INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 18:26 UTC

OT/ICS Post-Quantum Cryptographic Readiness Gap: Compliance Theater in Critical Infrastructure

GOVERNANCE | HIGH | CVSS 7.5

SCC Item ID	SCC-GOV-2026-0015
Type	Governance
Severity	HIGH
CVSS Base Score	7.5
Affected Products	OT/ICS environments broadly; critical infrastructure operators across energy, water, manufacturing, and transportation sectors
Published	2026-04-13T15:10:55
Discovery Source	Rss

Executive Summary

Critical infrastructure operators across energy, water, manufacturing, and transportation sectors are signing post-quantum cryptography readiness attestations they cannot operationalize; the tooling to assess or implement PQC in OT environments does not yet exist at the required scale or maturity. Nation-state threat actors documented with capability to target OT networks, including those assessed to have conducted reconnaissance on critical infrastructure, are engaging in 'harvest now, decrypt later' campaigns against OT networks, exfiltrating encrypted operational data for future decryption once cryptographically relevant quantum computers become available. The business risk is a compliance posture built on attestations that exceed operational capability, combined with a live data exfiltration threat with a delayed but high-consequence detonation profile.

Technical Analysis

OT/ICS environments rely heavily on legacy cryptographic implementations covered by CWE-327 (use of broken or risky cryptographic algorithms) and CWE-326 (inadequate encryption strength), with PKI-dependent environments further exposed via CWE-295 (improper certificate validation). NIST finalized PQC standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) in August 2024, but OT-specific migration tooling and implementation guidance remain nascent. OT constraints, limited compute on legacy hardware, 10-30 year asset lifecycles, real-time control requirements, and narrow maintenance windows, make direct PQC algorithm substitution impractical without vendor support that does not broadly exist. MITRE ATT&CK for ICS

techniques T1040 (network sniffing) and T1557 (adversary-in-the-middle) map to active collection activity; T1600 and T1600.001 (weaken encryption) map to cryptographic downgrade risk; T0802, T0869, T0885 map to broader OT manipulation and disruption post-decryption exploitation. As of 2026-03-04, CISA has published general quantum readiness guidance for critical infrastructure but has not released OT-specific PQC migration frameworks at the operational level.

Action Checklist

1. Step 1: Containment, Inventory all encrypted OT communications channels (historian connections, engineering workstation-to-controller links, remote access tunnels) and identify which rely on RSA, ECC, or Diffie-Hellman key exchange; these are the highest exfiltration exposure points. Prioritize network segments accessible to external connections or vendor remote access.
2. Step 2: Detection, Deploy network traffic capture on OT DMZ and inter-zone boundaries to detect anomalous bulk traffic collection consistent with T1040 and T1557 activity. Review firewall and historian logs for sustained outbound data transfers to unrecognized endpoints. Focus on baseline deviation in data volumes rather than signature-based detection.
3. Step 3: Eradication, No patch is available; this is a structural cryptographic gap. Immediate mitigation is network segmentation hardening: enforce strict egress filtering on OT network zones, disable unnecessary encrypted tunnels to external systems, and revoke any vendor remote access credentials not actively in use. Apply CISA's ICS security guidance at https://www.cisa.gov/topics/industrial-control-systems as the current authoritative baseline.
4. Step 4: Recovery, Validate that network segmentation changes have not disrupted operational communications by reviewing historian data continuity and HMI connectivity. Monitor for re-establishment of any previously blocked external connections. Document current cryptographic algorithm inventory per asset class as the baseline for future PQC migration gap assessments.
5. Step 5: Post-Incident, This item exposes a systemic control gap: absence of a cryptographic asset inventory for OT environments. Initiate a formal PQC readiness assessment aligned to NIST IR 8413 and track CISA for OT-specific migration framework releases. Review existing regulatory attestations for accuracy against operational capability. Escalate findings to legal and compliance leadership to assess exposure from attestations made ahead of operational implementation.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO, legal counsel, and operational leadership if network monitoring identifies bulk encrypted data transfers from OT historian or engineering workstation segments to unrecognized external IPs (consistent with active Volt Typhoon HNDL staging), if any regulatory body requests documentation of PQC readiness attestations that cannot be substantiated by an operational cryptographic inventory, or if ICS vendor notification confirms that any deployed OT component lacks a PQC migration roadmap within the NIST-defined migration window.

Recovery Notes	Recovery for an HNDL-class governance gap is not a single event — it is a sustained posture improvement. Verify that egress filtering changes have not degraded historian data continuity or HMI-to-controller communications by reviewing tag data completeness and protocol-level connectivity within 24 hours of any segmentation change. Maintain elevated network monitoring at OT DMZ boundaries for a minimum of 90 days given Volt Typhoon's documented multi-month dwell times and their pattern of re-establishing access through alternative paths after initial detection. Treat the cryptographic algorithm inventory produced during recovery as a living document with quarterly review cycles tied to NIST PQC standard updates and ICS vendor roadmap disclosures.
Forensic Artifacts	OT historian server access logs (OSIsoft PI audit logs, Wonderware InTouch audit trail, or GE Historian event log) filtered for bulk tag read operations — HNDL campaigns targeting operational data will generate anomalous read volumes across all process historian tags within a short collection window, distinguishable from normal SCADA polling patterns | Zeek ssl.log and conn.log captures from OT DMZ SPAN port showing TLS handshake cipher suite negotiations — specifically ServerHello records identifying RSA, ECDHE, or DHE key exchange on connections from engineering workstations or historian servers to external IPs, documenting exactly which encrypted sessions were exposed to HNDL collection | Windows Security Event Log Event ID 4688 (Process Creation) on engineering workstations filtering for netsh.exe, wmic.exe, certutil.exe, and msiexec.exe parent-child chains — Volt Typhoon LOTL tradecraft documented in CISA Advisory AA23-144A relies on these built-in tools to avoid EDR detection on OT-adjacent Windows hosts | Firewall session logs from OT-to-enterprise and OT-to-internet boundaries with bytes_out > 10MB and session duration > 10 minutes to non-operational external destinations — sustained large-volume outbound sessions to unrecognized IPs or ASNs are the primary behavioral indicator of HNDL data staging from OT network segments | VPN gateway authentication and session logs for all vendor remote access accounts covering a minimum 90-day lookback period, cross-referenced against scheduled maintenance windows — Volt Typhoon has used compromised vendor remote access credentials to establish persistent access to OT environments, and sessions occurring outside scheduled maintenance windows are primary indicators of credential compromise

Per-Action IR Details

Step 1: Containment — Inventory all encrypted OT communications channels (historian connections, engineering workstation-to-controller links, remote access tunnels) and identify which rely on RSA, ECC, or Diffie-Hellman key exchange; these are the highest HNDL exposure points. Prioritize network segments accessible to external connections or vendor remote access.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; CSF [RS] — Categorize and contain to limit ongoing HNDL exposure surface

Controls: NIST IR-4 (Incident Handling) — execute containment phase of incident handling capability, NIST SI-7 (Software, Firmware, and Information Integrity) — identify communications relying on cryptographic mechanisms susceptible to future quantum decryption, NIST SC-8 (Transmission Confidentiality and Integrity) — enumerate channels where transmission protection is provided by RSA/ECC/DH and therefore vulnerable to HNDL, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — extend asset inventory to include cryptographic algorithm per communication channel, not just device class, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — document current cryptographic configuration of OT network segments as a security baseline

Compensating: Run `nmap --script ssl-enum-ciphers -p 443,102,20000,44818 ` against historian servers, engineering workstations, and remote access gateways to enumerate negotiated cipher suites and key exchange algorithms. For Modbus/DNP3 and proprietary ICS protocols, deploy Wireshark with the ICS protocol dissectors on a TAP or SPAN

port at the OT DMZ boundary and filter for TLS handshakes (`tls.handshake.type == 2`) to extract ServerHello cipher suite fields. Compile results into a spreadsheet mapping asset → protocol → key exchange algorithm → external reachability.

Evidence: Before modifying any network configurations, capture: (1) full pcap of TLS handshakes on historian-to-enterprise and remote access VPN interfaces to document which key exchange algorithms are currently negotiated — this establishes what was harvestable; (2) firewall rule exports (show running-config or equivalent) from OT DMZ firewalls documenting which vendor remote access tunnels were permitted and to which external IPs; (3) VPN gateway authentication logs showing all external connections established in the prior 90 days, particularly any associated with known Volt Typhoon infrastructure or unrecognized ASNs; (4) certificate inventory from engineering workstations and historian servers showing RSA/ECC key sizes in use.

Step 2: Detection — Deploy network traffic capture on OT DMZ and inter-zone boundaries to detect anomalous bulk traffic collection consistent with T1040 and T1557 activity. Review firewall and historian logs for sustained outbound data transfers to unrecognized endpoints. Volt Typhoon TTPs include living-off-the-land techniques that generate minimal signatures — focus on baseline deviation in data volumes rather than signature-based detection.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; CSF [DE.CM-01] — Networks and network services are monitored to find potentially adverse events; CSF [DE.AE-02] — Potentially adverse events are analyzed to better understand associated activities

Controls: NIST SI-4 (System Monitoring) — monitor OT network boundaries specifically for bulk encrypted data exfiltration patterns consistent with HNDL staging activity, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — analyze historian and firewall logs for sustained outbound transfers deviating from operational baselines, NIST AU-12 (Audit Record Generation) — ensure audit records are generated at OT DMZ boundary devices sufficient to reconstruct Volt Typhoon LOTL activity, NIST IR-5 (Incident Monitoring) — track and document anomalous traffic patterns as incident indicators for HNDL campaign attribution, CIS 8.2 (Collect Audit Logs) — ensure logging is enabled at OT DMZ boundary, historian servers, and remote access concentrators specifically to support HNDL detection, MITRE ATT&CK T1040 (Network Sniffing) — Volt Typhoon use of built-in tools to capture network traffic at staging points within OT environments, MITRE ATT&CK T1557 (Adversary-in-the-Middle) — collection of encrypted traffic transiting OT-to-enterprise links for offline decryption

Compensating: Deploy Zeek (formerly Bro) on a SPAN port at the OT DMZ boundary — it is free and produces structured conn.log, ssl.log, and notice.log outputs without requiring a SIEM. Write a Zeek script or use the built-in `conn.log` to flag any single connection transferring more than a configurable threshold (e.g., 50MB) to an external IP not in a pre-approved vendor allowlist. For historian-specific monitoring, query OSIsoft PI (or equivalent) audit logs for unusual read access patterns — bulk tag reads across all historian points in a short window is a behavioral indicator of HNDL data staging. Use the Sigma rule `proc_creation_win_netsh_command` and `net_connection_win_netsh` to detect Volt Typhoon's documented use of `netsh` for port proxying on Windows-based engineering workstations.

Evidence: Preserve before any network changes: (1) Zeek or tcpdump conn.log captures from OT DMZ SPAN ports for the maximum available lookback window — Volt Typhoon dwell times in critical infrastructure have been measured in months to years, so retain all available historical captures; (2) firewall session logs from OT-to-enterprise and OT-to-internet boundaries filtered for connections with duration > 10 minutes and bytes_out > 10MB to unrecognized external IPs; (3) historian server (OSIsoft PI, Wonderware, GE Historian) access logs showing which tags were read, by which account, and data volume retrieved per session; (4) Windows Security Event Log Event ID 4688 (Process Creation) on engineering workstations filtered for `netsh.exe`, `wmic.exe`, `powershell.exe`, and `certutil.exe` — Volt Typhoon LOTL tradecraft documented by CISA; (5) DNS query logs from OT network resolvers for any domain lookups to non-operational external destinations.

Step 3: Eradication — There is no patch available; this is a structural cryptographic gap. Immediate mitigation is network segmentation hardening: enforce strict egress filtering on OT network zones, disable unnecessary encrypted tunnels to external systems, and revoke any vendor remote access credentials not actively in use. Apply CISA's ICS security guidance at https://www.cisa.gov/topics/industrial-control-systems as the current authoritative baseline.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; CSF [RS] — Remove threat from environment; note: classical 'eradication' does not apply to a structural cryptographic gap — this phase addresses reducing the ongoing HNDL attack surface to the greatest extent operationally feasible

Controls: NIST SI-2 (Flaw Remediation) — in the absence of a vendor patch, document compensating controls as the interim remediation posture and establish a remediation tracking record, NIST SC-7 (Boundary Protection) — enforce strict egress filtering at OT network zone boundaries to prevent further encrypted traffic exfiltration to unrecognized external endpoints, NIST IA-5 (Authenticator Management) — revoke vendor remote access credentials not actively in use; rotate credentials for all remote access accounts with OT network access, NIST CM-7 (Least Functionality) — disable encrypted tunnels to external systems that are not operationally required, reducing RSA/ECC/DH key exchange exposure surface, NIST IR-4 (Incident Handling) — document the absence of a vendor patch as a gap in the incident handling record and escalate to risk acceptance or compensating control approval, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce deny-by-default egress rules on OT historian servers and engineering workstations to block unsanctioned outbound encrypted connections, CIS 6.2 (Establish an Access Revoking Process) — execute immediate revocation of inactive vendor remote access credentials as a documented, auditable access management action

Compensating: Use `iptables` (Linux) or Windows Firewall with Advanced Security GPO to implement default-deny egress on OT hosts, explicitly permitting only known operational destinations (control system vendor update servers, site-to-site VPN to approved corporate subnets). For vendor remote access, audit all active VPN accounts using `show vpn-sessiondb` (Cisco ASA) or equivalent and immediately terminate sessions and disable accounts not confirmed active by the responsible operational team. Document each disabled account and tunnel with timestamp, approving personnel, and operational justification in the incident record per NIST IR-5 (Incident Monitoring) requirements.

Evidence: Before executing segmentation changes: (1) export the complete firewall ruleset from all OT DMZ and inter-zone firewalls — this is the pre-remediation baseline and may be required for regulatory review; (2) extract VPN gateway active session and account lists documenting all vendor remote access credentials currently provisioned, including last-used timestamps; (3) capture a final pre-change pcap at each boundary being hardened to document the traffic state at time of containment — this may be required for forensic reconstruction if a regulatory inquiry follows; (4) collect Windows Security Event Log Event ID 4625 (Failed Logon) and 4624 (Successful Logon) from remote access infrastructure for the prior 90 days to identify whether any vendor accounts show access patterns inconsistent with scheduled maintenance windows.

Step 4: Recovery — Validate that network segmentation changes have not disrupted operational communications by reviewing historian data continuity and HMI connectivity. Monitor for re-establishment of any previously blocked external connections. Document current cryptographic algorithm inventory per asset class as the baseline for future PQC migration gap assessments.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; CSF [RC] — Execute recovery plan, restore systems, verify operational integrity, and communicate status to stakeholders

Controls: NIST IR-4 (Incident Handling) — verify operational recovery and confirm containment measures have not introduced new gaps in the OT environment, NIST CP-10 (System Recovery and Reconstitution) — validate that historian data continuity, HMI connectivity, and controller communications are intact following segmentation changes, NIST AU-11 (Audit Record Retention) — establish retention policy for the cryptographic algorithm inventory document as a baseline artifact for future PQC migration audits and regulatory review, NIST SI-4 (System Monitoring) — maintain heightened monitoring at previously blocked egress points for 30+ days post-containment to detect Volt Typhoon re-entry attempts or lateral movement to new exfiltration paths, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — the cryptographic algorithm inventory per asset class created in this step becomes a permanent, maintained component of the enterprise asset inventory, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — register the PQC migration gap as a tracked vulnerability in the vulnerability management process with a remediation timeline tied to NIST PQC standard availability

Compensating: Validate historian data continuity by querying OSIsoft PI or equivalent for a time-series gap report on critical process tags for the period spanning the segmentation change window — any gaps in tag data may indicate a disrupted communication path requiring remediation. For HMI connectivity validation, execute ping and protocol-level

connectivity tests (e.g., `mbtcp_ping` for Modbus TCP, or vendor-specific diagnostic tools) from each HMI to its associated PLCs and RTUs. Set up a cron job or Task Scheduler entry to run `netstat -an | grep ESTABLISHED` every 15 minutes on historian servers and log output to a local file for 30 days — review weekly for any re-established connections to previously blocked external IPs.

Evidence: Collect and retain: (1) the completed cryptographic algorithm inventory document mapping each OT asset class (historian, EWS, RTU, PLC, remote access gateway) to the key exchange algorithms in use — this is the PQC gap baseline and will be required for NIST IR 8413-aligned assessments; (2) historian data continuity report confirming no tag data gaps attributable to segmentation changes; (3) post-change firewall logs for the first 72 hours confirming that previously blocked connections were not re-established via alternative paths; (4) a timestamped record of all vendor remote access credentials revoked, with last-use timestamps, for regulatory and audit purposes.

Step 5: Post-Incident — This item exposes a systemic control gap: absence of a cryptographic asset inventory for OT environments. Initiate a formal PQC readiness assessment aligned to NIST IR 8413 (status of NIST's evaluation of PQC) and track CISA for OT-specific migration framework releases. Review existing regulatory attestations for accuracy; legal and compliance leadership should assess exposure from attestations made ahead of operational capability.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; CSF [GV, ID] — Lessons learned, update policies, improve detection capability, share intelligence with appropriate stakeholders

Controls: NIST IR-4 (Incident Handling) — conduct post-incident review to document the cryptographic inventory gap as a systemic control deficiency and assign ownership for remediation tracking, NIST IR-8 (Incident Response Plan) — update the incident response plan to incorporate a cryptographic algorithm inventory requirement and PQC readiness review as standing pre-incident preparation tasks, NIST RA-3 (Risk Assessment) — formally assess the HNDL risk posed by current RSA/ECC/DH usage in OT environments and document residual risk accepted pending PQC migration tooling maturity, NIST SI-2 (Flaw Remediation) — register PQC migration for each affected OT asset class as an open flaw remediation item with target dates aligned to NIST PQC standard finalization and vendor adoption timelines, NIST CA-7 (Continuous Monitoring) — incorporate monitoring for HNDL-indicative bulk exfiltration patterns as a permanent addition to the continuous monitoring strategy for OT environments, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — document the absence of a cryptographic asset inventory as a process gap and establish a formal remediation milestone within the vulnerability management program, CIS 7.2 (Establish and Maintain a Remediation Process) — assign the PQC migration gap a risk-tiered remediation priority and schedule quarterly review against NIST, CISA, and ICS vendor PQC roadmap updates

Compensating: For the PQC readiness assessment without a dedicated GRC platform, create a structured spreadsheet based on NIST IR 8413 algorithm categories (ML-KEM, ML-DSA, SLH-DSA) cross-referenced against each OT asset class and its current key exchange algorithm — this becomes the migration gap register. Assign a specific analyst to monitor the CISA ICS security advisories RSS feed and the NIST PQC project page for OT-relevant migration guidance releases. For the regulatory attestation review, map each submitted attestation against the cryptographic inventory baseline created in Step 4, flagging any attestation where the claimed capability cannot be substantiated by the inventory — this mapping is the disclosure risk analysis input for legal and compliance leadership.

Evidence: Preserve and archive: (1) all regulatory attestations related to cryptographic readiness or PQC compliance submitted prior to this assessment, with submission dates and the specific claims made — these are the documents requiring accuracy review by legal and compliance; (2) the lessons-learned record from this incident review documenting the cryptographic inventory gap, its discovery date, and the remediation plan accepted by risk leadership; (3) any threat intelligence reports or CISA advisories referencing Volt Typhoon or XENOTIME HNDL activity that were available prior to the attestations being submitted — this establishes the threat landscape context at the time of attestation for regulatory and legal purposes; (4) the PQC gap register created during this step, version-controlled from initial creation, as the baseline artifact for all future PQC migration progress tracking.

Detection Guidance

No CVE-specific IOCs exist for this governance gap, but data exfiltration activity has observable signatures. Monitor OT network egress for sustained encrypted data transfers, particularly from historian servers, engineering workstations, and SCADA head-end systems. Threat actors conducting harvest campaigns have been documented using native tools and living-off-the-land approaches to minimize footprint; prioritize anomaly-based detection over signature matching. Look for T1040 indicators: unexpected packet capture tool execution on OT-adjacent Windows hosts; T1557 indicators: unexpected ARP table changes or certificate errors on OT network segments; T1600 indicators: negotiation of weaker cipher suites on monitored encrypted channels. For PKI-dependent environments, alert on certificate validation failures (CWE-295 exposure surface) that may indicate interception attempts.

Framework Mappings

MITRE-ATTACK

- **T0802** — Automated Collection
- **T0869** — Standard Application Layer Protocol
- **T0885** — Commonly Used Port
- **T1040** — Network Sniffing
- **T1600** — Weaken Encryption
- **T1557** — Adversary-in-the-Middle
- **T1600.001** — Reduce Key Space

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

NIST-800-53R5

- **SC-13** — Cryptographic Protection
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates

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

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0802	Automated Collection	Collection
T0869	Standard Application Layer Protocol	Command-And-Control
T0885	Commonly Used Port	Command-And-Control
T1040	Network Sniffing	Credential-Access
T1600	Weaken Encryption	Defense-Evasion
T1557	Adversary-in-the-Middle	Credential-Access
T1600.001	Reduce Key Space	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/ics-ot-security/ot-lacks-tools-cryptogr...	T3
Tosi reports US enterprises improve OT security maturity, but vendor ...	https://industrialcyber.co/reports/tosi-reports-us-enterprises-impr...	T3
Industrial Control Systems | Cybersecurity and Infrastructure ... - CISA	https://www.cisa.gov/topics/industrial-control-systems	T1
5 “Unique” Security Challenges Facing OT/ICS Environments - Cyolo	https://cyolo.io/blog/5-unique-security-challenges-facing-ot-ics-en...	T3
56 Vulnerabilities Discovered in OT Products From 10 Different ...	https://www.darkreading.com/vulnerabilities-threats/study-finds-56-...	T3

Generated 2026-04-13 18:26 UTC by TJS Security Command Center