INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-26 18:40 UTC

2030 PQC Migration Deadline Exposes Critical Cryptographic Inventory Gaps in IT/OT Environments

GOVERNANCE | HIGH | CVSS 7.5

SCC Item ID	SCC-GOV-2026-0084
Type	Governance
Severity	HIGH
CVSS Base Score	7.5
Affected Products	General IT/OT infrastructure across multivendor environments, no specific product or version
Published	2026-06-26T09:30:00
Discovery Source	Rss

Executive Summary

Federal mandates including NIST's finalized post-quantum cryptography standards (FIPS 203, 204, 205) and NSM-10/OMB M-23-02 set 2030 as the deadline for migrating federal and critical infrastructure systems to quantum-resistant cryptography. The primary blocker is not algorithm readiness but cryptographic asset discovery: most organizations cannot locate every instance of quantum-vulnerable cryptography (RSA, ECC, Diffie-Hellman) across their IT and OT environments. Organizations that have not begun inventory work are already behind schedule given typical OT remediation cycles of 3-7 years.

Technical Analysis

NIST finalized three post-quantum cryptography standards in 2024: FIPS 203 (ML-KEM, key encapsulation), FIPS 204 (ML-DSA, digital signatures), and FIPS 205 (SLH-DSA, stateless hash-based signatures). NSM-10 and OMB M-23-02 direct federal agencies and critical infrastructure operators to inventory cryptographic assets and begin migration planning toward these standards by 2030. The foundational technical problem is cryptographic asset discovery, not algorithm selection. Classical cryptographic dependencies are embedded across TLS, SSH, IKE, and S/MIME protocol stacks using RSA, ECC, and Diffie-Hellman for key exchange; third-party libraries and middleware; hardware security modules (HSMs); and proprietary OT firmware with long device lifecycles and infrequent patch cycles. Symmetric encryption (AES) is less immediately threatened by quantum computing but NIST recommends AES-256 for data with long-term sensitivity. Relevant weakness classes are CWE-326 (Inadequate Encryption Strength) and CWE-327 (Use of a Broken or Risky Cryptographic Algorithm). MITRE ATT&CK techniques T1600 (Weaken Encryption), T1600.001 (Reduce Key Space), and

T1040 (Network Sniffing) represent the adversary tradecraft enabled by quantum-vulnerable cryptography left in place. CISA and NIST both recommend cryptographic bill of materials (CBOM) development as the immediate first step. Air-gapped and semi-isolated OT segments compound discovery difficulty because standard network scanning tools cannot operate in those environments, leaving cryptographic dependencies invisible to most enterprise tooling.

Action Checklist

1. Step 1: Inventory Initiation. Launch a cryptographic asset discovery effort scoped to all IT and OT environments. Prioritize internet-facing systems, remote access infrastructure (VPN, SSH gateways), and OT segments that use TLS, IKE, or S/MIME. Document every identified instance of RSA, ECC, and Diffie-Hellman key exchange with key lengths, asset owner, protocol context, and device lifecycle status. This produces the CBOM recommended by CISA and NIST. Mapped control: NIST AC-20 (Use of External Systems) for third-party cryptographic dependencies; CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) for asset tracking.
2. Step 2: Detection. Determine which systems are running quantum-vulnerable algorithms by scanning TLS handshake negotiation logs, SSH key exchange logs, and PKI certificate inventories for RSA and ECC key usage. For OT environments where active scanning is not feasible, review vendor firmware documentation and request cryptographic dependency disclosures from OT vendors. Query certificate management systems for certificates using RSA-2048 or ECC P-256 with expiration dates beyond 2030. Mapped control: NIST AU-6 (Audit Record Review, Analysis, and Reporting); NIST SI-4 (Information System Monitoring) for continuous detection of cryptographic algorithm usage; CIS 8.2 (Collect Audit Logs); D3-SFA (System File Analysis) for firmware and configuration review.
3. Step 3: Eradication. There is no single patch. Remediation requires replacing quantum-vulnerable algorithms with NIST-approved PQC algorithms (ML-KEM per FIPS 203, ML-DSA per FIPS 204, SLH-DSA per FIPS 205) on a system-by-system basis. Prioritize systems handling long-lived sensitive data first, as harvest-now-decrypt-later attacks are already possible. For OT devices that cannot be upgraded, document as accepted risk with compensating controls and flag for device replacement planning. Engage OT vendors on PQC roadmaps for long-lifecycle equipment. Mapped control: NIST SI-4 (Information System Monitoring) for continuous cryptographic algorithm monitoring post-remediation; CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) apply to upgradeable systems.
4. Step 4: Recovery. After replacing cryptographic implementations, validate that updated systems negotiate only approved PQC or hybrid PQC/classical cipher suites. Re-scan TLS and SSH endpoints to confirm removal of RSA and ECC key exchange. Update the CBOM to reflect remediated assets and re-verify certificate inventories. Establish recurring CBOM review cycles to catch new cryptographic dependencies introduced through software updates, vendor changes, or new OT deployments. Mapped control: NIST AU-3 (Content of Audit Records) for validation logging; NIST CA-7 (Continuous Monitoring) for ongoing validation; CIS 7.1 (Establish and Maintain a Vulnerability Management Process).
5. Step 5: Post-Incident. This gap exposes two structural control weaknesses: absence of cryptographic asset visibility and absence of a formal cryptographic lifecycle management process. Implement a CBOM as a standing artifact updated on a defined cadence. Integrate cryptographic algorithm review into procurement requirements for all new OT equipment and software. Establish vendor attestation requirements for PQC readiness on contracts beyond 2027. Mapped controls: NIST AC-1 (Policy and Procedures) for cryptographic policy formalization; CIS 2.1 (Establish and Maintain a Software Inventory)

to capture library-level cryptographic dependencies; D3-CH (Credential Hardening) for algorithm hardening across authentication infrastructure.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal counsel if CBOM discovery reveals quantum-vulnerable encryption protecting data subject to regulatory retention requirements (HIPAA, PCI DSS, ITAR, CUI) where harvest-now-decrypt-later exposure has already occurred, or if OT vendor assessment confirms no PQC upgrade path exists for safety-critical systems with lifecycle dates extending beyond 2030.
Recovery Notes	Post-remediation, re-scan all TLS and SSH endpoints on a monthly cadence using the same tooling used in Steps 1–2 to detect cryptographic regressions introduced by software updates, vendor patches, or new OT deployments that silently re-introduce RSA or ECC key exchange. Maintain the CBOM as a living artifact with a defined update trigger (new software deployment, vendor firmware update, certificate renewal, new OT procurement) rather than a point-in-time snapshot. Continue monitoring NSA/CISA PQC transition guidance and NIST FIPS 203/204/205 implementation errata for algorithm updates that may require cipher suite adjustments before the 2030 deadline.
Forensic Artifacts	TLS handshake negotiation logs from load balancers, reverse proxies (nginx, Apache, F5), and VPN concentrators — specifically the negotiated cipher suite field showing RSA or ECDHE key exchange, which identifies quantum-vulnerable endpoints and establishes the pre-remediation exposure baseline | SSH daemon logs (`/var/log/auth.log`, `journalctl -u sshd`) and `sshd_config` files from SSH gateway hosts — showing configured and negotiated key exchange algorithms (e.g., `diffie-hellman-group14-sha256`, `ecdh-sha2-nistp256`) that are quantum-vulnerable under Shor's algorithm | PKI certificate inventory exports from all certificate management systems — specifically certificates using RSA-2048 or ECC P-256/P-384 key types with expiration dates beyond 2030, which are subject to harvest-now-decrypt-later risk for their full remaining validity period | OT vendor firmware documentation and written cryptographic dependency disclosures — identifying embedded TLS, IKE, or S/MIME implementations in long-lifecycle ICS/SCADA devices that cannot be actively scanned and may have no PQC upgrade path before end-of-life | Software bill of materials (SBOM) and library dependency manifests for applications — specifically identifying OpenSSL, BouncyCastle, NSS, or other cryptographic library versions in use, which are the primary source of undiscovered quantum-vulnerable algorithm dependencies not visible through network scanning alone

Per-Action IR Details

Step 1: Inventory Initiation — Launch a cryptographic asset discovery effort scoped to all IT and OT environments. Prioritize internet-facing systems, remote access infrastructure (VPN, SSH gateways), and OT segments that use TLS, IKE, or S/MIME. Document every identified instance of RSA, ECC, DH, and AES-128 with asset owner, protocol context, and device lifecycle status. This produces the CBOM recommended by CISA and NIST. Mapped control: NIST AC-20 (Use of External Systems) for third-party cryptographic dependencies; CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) for asset tracking.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing the cryptographic asset visibility baseline required before detection or remediation of quantum-vulnerable algorithm exposure is possible

Controls: NIST AC-20 (Use of External Systems) — governs terms and conditions for third-party systems that introduce external cryptographic dependencies (e.g., vendor-managed VPN concentrators, cloud PKI, SaaS endpoints negotiating TLS with RSA/ECC), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — directly mandates the accurate, detailed asset inventory that is the prerequisite for producing a CBOM covering IT and OT devices running quantum-vulnerable algorithms

Compensating: For a 2-person team without enterprise asset management tooling: run `nmap --script ssl-enum-ciphers -p 443,8443,22,500,4500 ` against internet-facing and VPN ranges to enumerate negotiated cipher suites and flag RSA/DH/ECC key exchange. Use `ssh-audit` (free, Python-based) against SSH gateways to enumerate key exchange algorithms. For OT segments where active scanning is prohibited, use Wireshark in passive capture mode on a SPAN port to identify TLS ClientHello/ServerHello handshakes negotiating RSA or ECDHE cipher suites without disrupting device operation. Compile results into a spreadsheet CBOM template aligned to CISA's cryptographic inventory guidance.

Evidence: This step does not alter live system state and does not require volatile evidence capture as a prerequisite. However, document baseline cryptographic negotiation behavior before any remediation begins: capture TLS handshake PCAPs from internet-facing ingress points showing negotiated cipher suite, certificate chain, and key exchange method; export current SSH server host key fingerprints and configured kex algorithms from `/etc/ssh/sshd_config` and `ssh -Q kex`; export PKI certificate inventory exports (Subject, Key Algorithm, Key Size, Expiration, SAN) from all certificate management systems; for OT environments, photograph or export firmware version screens and request vendor cryptographic dependency disclosures in writing to establish a pre-remediation baseline.

Step 2: Detection — Determine which systems are running quantum-vulnerable algorithms by scanning TLS handshake negotiation logs, SSH key exchange logs, and PKI certificate inventories for RSA and ECC key usage. For OT environments where active scanning is not feasible, review vendor firmware documentation and request cryptographic dependency disclosures from OT vendors. Query certificate management systems for certificates using RSA-2048 or ECC P-256 with expiration dates beyond 2030. Mapped control: NIST AU-6 (Audit Record Review, Analysis, and Reporting); CIS 8.2 (Collect Audit Logs); D3-SFA (System File Analysis) for firmware and configuration review.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: analyzing existing log sources and configuration artifacts to identify the scope of quantum-vulnerable cryptographic algorithm usage across IT and OT assets

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — directly governs the review and analysis of TLS negotiation logs, SSH key exchange logs, and PKI audit trails to identify RSA-2048 and ECC P-256 usage, CIS 8.2 (Collect Audit Logs) — mandates that audit logging is enabled across enterprise assets, which is the prerequisite for querying TLS and SSH negotiation records to detect quantum-vulnerable algorithm use

Compensating: Without a SIEM: use `openssl s_client -connect :443 &1 | grep 'Cipher\|Server public key'` against each internet-facing endpoint to confirm negotiated cipher and key size. For SSH, run `ssh -vv 2>&1 | grep 'kex: algorithm'` to enumerate the negotiated key exchange. For certificate inventory without a certificate manager, run `echo | openssl s_client -connect :443 2>/dev/null | openssl x509 -noout -text | grep -E 'Public Key Algorithm|RSA Public-Key|Signature Algorithm|Not After'` across all TLS endpoints. For OT: cross-reference vendor firmware release notes against a manually maintained spreadsheet of devices and request written cryptographic dependency disclosures from ICS/SCADA vendors.

Evidence: This step does not alter live system state. Before logging queries are run, preserve raw log files to prevent rotation from overwriting evidence: archive current TLS access logs (e.g., `/var/log/nginx/access.log`, Apache `ssl_request_log`, F5 SSL handshake logs) that contain negotiated cipher suite fields; export SSH daemon logs (`/var/log/auth.log` or `journalctl -u sshd`) showing key exchange algorithm negotiation events; export full certificate inventory from PKI/CA systems including key algorithm, key size, issuer, and expiration date; for OT, preserve firmware version strings and any available ICS protocol logs (e.g., DNP3, Modbus session logs) that may indicate embedded TLS or IKE usage. These records establish the pre-remediation cryptographic exposure baseline required for post-remediation validation in Step 4.

Step 3: Eradication — There is no single patch. Remediation requires replacing quantum-vulnerable algorithms with NIST-approved PQC algorithms (ML-KEM per FIPS 203, ML-DSA per FIPS 204, SLH-DSA per FIPS 205) on a system-by-system basis. Prioritize systems handling long-lived sensitive data first, as harvest-now-decrypt-later attacks are already possible. For OT devices that cannot be upgraded, document as accepted risk with compensating controls and flag for device replacement planning. Engage OT vendors on PQC roadmaps for long-lifecycle equipment. Mapped control: NIST SI-4 is not listed in the provided control reference — no mapped control for continuous monitoring from this knowledge base. CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) apply to upgradeable systems.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: removing the quantum-vulnerable cryptographic configurations from affected systems and replacing with NIST FIPS 203/204/205-approved PQC algorithms on a prioritized, system-by-system basis

Controls: CIS 7.3 (Perform Automated Operating System Patch Management) — governs OS-level cryptographic library updates (e.g., OpenSSL, Windows CNG) required to deploy ML-KEM and ML-DSA algorithm support on upgradeable servers and endpoints, CIS 7.4 (Perform Automated Application Patch Management) — governs application-level updates for TLS libraries, SSH daemons, VPN clients, and PKI-integrated applications that must be patched to support FIPS 203/204/205 algorithm suites

Compensating: For teams without automated patch management: maintain a prioritized remediation queue in a spreadsheet ordered by (1) data sensitivity, (2) asset internet exposure, and (3) certificate expiration date relative to 2030. For each upgradeable system, test PQC cipher suite availability using `openssl list -public-key-algorithms` after updating to OpenSSL 3.3+ which includes ML-KEM/ML-DSA support. For OT devices that cannot be upgraded, implement network-layer compensating controls: configure host-based firewall rules using `iptables` or Windows Firewall to restrict communication to known internal endpoints, reducing the harvest-now-decrypt-later exposure window by limiting traffic interception opportunities. Document each non-upgradeable OT device as a formal accepted-risk exception with asset owner sign-off.

Evidence: Before replacing any cryptographic configuration on a live system, capture the pre-change state to support rollback and post-remediation validation: export the current TLS cipher suite configuration from each target system (e.g., `openssl s_client` output, nginx/Apache SSL config, Windows `Get-TlsCipherSuite` PowerShell output); capture the current SSH `sshd_config` and `ssh_config` key exchange algorithm lists; export the current certificate binding from each endpoint (`certutil -store` on Windows, `openssl x509 -in -noout -text` on Linux); for OT systems being flagged as accepted risk, document the exact firmware version, vendor PQC roadmap response, and network topology showing data flows that traverse the quantum-vulnerable channel. This pre-change baseline is required to validate eradication success in Step 4.

Step 4: Recovery — After replacing cryptographic implementations, validate that updated systems negotiate only approved PQC or hybrid PQC/classical cipher suites. Re-scan TLS and SSH endpoints to confirm removal of RSA and ECC key exchange. Update the CBOM to reflect remediated assets and re-verify certificate inventories. Establish recurring CBOM review cycles to catch new cryptographic dependencies introduced through software updates, vendor changes, or new OT deployments. Mapped control: NIST AU-3 (Content of Audit Records) for validation logging; CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verifying that quantum-vulnerable algorithm configurations have been successfully replaced and that restored systems negotiate only FIPS 203/204/205-approved or hybrid PQC cipher suites before returning to production

Controls: NIST AU-3 (Content of Audit Records) — governs that post-remediation validation logs capture sufficient detail (negotiated cipher suite, key exchange algorithm, certificate key type, timestamp, system identifier) to confirm successful removal of RSA/ECC and adoption of PQC algorithms, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — governs the recurring CBOM review cycle and re-scan cadence that ensures newly

introduced cryptographic dependencies from software updates or vendor changes are detected and remediated before 2030

Compensating: For a 2-person team: re-run the `nmap --script ssl-enum-ciphers` and `ssh-audit` scans performed in Step 1 against all remediated endpoints and diff the output against the pre-remediation baseline captured in Step 3 to confirm RSA and ECC key exchange are no longer negotiated. Use `openssl s_client -connect :443 &1 | grep 'Cipher\|Server public key'` to confirm PQC or hybrid cipher suite negotiation on each TLS endpoint. Schedule monthly re-scans using a cron job to catch cryptographic regressions introduced by software updates. Maintain a version-controlled CBOM flat file (CSV or JSON) in a Git repository with commit history to track changes over time.

Evidence: Post-remediation validation evidence to retain for audit and compliance purposes: save the post-change `nmap ssl-enum-ciphers` and `ssh-audit` output for each remediated system alongside the pre-change baseline from Step 3, with timestamps and operator identity recorded; export updated certificate inventory showing replacement certificates using ML-DSA or hybrid key types with expiration dates and issuing CA; retain configuration change logs from each system showing the cryptographic configuration diff (old cipher list vs. new cipher list); for OT systems listed as accepted risk, retain the signed accepted-risk exception documentation and vendor PQC roadmap correspondence as evidence of compensating control. These artifacts are the primary evidence set for FIPS 140-3 compliance review and NSM-10/OMB M-23-02 milestone reporting.

Step 5: Post-Incident — This gap exposes two structural control weaknesses: absence of cryptographic asset visibility and absence of a formal cryptographic lifecycle management process. Implement a CBOM as a standing artifact updated on a defined cadence. Integrate cryptographic algorithm review into procurement requirements for all new OT equipment and software. Establish vendor attestation requirements for PQC readiness on contracts beyond 2027. Mapped controls: NIST AC-1 (Policy and Procedures) for cryptographic policy formalization; CIS 2.1 (Establish and Maintain a Software Inventory) to capture library-level cryptographic dependencies; D3-CH (Credential Hardening) for algorithm hardening across authentication infrastructure.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conducting lessons-learned analysis to address the structural control gaps (no cryptographic asset visibility, no cryptographic lifecycle policy) that allowed quantum-vulnerable algorithm proliferation across IT/OT environments to go undetected

Controls: NIST AC-1 (Policy and Procedures) — governs the development and documentation of a formal cryptographic lifecycle management policy that mandates PQC algorithm requirements, CBOM maintenance cadence, and vendor attestation requirements for contracts beyond 2027, CIS 2.1 (Establish and Maintain a Software Inventory) — governs the software inventory process that must be extended to capture library-level cryptographic dependencies (e.g., OpenSSL version, BouncyCastle version, vendor SDK cryptographic modules) that are the primary source of undiscovered quantum-vulnerable algorithm usage

Compensating: For a 2-person team without GRC tooling: draft a one-page Cryptographic Algorithm Policy using NIST FIPS 140-3 and NSM-10 as the normative references, establishing RSA/ECC/DH deprecation timelines and mandating ML-KEM/ML-DSA as approved algorithms for new systems. Add a cryptographic algorithm field to the existing software inventory spreadsheet and require it to be populated for all new software procurement requests. Create a procurement checklist question — 'Does this product support ML-KEM (FIPS 203) or ML-DSA (FIPS 204)?' — and add it to the standard vendor evaluation template. Schedule a semi-annual CBOM review as a recurring calendar item with a designated owner.

Evidence: Post-incident documentation artifacts to retain as the institutional record of this remediation effort: the final CBOM showing all identified quantum-vulnerable assets, their remediation status (mitigated, accepted risk, or pending), and the date of last review; lessons-learned meeting notes documenting the root cause (absence of cryptographic asset visibility) and the two structural gaps identified; the updated procurement checklist and cryptographic algorithm policy with version history; vendor PQC readiness attestation letters or written responses received during Steps 1–4; and the CBOM review schedule and designated ownership assignment. These artifacts are the primary evidence set for demonstrating progress toward NSM-10/OMB M-23-02 2030 compliance milestones and for informing future cryptographic posture assessments.

Detection Guidance

No CVE-specific IOCs exist for this governance item. Detection focus is cryptographic algorithm enumeration across the environment. For TLS: query network traffic logs and load balancer/proxy logs for cipher suite negotiation records showing RSA key exchange (TLS_RSA_*) or ECDHE with P-256/P-384 curves. For SSH: review SSH daemon configuration files and connection logs for key exchange algorithms (diffie-hellman-group*, ecdh-sha2-*). For PKI: export the full certificate inventory from all certificate authorities and certificate management platforms; flag any certificate using RSA or ECC key types with validity beyond 2030. For OT: request cryptographic algorithm documentation from OT vendors for all deployed firmware versions; treat absence of documentation as a gap requiring escalation. For IKE/IPsec: review VPN gateway configurations for Phase 1 and Phase 2 algorithm selections. D3-SFA (System File Analysis) applies to configuration and firmware review in OT segments where active scanning is not viable. Absence of a CBOM is itself a detection gap indicator; if one does not exist, the organization cannot confirm its exposure surface.

Framework Mappings

MITRE-ATTACK

- **T1600.001** — Reduce Key Space
- **T1600** — Weaken Encryption
- **T1040** — Network Sniffing

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures

NIST-800-53R5

- **SC-13** — Cryptographic Protection

ISO-27001-2022

- **A.8.24** — Use of cryptography
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1600.001	Reduce Key Space	Defense-Evasion
T1600	Weaken Encryption	Defense-Evasion
T1040	Network Sniffing	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cybersecurity-operations/meeting-2030-q...	T3
Tosi reports US enterprises improve OT security maturity, but vendor ...	https://industrialcyber.co/reports/tosi-reports-us-enterprises-impr...	T3
IT/OT Convergence: Benefits, Risks, and Protection Tips	https://www.txone.com/blog/the-it-ot-convergence/	T3
Converged IT/OT: The Critical Infrastructure Risk - YouTube	https://www.youtube.com/watch?v=udrZvXpO-uQ	T3
[PDF] Securing IT/OT Convergence for Industry 4.0 Success - Karta Corp	https://kartacorp.com/wp-content/uploads/2023/07/Whitepaper-IDC_Sec...	T3

Generated 2026-06-26 18:40 UTC by TJS Security Command Center