deprecation, because it moves the classical algorithms most products use today into the 2030 deprecation category. The final report explains that NIST's earlier long-range plans in SP 800-57 Part 1 would have disallowed 112-bit public-key schemes on January 1, 2031. Instead, NIST "will deprecate all quantum-vulnerable digital signature algorithms after 2030 and disallow their use under NIST standards and guidelines after 2035" [1]. The same treatment applies to finite-field and elliptic-curve Diffie-Hellman, MQV, and RSA key establishment [1]. The table below summarizes the final schedule.

| Algorithm family          | Standard   | Parameters covered          | After 2030 | After 2035 |
|---------------------------|------------|-----------------------------|------------|------------|
| RSA signatures            | FIPS 186   | ≥112-bit classical strength | Deprecated | Disallowed |
| ECDSA                     | FIPS 186   | ≥112-bit classical strength | Deprecated | Disallowed |
| EdDSA                     | FIPS 186   | ≥128-bit classical strength | Deprecated | Disallowed |
| Finite-field DH and MQV   | SP 800-56A | ≥112-bit classical strength | Deprecated | Disallowed |
| Elliptic-curve DH and MQV | SP 800-56A | ≥112-bit classical strength | Deprecated | Disallowed |
| RSA key establishment     | SP 800-56B | ≥112-bit classical strength | Deprecated | Disallowed |

Source: NIST IR 8547 final, Tables 2 and 4 [1].

The word "deprecated" carries a specific meaning in NIST usage, and it should not be read as "banned." A deprecated algorithm "may be used, but there is some security risk," and "the data owner must examine this risk potential and decide whether to continue" [1]. For commercial organizations, deprecation after

2030 therefore creates a documented risk-acceptance obligation rather than a prohibition. For federal HVAs and high impact systems, the report states that continued use of deprecated algorithms "is constrained by the earlier migration deadlines established under EO 14412" [1]. In practice, those systems face hard dates of 2030 and 2031, not a five-year grace period.

The final report also sharpens several technical positions. NIST now recommends ML-KEM-768 as the default parameter set because it offers "a large security margin at a reasonable performance cost," and it states that it has no current plans to standardize additional KEMs beyond HQC [1]. Ascon (SP 800-232) has been added to the approved symmetric primitives. The report also notes that the few remaining 112-bit symmetric standards will be disallowed in 2030 [1]. TLS is named as an early migration priority. Agencies must support TLS 1.3 no later than January 2, 2030, and hybrid key-exchange guidance for TLS is deferred to the next revision of SP 800-52 [5][1]. One independent analysis of the two versions notes that the final text removed the draft's statement that "flexibility in migration planning is essential" and added a new section on migrating PIV credentials. The same analysis flags a residual inconsistency between a passage in Section 3.1.2 and the 2035 disallowance date [12].

## Hybrid Cryptography Gets a Validation Path

For vendors, the clarification on hybrid key establishment may matter more in practice than the date changes, because it determines whether products already shipping hybrid modes can keep their validation status. CISA's product-category list already identifies web browsers and cloud services as categories where PQC-capable key establishment is widely available [6][17]. M-26-15 describes a hybrid TLS 1.3 key-exchange model that pairs ML-KEM with a classical exchange [5], and in widely deployed browser and CDN implementations the classical half is typically X25519, as specified in the IETF's X25519MLKEM768 hybrid mechanism [18]. Until now, it was unclear how such constructions would fare in FIPS 140 validation once the classical half became deprecated or disallowed. The final report states that the SP 800-56C composite technique "is allowed, even if T is derived from an unapproved source (including a disallowed algorithm)." It also states that "as long as at least one of the inputs to an approved composite (i.e., hybrid) key-establishment technique comes from an approved key-establishment scheme, the combination can be FIPS 140-validated" [1]. NIST also intends to update SP 800-56C so that either ordering of the shared secrets is permitted, and it points implementers to SP 800-227 for key-combiner guidance [1][10].

This position removes a procurement obstacle: vendors can now ship hybrid modes without risking validation status as the classical component ages out. Buyers should still treat the claim carefully. A validated module that *supports* hybrid ML-KEM does not prove that a given deployment *negotiates* it. On hybrid signatures, NIST is more cautious. It will accommodate dual signatures in validation but notes that

"the security properties of hybrid signatures are complex and need to be carefully analyzed" [1]. Signature migration, which touches certificate authorities, PIV cards, firmware signing, and HSMs, is likely to remain the slower and more operationally disruptive half of the transition.

### How the Deadlines Reach Vendors

NIST IR 8547 is not itself binding on private companies. Its deadlines reach vendors through five mechanisms, summarized in the table below, and their combined effect explains why this report functions as a vendor requirement in practice. Several of these mechanisms run on clocks set by the executive order: §6(b) directs NIST to revise CMVP processes within 180 days, §6(c) gives the FAR Council 180 days to propose the PQC compliance rule, and §5(d) and §6(d) set 270-day clocks for the CBOM minimum elements and the cryptographic vulnerability disclosure rule [3].

| Mechanism            | Instrument                 | What it requires                                                                                                                                                                                 | Status as of 2026-10-30                                      |
|----------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Contract clauses     | EO 14412<br>§6(c)          | FAR Council to propose a rule requiring covered contractors to comply with PQC-related FIPS by December 31, 2030                                                                                 | Proposed rule due ~December 19, 2026 (derived, 180 days) [3] |
| Product requirements | OMB M-26-15                | Agencies to ensure requirements for products in CISA-listed categories include PQC integration; program offices to include PQC-readiness and crypto-agility provisions                           | In effect [5][6]                                             |
| Cloud services       | OMB M-26-15                | Agencies to define PQC responsibilities with FedRAMP-authorized providers within the shared responsibility model; CISA and the Department of War to lead efforts for multi-agency cloud services | In effect [5]                                                |
| Module validation    | EO 14412<br>§6(b); IR 8547 | NIST to revise CMVP processes to accelerate validation of PQC modules; hybrid modes validatable with one approved component                                                                      | Revision due ~December 19, 2026 (derived, 180 days) [1][3]   |

| Mechanism    | Instrument               | What it requires                                                                                                                                     | Status as of 2026-10-30                     |
|--------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Transparency | EO 14412<br>§5(d), §6(d) | CISA minimum elements for a CBOM;<br>FAR rule extending vulnerability disclosure programs to cryptographic weaknesses, including non-FIPS algorithms | Due ~March 19, 2027 (derived, 270 days) [3] |

The procurement mechanisms began operating earlier than the contract rule. CISA published its list of product categories that use PQC standards in January 2026. The list covers categories such as cloud platform and infrastructure services, web browsers, collaboration software, and endpoint encryption, where PQC-capable products are widely available, and it states that organizations "should acquire only PQC-capable products within the listed categories" [6][17]. M-26-15 converts that recommendation into an agency expectation [5]. As a result, vendors in those categories should expect to be evaluated on PQC capability in federal acquisitions now, independent of the FAR timeline.

The final report also addresses hardware vendors directly. Because hardware security modules and TPMs have long design and fabrication lead times, NIST states that "it is a high priority for vendors to initiate the integration of PQC support immediately" [1]. Hardware roots of trust that ship in 2027 and remain in service for a decade will operate well past the 2030 deprecation point. If they cannot be updated, they will likely fall into the replacement-or-decommission category that both NIST and OMB expect agencies to identify [1][5].

## Open Questions and Risks

Several material uncertainties remain. The term "covered contractors" will be defined in the FAR rulemaking. Until a proposed rule is published and finalized through notice and comment, the reach of the flow-down to subcontractors and SaaS suppliers can only be estimated. The order's implementation is "subject to the availability of appropriations," so agency migration pace may vary [3]. SP 800-131A, the document that operationalizes transition schedules for federal use, has not yet been revised to match the final IR, and the hybrid TLS guidance in SP 800-52 is also pending [1]. Finally, the distinction between a product that is PQC-*capable* and a deployment that is PQC-*enabled* gives vendors room to make capability claims that buyers cannot easily verify. The forthcoming CBOM guidance appears intended to address this risk [3].

# Recommendations

## Immediate Actions

Vendors selling into the federal market, including cloud and SaaS providers, should update public PQC roadmaps to reflect the final deprecation scope. Any plan that treated RSA-3072 or P-256 as fully acceptable through 2035 should be revised, because under the final IR those algorithms are deprecated after 2030 and their continued use requires documented risk acceptance. Roadmaps should state, by product line, when ML-KEM (or hybrid ML-KEM) key establishment will be enabled by default, when ML-DSA or SLH-DSA signatures will be supported, and which FIPS 140 validations are in progress. Enterprises should send the same questions to their critical suppliers, focusing first on HSMs, PKI, VPN and network gateways, identity providers, and cloud key management services. Federal agencies whose M-26-15 plans were drafted against the 2024 draft should check whether the plans assumed 2035 viability for 128-bit-and-above classical algorithms and correct them where necessary.

## Short-Term Mitigations

Over the next six to twelve months, organizations should make ML-KEM-768 hybrid key establishment the default for TLS 1.3 and other protocols that protect long-lived sensitive data, ahead of the pending SP 800-52 revision, because it directly mitigates "harvest now, decrypt later" collection [1]. Cryptographic inventories should be automated and continuously updated, as M-26-15 expects, and should be structured so that they can be emitted as a CBOM once CISA publishes its minimum elements [3][5]. Contract language for new and renewing agreements should require PQC readiness and cryptographic agility. That language should include dated commitments, notification of cryptographic changes, and evidence of *enabled* rather than merely *supported* PQC configurations. Organizations should also track the FAR proposed rule, expected around December 2026, and comment on the definition of covered contractors and the flow-down mechanics.

## Strategic Considerations

The signature transition deserves dedicated program investment. It will require re-issuing certificate hierarchies, reprovisioning hardware credentials, and changing firmware and software signing pipelines, and NIST names LMS and XMSS for firmware signing [1]. Product teams should design for cryptographic agility by externalizing algorithm choices into configuration, supporting protocol-level algorithm negotiation with downgrade protection, and avoiding hard-coded key and signature sizes. These are design principles that M-26-15 also calls out [5]. Commercial organizations outside the federal market

should consider adopting the 2030/2035 dates as internal governance milestones. Supply-chain convergence, critical infrastructure expectations, and long data-retention horizons all suggest that federal timelines will become de facto commercial ones. Boards and risk committees should anticipate that deprecated-algorithm risk acceptances are likely to become a recurring audit item after 2030.

## CSA Resource Alignment

CSA's *Post-Quantum Cryptography Key Management* (2026) addresses the key management components that IR 8547 identifies as long-lead-time vendor priorities [13]. Its phased roadmap for modernizing cloud key management covers hybrid key handling, HSM and KMS readiness, and the operational effects of larger PQC keys. Cloud providers and their customers can use the guide to structure the shared-responsibility conversations that M-26-15 now requires for FedRAMP-authorized services.

*The State of Post-Quantum Cryptography* (2018) from CSA's Quantum-Safe Security Working Group provides background on the quantum threat and the post-quantum algorithm families that underpin the transition schedule, including the threat to long-lived encrypted data that motivates early migration [14] [1]. *Quantum-Safe Security Governance with the Cloud Controls Matrix* (2024) maps quantum risk to CCM controls and offers a framework for converting the 2030/2035 dates into auditable control objectives and supplier assessments [15]. Organizations should pair these with the cryptography, encryption, and key management domain and the supply chain management domain of the *AI Controls Matrix (AICM) v1.1* [16]. Those domains provide control language for crypto-agility requirements, CBOM-style inventory, and third-party assurance, and they extend to AI model infrastructure whose training data and model weights carry long-lived confidentiality requirements. CSA STAR assessments offer one channel for cloud providers to disclose PQC migration status to customers ahead of formal FAR requirements.

# References

- [1] Moody, D., Perlner, R., Regenscheid, A., Robinson, A., Cooper, D. "[Transition to Post-Quantum Cryptography Standards \(NIST IR 8547, Final\)](#)." NIST, October 2026. DOI: [10.6028/NIST.IR.8547](#).
- [2] NIST. "[Transition to Post-Quantum Cryptography Standards \(NIST IR 8547, Initial Public Draft\)](#)." NIST, November 2024.
- [3] The White House. "[Securing the Nation Against Advanced Cryptographic Attacks \(Executive Order 14412\)](#)." The White House, June 22, 2026.
- [4] U.S. Government Publishing Office. "[Executive Order 14412—Securing the Nation Against Advanced Cryptographic Attacks \(DCPD-202600417\)](#)." GovInfo, June 2026.
- [5] Office of Management and Budget. "[M-26-15: Execution of the Migration to Post-Quantum Cryptography](#)." The White House, June 24, 2026.
- [6] CISA. "[Product Categories for Technologies That Use Post-Quantum Cryptography Standards](#)." Cybersecurity and Infrastructure Security Agency, January 2026.
- [7] NIST. "[FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard](#)." NIST, August 2024.
- [8] NIST. "[FIPS 204: Module-Lattice-Based Digital Signature Standard](#)." NIST, August 2024.
- [9] NIST. "[FIPS 205: Stateless Hash-Based Digital Signature Standard](#)." NIST, August 2024.
- [10] NIST. "[SP 800-227: Recommendations for Key-Encapsulation Mechanisms](#)." NIST, September 2025.
- [11] NIST. "[NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption](#)." NIST, March 2025.
- [12] Ivezic, M. "[NIST Finalizes Its Post-Quantum Transition Plan, Deprecating RSA and ECC at All Approved Key Sizes After 2030](#)." PostQuantum.com, October 28, 2026.
- [13] Cloud Security Alliance. "[Post-Quantum Cryptography Key Management](#)." Cloud Security Alliance, August 2026.
- [14] Cloud Security Alliance. "[The State of Post-Quantum Cryptography](#)." CSA Quantum-Safe Security Working Group, May 2018.

- [15] Cloud Security Alliance. "[Quantum-Safe Security Governance with the Cloud Controls Matrix](#)." CSA Quantum-Safe Security Working Group, July 2024.
- [16] Cloud Security Alliance. "[AI Controls Matrix \(AICM\) v1.1](#)." Cloud Security Alliance, 2025.
- [17] Infosecurity Magazine. "[CISA Releases List of Post-Quantum Cryptography Product Categories](#)." Infosecurity Magazine, January 2026.
- [18] Kwiatkowski, K., Kampanakis, P., Westerbaan, B. E., Stebila, D. "[RFC 10024: Post-Quantum Traditional \(PQ/T\) Hybrid Key Agreement Mechanisms for TLS 1.3](#)." IETF, 2026.