



QTONIC QUANTUM
POST QUANTUM READY

QUANTUM CYBERSECURITY FOR THE U.S. MILITARY

Mission assurance in a post-quantum world

100-PAGE EXECUTIVE FIELD GUIDE

TECHNET AUGUSTA 2026

QSCOUT PULSE - 24/7/365 | QSTRIKE | QSOLVE

QHUNT - LAUNCHING AT TECHNET AUGUSTA 2026

Photo: Josef Cole / U.S. Cyber Command / DVIDS | Public domain

INDEPENDENT VENDOR FIELD GUIDE

The appearance of U.S. Department of War visual information does not imply or constitute DoW endorsement. No AFCEA or TechNet Augusta endorsement is implied.

EVIDENCE BEFORE ASSERTION

Document control and credibility boundary

A serious defense publication distinguishes external requirements, current vendor facts, engagement-specific capability, analytical judgment, and target-state design.

01

EXTERNAL REQUIREMENT

Official U.S. Government publications control policy, dates, profiles, and acquisition obligations.

02

QTONIC QUANTUM CURRENT STATE

Vendor-authored product boundaries are labeled and separated from independent requirements.

03

ENGAGEMENT-SPECIFIC

Access, methods, deployment, testing, and deliverables depend on signed scope and authorization.

04

PROPOSED TARGET STATE

Recommended controls and architectures are not represented as already deployed.

05

NO ENDORSEMENT

Military, agency, conference, and depicted-person references provide context only; no official endorsement is implied.

06

OPERATIONS SECURITY FIRST

Operations security (OPSEC) means classified data, live secrets, operational plans, and unnecessary controlled content stay outside a commercial workflow.

THE STANDARD

We would rather state a limitation than manufacture certainty. Every material claim should be traceable to a current source, an observed artifact, or an explicitly labeled judgment.

PLAIN-ENGLISH RULE

Spell out a term on first use. Keep the acronym only when it recurs. Define mission meaning, not just the letters.



LETTER FROM THE CO-FOUNDER

“The decisive question is not when quantum arrives. It is which mission failures become unacceptable before migration is complete.”

A NOTE TO THE WARFIGHTER AND THE ACQUISITION ENTERPRISE

Mission assurance before the quantum deadline

Quantum cybersecurity is often presented as a physics story. For the U.S. military, it is a mission-assurance, architecture, acquisition, and sustainment problem. Public-key cryptography is embedded in identity, command and control, data links, software signing, coalition access, cloud services, tactical radios, space systems, weapons, logistics, operational technology, and the Defense Industrial Base. Replacement must occur across complete trust paths - not only inside a data center or a single application.

The Department's 2026 strategy makes the direction unmistakable: inventory cryptography, prioritize mission consequences, build and integrate quantum-resistant capabilities, and move toward hard 2030 and 2031 outcomes. Program offices need evidence that connects cryptographic objects to data lifetimes, mission owners, suppliers, dependencies, and attack paths. They also need a governed way to validate risk without turning production systems into test ranges.

Qtonic Quantum makes the decision record inspectable. QScout finds and prioritizes evidence. QScout Pulse operates continuously, 24/7/365, across the approved external surface and configured evidence sources. QStrike validates selected forward-threat paths. QSolve sequences migration with owners and acceptance criteria. QHunt launches at TechNet Augusta 2026 as a quantum-aware red-team intelligence capability for warfighters. Judge us on evidence, scope discipline, and measurable outcomes - not slogans.

J. Nathaniel Ader

Co-Founder and Chief Innovation Officer | Qtonic Quantum Corp

THE ENTIRE REPORT IN ONE PAGE

Executive command brief

Quantum risk is already an information-lifetime, trust-path, acquisition, and modernization risk - even before a cryptographically relevant quantum computer exists.

EXTERNAL REQUIREMENTS

2030 - DOW OUTCOME

Support post-quantum cryptography or phase out affected systems by December 31, 2030.

2031 - DOW OUTCOME

Use post-quantum cryptography by December 31, 2031, unless otherwise noted.

QTONIC QUANTUM OPERATING CONSTRUCTS

20 MISSION DOMAINS

A coverage model for scoping the military cryptographic estate. It is not a government mandate or universal priority ranking.

30-DAY MISSION DECISION

A Qtonic Quantum engagement construct that converts one mission thread into an evidence-backed decision path. It is not a statutory deadline.

THREAT

Shor threatens widely used RSA and elliptic-curve systems. Harvest-now-decrypt-later exposure can become present loss.

SCOPE

Confidentiality, identity, signatures, software trust, devices, suppliers, archives, and mission-partner interfaces.

CONSTRAINT

Latency, jamming, bandwidth, power, disconnected operations, long hardware life, classification, and coalition interoperability.

METHOD

Inventory by mission. Model complete trust paths. Prioritize by data lifetime and consequence. Validate bounded environments. Verify closure.

FAILURE MODE

One post-quantum endpoint is not readiness. A vulnerable root, signer, gateway, supplier, or fallback can preserve the attack path.

ENGAGEMENT

QScout finds. QScout Pulse sustains. QStrike and QHunt prove. Qsolve governs the fix. The output is a decision record, not a demo.

COMMANDER / CHIEF INFORMATION OFFICER / PROGRAM EXECUTIVE OFFICER CHECKLIST

Ten decisions leaders must make now

A quantum program becomes executable only when authority, scope, priorities, funding, and acceptance evidence are explicit.

01

Name the accountable executive

One authority owns inventory, migration sequence, funding, risk acceptance, and reporting.

02

Define the mission boundary

Name systems, data classes, operating environments, suppliers, coalition interfaces, and end-to-end trust paths.

03

Set the inventory schema

Capture algorithm, use, key size, certificate chain, protocol, library, hardware anchor, owner, data lifetime, and provenance.

04

Prioritize long-lived data

Rank secrecy and integrity lifetime, collection opportunity, adversary interest, replacement lead time, and mission effect.

05

Freeze new quantum debt

Make cryptographic agility and approved transition support acquisition gates for hardware, software, services, firmware, and renewals.

06

Choose validation rules

Define safe-stop conditions, permitted methods, test environment, recovery, evidence handling, and release authority.

07

Fund complete trust paths

Budget public key infrastructure (PKI), applications, protocols, devices, roots of trust, signing, suppliers, testing, and sustainment - not just libraries.

08

Separate national security systems and non-NSS

Map each system to its controlling authority and profile. Do not apply civilian milestones to a National Security System (NSS).

09

Measure migration acceptance

Require functional, security, performance, interoperability, recovery, rollback, and mission-thread evidence.

10

Maintain the decision record

Reconcile after releases, architecture changes, certificate events, vendor updates, incidents, waivers, and policy changes.

TECHNET AUGUSTA 2026

Read this report like an operator.

Start with the decision you own. Jump to the policy, mission domain, evidence, validation, or migration page that closes it.

7-MINUTE PATH

Pages 4, 5, 23, 60, 90, 97, 98

15-MINUTE PEO

Pages 23, 29, 38, 51, 76, 88, 91-95

15-MINUTE CISO

Pages 2, 18-20, 40, 47, 61-74, 96

C2 / counter-C2 in support of Army and Joint warfighting

Report at a glance

Navigate 100 pages in seconds. Acronyms and mission terms: pages 19-20.

01

Quantum fundamentals

PAGES 9-21

What changes, what does not, and why timing matters.

02

Policy and standards

PAGES 22-38

Department of War, NSA, NIST, OMB, acquisition gates, and authority lanes.

03

Military mission exposure

PAGES 39-60

Twenty mission domains, trust paths, data, systems, and suppliers.

04

Discovery and intelligence

PAGES 61-74

QScout, evidence fusion, CBOM, HNDL priority, and Pulse.

05

Validation and red teaming

PAGES 75-86

Safe-stop proof, QStrike, QHunt, falsification, and evidence.

06

Migration and execution

PAGES 87-96

Architecture patterns, ACDI, procurement controls, and QSolve.

07

People and action

PAGES 97-100

Leadership, 30-day mission decision, evidence register, and contact.

Quick terms: PQC = post-quantum cryptography | CRQC = cryptographically relevant quantum computer | HNDL = harvest now, decrypt later | ACDI = automated cryptography discovery and inventory | CBOM = cryptographic bill of materials.

ONE MISSION. FOUR GOVERNED ACTIONS.

From exposure to accepted change

Qtonic Quantum connects cryptographic evidence to the decision, the proof, the owner, and the migration sequence.

FIND | QSCOUT

Approved-scope cryptographic exposure intelligence, HNDL priority, CBOM output where approved, and a governed catalog across Surface, Silver, and Gold. Applicable registered modules execute by scope; others are explicitly dispositioned.

PROVE | QSTRIKE

Selected forward-threat validation with explicit modeled-runtime boundaries, safe-stop conditions, falsification, and a reviewable evidence package.

FIX | QSOLVE

Vendor-neutral migration governance connecting findings to owners, dependencies, transition patterns, waves, acceptance, and sustainment.

HUNT | QHUNT

Launching at TechNet Augusta 2026 as Qtonic Quantum's quantum-aware cyber risk and vulnerability red-team intelligence capability for warfighters. Non-destructive by default; invasive methods require explicit authority.

Mission leadership. Enterprise accountability.

Private-sector leadership and advisory roles supporting mission standards, enterprise execution, allied readiness, and national cyber policy.



Weatherington



Renner



Jung



Cloutier



Beagle



Mussington

Approved portraits identify current private-sector leaders and advisers.

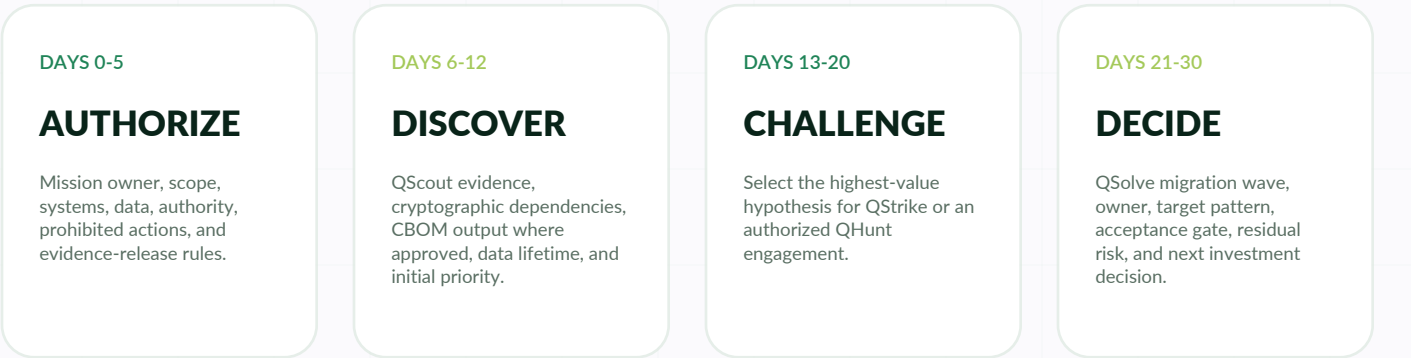
Official attire, flags, ranks, and insignia do not imply current public office or government/service endorsement.

The evidence tells you what comes next - not the vendor.

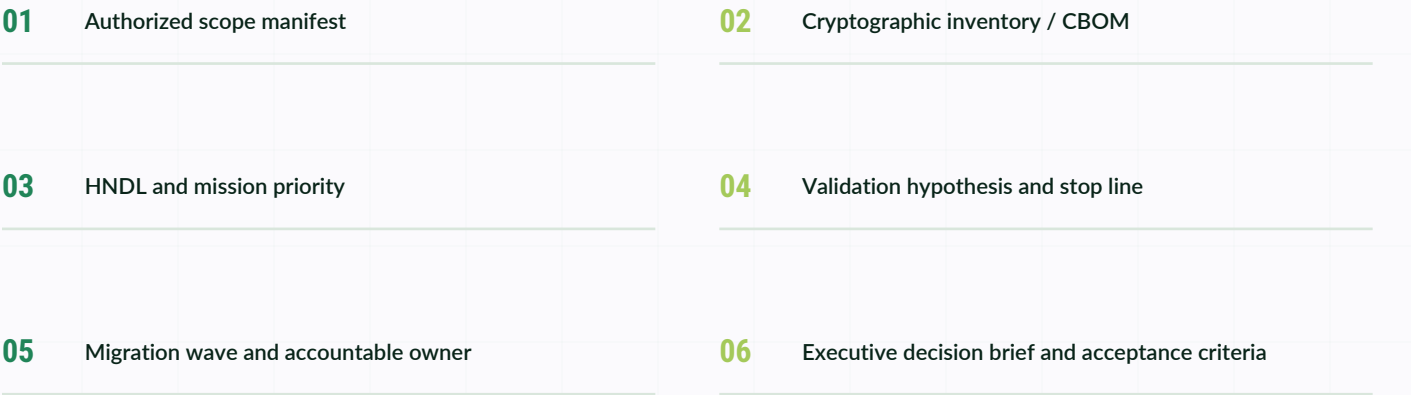
A BOUNDED START WITH A DECISION AT THE END

What a 30-day mission engagement delivers

Bring one consequential mission thread, one long-lived data exposure, one contested trust assumption, and one supplier constraint.



The evidence package



Bring one mission thread. Leave with a decision you can defend.

qtonicquantum.com/contact | info@qtonicquantum.com | +1 (866) 4-QTONIC



Quantum fundamentals without the hype

Physics, algorithms, HNDL, uncertainty, and the minimum technical fluency required for defensible decisions.

IN THIS PART

- What a quantum computer is - operationally
- Harvest-now-decrypt-later timing
- Shor, Grover, and cryptographic effect
- Risk scoring without false certainty

KEY TERMS

PQC - post-quantum cryptography | CRQC - cryptographically relevant quantum computer | HNDL - harvest now, decrypt later | KEM - key-encapsulation mechanism | PKI - public key infrastructure



FROM PHYSICS TO MISSION EFFECT

What a quantum computer is - operationally

A quantum computer is not a universally faster computer. Its relevance comes from specific algorithms that change the cost of selected mathematical problems.

MISSION TAKEAWAY

The military planning question is not whether quantum computers replace classical computing. It is whether a future adversary can apply a specialized quantum algorithm to a trust mechanism your mission still depends on.

Qubits encode amplitudes.

A qubit can be prepared in a state described by amplitudes over 0 and 1. Multiple qubits form a state space whose size grows exponentially. That mathematical space is useful only when an algorithm can shape interference toward a measurable answer.

Gates implement controlled evolution.

Quantum gates transform amplitudes. A circuit is a sequence of gates designed so useful outcomes reinforce while unwanted outcomes cancel. Measurement returns classical information, so the circuit must extract structure efficiently.

Noise is the engineering barrier.

Physical qubits are fragile. Errors from control imperfections, decoherence, crosstalk, leakage, and measurement accumulate. A cryptographically relevant system is expected to require large-scale fault tolerance and error correction.

Advantage is workload-specific.

Quantum speedup depends on the problem, algorithm, data access, circuit depth, error correction, and implementation. Many logistics, AI, and cybersecurity tasks do not automatically become exponentially faster.

THE FIVE-LAYER REALITY

From physical qubits to a cryptographic effect

A headline qubit count is not a mission-relevant measure by itself.

DECISION RULE

A cryptographic threat requires a full stack: sufficiently capable physical devices, error-corrected logical qubits, a workable algorithm and circuit, reliable execution, and a usable operational target.

MISSION EFFECT

Attack path and decision

ALGORITHM

Shor / Grover / workload

FAULT TOLERANCE

Scale and depth

LOGICAL QUBITS

Error-corrected operations

PHYSICAL QUBITS

Noise, control, coherence

HEADLINE QUBIT COUNTS ARE NOT MISSION-RELEVANT BY THEMSELVES

PUBLIC-KEY CRYPTOGRAPHY

Shor's algorithm: what changes

Shor changes the security assumption behind integer factorization and discrete logarithms on a sufficiently capable fault-tolerant quantum computer.

COMMANDER'S TAKEAWAY

Rivest-Shamir-Adleman (RSA), finite-field Diffie-Hellman (DH), elliptic-curve Diffie-Hellman (ECDH), the Elliptic Curve Digital Signature Algorithm (ECDSA), and related public-key mechanisms require transition. Inventory confidentiality, key establishment, signatures, identity, and software trust separately.

01

CONFIDENTIALITY AND KEY ESTABLISHMENT

RSA key transport, finite-field DH, ECDH, Transport Layer Security (TLS) and Internet Protocol Security (IPsec) handshakes, virtual private networks (VPNs), secure messaging, device enrollment, and proprietary key-agreement protocols require transition analysis.

02

AUTHENTICITY AND DIGITAL SIGNATURES

RSA, ECDSA, and Edwards-curve Digital Signature Algorithm (EdDSA) signatures support identity, certificates, code signing, firmware, secure boot, software updates, documents, messages, tokens, logs, and configuration integrity.

03

MISSION EFFECT - CONFIDENTIALITY

Recovered session or long-term keys can expose captured data, facilitate impersonation, or undermine protected channels. Historical-session safety also depends on forward secrecy and key handling.

04

MISSION EFFECT - AUTHENTICITY

Forged signatures can enable malicious software, unauthorized devices, false commands, counterfeit credentials, tampered data, or persistence below the operating system.

05

PLANNING IMPLICATION - SIGNING

Confidentiality-only migration is incomplete. Signing roots, validation software, timestamping, archival verification, secure boot, and recovery workflows require separate transition plans.

06

PLANNING IMPLICATION - KEY ESTABLISHMENT

Identify every asymmetric exchange, the data it protects, the confidentiality horizon, and whether every endpoint and intermediary can support the approved profile.

SYMMETRIC CRYPTOGRAPHY AND HASHING

Grover's algorithm: what changes - and what does not

Grover's algorithm provides a generic quadratic search speedup in an idealized model; it does not collapse symmetric cryptography the way Shor's algorithm threatens public-key systems.

DECISION RULE

Use adequate symmetric key and hash strengths, but do not let the Grover discussion distract from the larger migration burden: vulnerable public-key establishment and signatures embedded across the enterprise and mission edge.

PRIMITIVE	CLASSICAL MARGIN	IDEALIZED GROVER	OPERATIONAL DECISION
AES-128	128	64	Idealized comparison only; not a deployment estimate.
AES-256	256	128	Strong default when required by the controlling profile.
SHA-256 preimage	256	128	Construction, output length, and mission context still matter.

Public-key migration is intentionally excluded from this table because Shor-driven RSA and ECC transition is not a Grover-margin comparison. It is the larger enterprise migration burden.

CRYPTOGRAPHIC TRIAGE

What breaks, what changes, what remains

A disciplined inventory separates public-key risk, symmetric-strength questions, implementation defects, and non-cryptographic cyber risk.

DECISION RULE

Post-quantum cryptography (PQC) is necessary but not sufficient. It does not fix stolen credentials, weak authorization, exposed management planes, poor key custody, vulnerable software, supply-chain compromise, or operational misconfiguration.

01

RSA AND FINITE-FIELD DH

Shor threatens integer factorization and discrete logarithms. Replace affected mechanisms according to the approved profile and trace impact across public key infrastructure (PKI), VPN, TLS, key transport, and embedded protocols.

02

ELLIPTIC-CURVE CRYPTOGRAPHY

Shor threatens elliptic-curve discrete logarithms, affecting ECDH, ECDSA, EdDSA, certificate ecosystems, secure messaging, constrained devices, and modern TLS.

03

SYMMETRIC ENCRYPTION

Grover provides an idealized generic-search speedup, not a practical break estimate. Apply the strength required by the controlling profile; CNSA 2.0 specifies AES-256 for applicable NSS use.

04

HASH FUNCTIONS

Quantum preimage and collision effects differ. Inventory signatures, commitments, integrity checks, and long-term validation, then apply the approved hash and output strength.

05

IMPLEMENTATION DEFECTS REMAIN

PQC does not cure stolen credentials, weak authorization, exposed management planes, poor randomness, unsafe error handling, or vulnerable software.

06

KEY MANAGEMENT REMAINS DECISIVE

Migration must include generation, custody, rotation, revocation, backup, recovery, hardware security module / key-management system integration, and operational procedures.

FIPS 203 AND NIST SP 800-227

Key-encapsulation mechanisms are not drop-in public-key encryption

The Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) establishes a shared secret that is then used with symmetric cryptography. Its application programming interface (API), validation, and failure handling need explicit design.

COMMANDER'S TAKEAWAY

Treat key-encapsulation mechanism (KEM) adoption as a protocol and software-engineering change, not a search-and-replace of RSA calls. Encapsulation, decapsulation, key derivation, error handling, authentication, and transcript binding are security-relevant.

01

KEY GENERATION

The recipient creates an ML-KEM public key and secret key using an approved implementation and protected randomness.

02

ENCAPSULATE

The sender uses the public key to produce a ciphertext and shared secret.

03

DECAPSULATE

The recipient uses the secret key and ciphertext to derive the corresponding shared secret.

04

DERIVE AND PROTECT

A key-derivation function (KDF) and symmetric authenticated encryption protect the actual data or session.

05

AUTHENTICATION IS SEPARATE

A KEM establishes key material; the protocol must bind endpoint identity, role, transcript, and downgrade resistance.

06

FAILURE BEHAVIOR MATTERS

Malformed ciphertext, decapsulation failures, timing, error channels, randomness, key reuse, memory handling, and provider interfaces can create vulnerabilities.

FEDERAL INFORMATION PROCESSING STANDARDS 204 AND 205

Digital signatures are the control plane of trust

Signatures authorize software, devices, identities, commands, updates, and data provenance - not merely documents.

COMMANDER'S TAKEAWAY

A migration that protects network confidentiality but leaves classical code-signing, firmware, secure-boot, or certificate roots in place can preserve the most consequential attack path.

01

ML-DSA

The Module-Lattice-Based Digital Signature Algorithm (ML-DSA) is NIST's lattice-based post-quantum signature standard.

02

SLH-DSA

The Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) is NIST's hash-based signature standard derived from SPHINCS+.

03

ML-DSA PLANNING STRENGTH

A primary general-purpose PQC signature foundation with standardized parameter sets for many certificate, identity, software, data, and message-signing contexts.

04

SLH-DSA PLANNING STRENGTH

Security rests on hash-function assumptions rather than lattices, providing algorithmic diversity for selected roots of trust or long-lived signatures. It is not approved for NSS use under current CNSA 2.0 guidance.

05

ENGINEERING: SIZE AND PERFORMANCE

Test constrained links, certificates, firmware, boot chains, high-volume signing, verification latency, memory, and hardware support.

06

ENGINEERING: IMPLEMENTATION ASSURANCE

Evaluate randomness, side-channel resistance, key custody, certificate formats, hardware security module support, validation status, interoperability, and lifecycle operations.

THE TRUST FABRIC

Why certificates, public key infrastructure, and machine identities dominate migration

The visible algorithm is only one layer of a certificate lifecycle and identity ecosystem.

COMMANDER'S TAKEAWAY

Inventory roots, intermediates, leaf certificates, enrollment, issuance, validation, revocation, hardware security modules, trust stores, device and service identities, automation, and recovery.

01

ROOT - TRUST ANCHORS

Offline roots, cross-certificates, trust lists, policy object identifiers (OIDs), key ceremonies, hardware security modules (HSMs), backup and recovery, algorithm and parameter rules, compromise response, and long validity periods.

02

ISSUANCE - CERTIFICATE AUTHORITIES

Intermediate certificate authorities (CAs), registration authorities, enrollment protocols, identity proofing, templates, issuance policy, revocation, Online Certificate Status Protocol (OCSP), certificate revocation lists (CRLs), audit, and service availability.

03

IDENTITY - PEOPLE AND MACHINES

Users, administrators, workloads, application programming interfaces, containers, devices, radios, sensors, gateways, services, robots, code signers, and non-person entities at tactical and enterprise scale.

04

CONSUMPTION - APPLICATIONS AND PROTOCOLS

Transport Layer Security, Internet Protocol Security, Secure Shell, secure email, signing pipelines, secure boot, tokens, authentication, message security, databases, cloud control planes, and proprietary mission protocols.

05

OPERATIONS - LIFECYCLE AUTOMATION

Discovery, renewal, rotation, inventory reconciliation, policy enforcement, outage prevention, telemetry, exception handling, supplier coordination, and evidence that the deployed path matches the approved design.

TIMING, CONSEQUENCE, AND UNCERTAINTY

HNDL is a timing equation - and a scenario, not a date

Harvest now, decrypt later (HNDL) becomes material when protected data or trust remains valuable long enough for collection today and decryption or forgery after a plausible cryptographically relevant quantum computer (CRQC) scenario.

DECISION RULE

Use early, central, and late capability scenarios. Recalculate when data lifetime, collection opportunity, mission consequence, supplier lead time, or migration evidence changes. Never present one forecast as certainty.

MATERIAL WINDOW

Data or trust value persists into or beyond the plausible CRQC window.



LOWER-URGENCY WINDOW

Data loses material value before the plausible collection-and-decrypt window; keep it inventoried, but do not displace higher-consequence threads.



SIX FACTORS THAT SET PRIORITY

1

DATA / TRUST LIFE

2

COLLECTION OPPORTUNITY

3

ADVERSARY VALUE

4

MIGRATION LEAD TIME

5

MISSION CONSEQUENCE

6

EVIDENCE CONFIDENCE

ACRONYMS AND MISSION TERMS

Acronyms and mission terms: A-M

Plain-English expansions, mission meaning, and the pages where the term matters. Product names are not treated as acronyms.

ACDI	Automated cryptography discovery and inventory. Tool-assisted discovery of cryptographic use across approved systems and evidence sources. See 92.	CNSS	Committee on National Security Systems. Governance body for cybersecurity policy and baseline requirements for NSS. See 27.	HSM	Hardware security module. Protected hardware for generating, storing, and using cryptographic keys. See 17, 68.
AES	Advanced Encryption Standard. Symmetric encryption; CNSA 2.0 specifies AES-256 for applicable NSS use. See 13, 29.	CRQC	Cryptographically relevant quantum computer. A quantum system capable of defeating currently deployed public-key mechanisms at relevant scale. See 18.	HVA	High-value asset. Federal information system or data whose compromise could materially affect national or agency interests.
AFCEA	Armed Forces Communications and Electronics Association. Organizer of TechNet Augusta; reference does not imply endorsement.	CUI	Controlled Unclassified Information. Information requiring safeguarding or dissemination controls under federal policy. See 51.	IPsec	Internet Protocol Security. A suite protecting IP communications; its key establishment and authentication require migration review.
AI / ML	Artificial intelligence / machine learning. Models, data, services, agents, and deployment pipelines with cryptographic dependencies. See 55.	DIB	Defense Industrial Base. Companies, suppliers, and partners supporting military systems, missions, and sustainment. See 51.	ISR	Intelligence, surveillance, and reconnaissance. Mission data and systems whose provenance and long-term value drive risk. See 54.
API	Application programming interface. A software interface through which services, tools, and systems exchange requests and data.	DoW	Department of War. Departmental authority used throughout the 2026 PQC Strategy and this field guide.	KDF	Key-derivation function. Converts shared secrets or key material into cryptographic keys for defined uses. See 15.
ASN	Autonomous system number. An identifier used to map Internet routing ownership during authorized external discovery. See 66.	DVIDS	Defense Visual Information Distribution Service. Source of public-domain military editorial imagery used with attribution.	KEM	Key-encapsulation mechanism. Establishes a shared secret; ML-KEM is the NIST standardized post-quantum KEM. See 15, 30.
CA	Certificate authority. An entity that issues and signs digital certificates within a public key infrastructure. See 17.	ECC	Elliptic-curve cryptography. Public-key mechanisms based on elliptic-curve discrete logarithms; quantum-vulnerable under Shor. See 12, 14.	KMI	Key-management infrastructure. Systems and services governing cryptographic keys, especially in high-assurance environments. See 93.
CBOM	Cryptographic bill of materials. A structured inventory of cryptographic objects, uses, dependencies, and provenance. See 65, 94.	ECDH	Elliptic-curve Diffie-Hellman. Key-establishment method requiring migration analysis. See 12, 14.	KMS	Key-management system or service. Software or cloud capability for key generation, custody, policy, rotation, and use. See 68.
C2	Command and control. The people, systems, processes, and communications used to direct forces and missions. See 41.	ECDSA	Elliptic Curve Digital Signature Algorithm. Classical signature method requiring migration analysis. See 12, 14.	LMS	Leighton-Micali Signature. Stateful hash-based signature approved for CNSA 2.0 software and firmware signing. See 29.
CI/CD	Continuous integration / continuous delivery. Software build, test, signing, and deployment pipelines. See 47-48.	EO	Executive order. A presidential directive governing executive-branch action; EO 14412 accelerates federal PQC migration. See 34.	LOE	Line of effort. A structured workstream in the DoW PQC Strategy. See 24.
CISA	Cybersecurity and Infrastructure Security Agency. Federal source for civilian and critical-infrastructure migration guidance.	FCEB	Federal Civilian Executive Branch. Civilian federal agencies governed through the non-NSS federal policy lane. See 27, 34.	MPE	Mission Partner Environment. Shared coalition or partner environment for exchanging mission information. See 58.
CISO	Chief information security officer. Executive accountable for enterprise cybersecurity risk and operating controls.	FIPS	Federal Information Processing Standards. NIST standards used for federal cryptographic requirements and validation. See 30-31.	ML-DSA	Module-Lattice-Based Digital Signature Algorithm. NIST FIPS 204 post-quantum signature standard. See 16, 31.
CLM	Certificate lifecycle management. Issuance, renewal, rotation, revocation, inventory, and policy for certificates. See 17, 95.	FPGA	Field-programmable gate array. Reconfigurable hardware that may embed cryptographic implementations and trust anchors.	ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism. NIST FIPS 203 post-quantum key-establishment standard. See 15, 30.
CMDB	Configuration management database. A system of record for assets and configuration relationships; one discovery evidence source.	GNSS	Global Navigation Satellite System. Positioning and timing services whose identity, integrity, and trust paths require protection.		
CNSA 2.0	Commercial National Security Algorithm Suite 2.0. NSA algorithm suite and transition profile for National Security Systems. See 28-29.	HNDL	Harvest now, decrypt later. Capture protected data now for possible future decryption. See 18.		

Use the full term on first use. Use the acronym only after the reader has been taught the concept.

ACRONYMS AND MISSION TERMS

Acronyms and mission terms: N-Z

Plain-English expansions, mission meaning, and the pages where the term matters. Product names are not treated as acronyms.

MFA	Multi-factor authentication. Identity verification requiring two or more independent factors.	OT	Operational technology. Systems that monitor or control physical processes, facilities, or industrial equipment. See 46.	SATCOM	Satellite communications. Space, ground, terminal, identity, telemetry, and control trust paths. See 44.
NIAP	National Information Assurance Partnership. Evaluates commercial products against approved protection profiles for NSS use.	PEO	Program Executive Officer. Senior acquisition leader accountable for portfolios, resources, and program execution.	SBOM	Software bill of materials. Inventory of software components and dependencies; related to, but distinct from, a CBOM.
NIST	National Institute of Standards and Technology. Publisher of FIPS, special publications, and migration guidance. See 30-33.	PIV / CAC	Personal Identity Verification / Common Access Card. Federal and defense identity credentials and access ecosystems. See 52.	SHA	Secure Hash Algorithm. Family of hash functions used for integrity, signatures, and key derivation; profile requirements vary. See 13, 29.
NSA	National Security Agency. National Manager for NSS and source of CNSA 2.0 guidance. See 27-29.	PKI	Public key infrastructure. Certificates, authorities, trust anchors, policies, systems, and operations supporting digital trust. See 17, 40.	SLH-DSA	Stateless Hash-Based Digital Signature Algorithm. NIST FIPS 205 standard; not approved for NSS use under current CNSA 2.0 guidance. See 16, 29, 31.
NSM-10	National Security Memorandum 10. Establishes national quantum leadership and migration risk-reduction goals, including 2035.	PLM / CAD	Product lifecycle management / computer-aided design. Engineering systems and technical data central to weapons and sustainment.	S/MIME	Secure / Multipurpose Internet Mail Extensions. Certificate-based protection for email confidentiality and signatures.
NSPM-12	National Security Presidential Memorandum 12. Re-establishes NSS cybersecurity governance, CNSS, and the NSA National Manager role. See 27.	PQC	Post-quantum cryptography. Cryptographic algorithms designed to resist known attacks from classical and quantum computers. See 13, 23, 29-31.	SOC	Security operations center. Team and capability for monitoring and responding to security events; QScout is not a SOC.
NSS	National Security System. A system meeting statutory national-security criteria and governed through the NSS authority lane. See 25, 27.	PSK	Pre-shared key. Secret distributed in advance; not a general substitute for approved asymmetric PQC migration. See 93.	SSH	Secure Shell. Protocol for protected remote access and administration; cryptographic dependencies require inventory.
OCSP	Online Certificate Status Protocol. A method for checking whether a digital certificate has been revoked. See 17.	QKD	Quantum key distribution. A quantum communications approach the DoW strategy says components will not test, pilot, use, or procure for quantum resistance. See 93.	TLS	Transport Layer Security. Protocol protecting network sessions; key establishment, certificates, and negotiation require migration.
OID	Object identifier. A standardized identifier used in certificate policies, algorithms, attributes, and protocols.	RACI	Responsible, accountable, consulted, and informed. A governance model; each decision should have one accountable owner. See 38.	VPN	Virtual private network. Protected network tunnel whose algorithms, profiles, endpoints, and gateways require transition analysis.
OMB	Office of Management and Budget. Leads civilian federal migration execution and oversight. See 34.	RFI	Request for information. A procurement mechanism for gathering supplier capability, evidence, and roadmap data. See 95.	XMSS	eXtended Merkle Signature Scheme. Stateful hash-based signature approved for CNSA 2.0 software and firmware signing. See 29.
OPSEC	Operations security. Protection of sensitive indicators, plans, capabilities, and activities from adversary exploitation.	RMF	Risk Management Framework. Federal process for categorizing, selecting, implementing, assessing, authorizing, and monitoring controls.	Zero Trust	Security model that continuously evaluates identity, device, policy, and context rather than relying on network location. See 36.
OS	Operating system. Platform software whose cryptography, update path, trust store, and signing chain require migration planning.	RSA	Rivest-Shamir-Adleman. Widely deployed public-key algorithm vulnerable to a sufficiently capable quantum computer. See 12, 14.		

Use the full term on first use. Use the acronym only after the reader has been taught the concept.

MYTH / REALITY

Ten quantum cybersecurity myths that create bad programs

The balanced position is neither panic nor dismissal: standards exist, deadlines are real, the estate is broad, and disciplined work can begin without claiming a current CRQC breaks deployed RSA-2048.

01

MYTH: Wait for a CRQC.

REALITY: Long-lived data can be collected now, while approvals, suppliers, hardware, and fielding take years.

02

MYTH: PQC requires a quantum computer.

REALITY: PQC runs on classical systems. Approved standards can be implemented and tested now.

03

MYTH: Replace RSA and finish.

REALITY: ECC, signatures, certificates, firmware, roots of trust, protocols, and fallback also matter.

04

MYTH: Stronger encryption fixes identity.

REALITY: A strong channel can still authenticate the wrong user, device, workload, or signer.

05

MYTH: Inventory is a one-time spreadsheet.

REALITY: Cryptography changes with releases, renewals, cloud services, suppliers, and exceptions.

06

MYTH: One PQC component means ready.

REALITY: Readiness requires the complete trust path, lifecycle, interoperability, recovery, and acceptance.

07

MYTH: A gateway makes endpoints PQC.

REALITY: A boundary can be temporary; it can also concentrate trust and leave endpoints unchanged.

08

MYTH: Lab speed predicts the tactical edge.

REALITY: Bandwidth, latency, power, disconnect, hardware, and certification decide mission fit.

09

MYTH: Software signing can wait.

REALITY: Firmware roots and update trust can be harder to change than transport encryption.

10

MYTH: The compliance date is the start date.

REALITY: The deadline is an end state. Discovery, acquisition, integration, and testing must begin earlier.

Program test: If a claim cannot name the authority, asset, trust path, evidence, consequence, owner, and next action, it is not yet decision-grade.

The U.S. military policy and standards stack

DoW strategy, NSA profiles, NIST standards, acquisition, governance, and the deadlines that shape architecture.

IN THIS PART

- DoW 2030 and 2031 outcomes
- NIST FIPS 203, 204, and 205
- CNSA 2.0 profile and milestones
- Governance, acquisition, and acceptance

KEY TERMS

DoW - Department of War | NSS - National Security System | CNSA 2.0 - Commercial National Security Algorithm Suite 2.0 | CNSS - Committee on National Security Systems | ACIDI - automated cryptography discovery and inventory

THE CLOCK IS AN ARCHITECTURE CONSTRAINT

The DoW 2030 and 2031 outcomes

The strategy was signed April 1, cleared for open publication April 16, and publicly released June 23, 2026. Those are three different dates and one hard execution problem.

2030

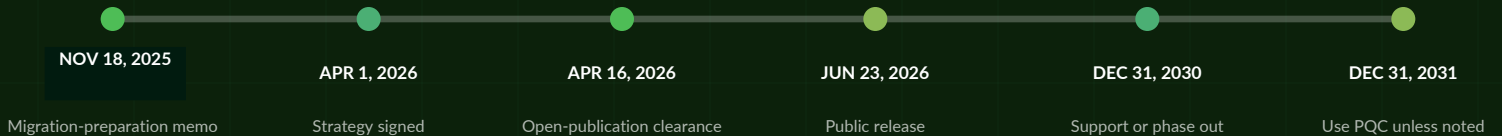
SUPPORT PQC OR PHASE OUT

No later than December 31, 2030.

2031

USE PQC

No later than December 31, 2031, unless otherwise noted.



OPERATIONAL CONSEQUENCE

Discovery, procurement, supplier commitments, architecture, testing, certification, fielding, exception governance, and sustainment must move in parallel. The end state is already inside normal defense acquisition and platform life cycles.

Precision note: April 16 is the clearance stamp, not the strategy signature date.

STRATEGY TO EXECUTION

The five DoW lines of effort

The Department's framework treats PQC as a coordinated enterprise modernization spanning governance, knowledge, development, commercial integration, and deployment.

DECISION RULE

No component can succeed with a tooling-only project. Governance, inventory, engineering, commercial product integration, high-assurance devices, DIB transition, certification, authorization, funding, and fielding must move together.

01

LOE 1 — Governance.

Align authorities, responsibilities, policy, priorities, funding, reporting, risk acceptance, certification, authorization, and enterprise coordination across Components and mission partners.

02

LOE 2 — Inventory and plan.

Identify cryptography across all system types and environments, connect it to mission relevance and quantum-attack risk, establish roadmaps, and maintain the decision record.

03

LOE 3 — Develop and analyze.

Design and evaluate high-assurance end cryptographic units, embedded modules, algorithms, architectures, implementation security, performance, resilience, and certification approaches.

04

LOE 4 — Integrate commercial solutions.

Use agile, interoperable commercial technologies where appropriate across PKI, signing, browsers, cloud, operating systems, networking, hardware, software, and the tactical edge.

05

LOE 5 — Deploy resistant devices.

Field resistant devices and capabilities across key management, data links, transport, space, telephony, radios, edge systems, unmanned platforms, sensors, and weapons-support ecosystems.

ALL CRYPTOGRAPHY | ALL SYSTEM TYPES

The inventory mandate is broader than enterprise information technology

The DoW memo and strategy extend inventory across mission, business, cloud, mobile, physical, unmanned, operational technology, and weapons environments.

COMMANDER'S TAKEAWAY

An inventory that omits disconnected systems, embedded cryptography, signing infrastructure, cloud services, physical access, supplier-managed services, or mission-partner interfaces cannot support migration decisions.

01

NATIONAL SECURITY SYSTEMS

Classified and other National Security System (NSS) environments; high-assurance cryptography; NSA profiles; key-management infrastructure; mission and intelligence systems.

02

NON-NSS AND BUSINESS SYSTEMS

Enterprise information technology (IT), financial, logistics, personnel, collaboration, email, identity, applications, databases, and long-lived administrative records.

03

WEAPONS AND EMBEDDED SYSTEMS

Platform electronics, secure boot, firmware, maintenance interfaces, datalinks, mission computers, embedded libraries, and long refresh cycles.

04

CLOUD AND SOFTWARE FACTORIES

Control planes, application programming interfaces, KMS/HSM, secrets, certificates, service meshes, containers, continuous integration / continuous delivery, artifact signing, repositories, build systems, and software-as-a-service dependencies.

05

OPERATIONAL TECHNOLOGY

Industrial controls, facilities, energy, logistics automation, weapons-support infrastructure, serial and proprietary protocols, safety constraints, and vendor-maintained devices.

06

MOBILE, IoT, UNMANNED, AND PHYSICAL

Endpoints, Internet of Things devices, sensors, access-control systems, badges, cameras, robotics, autonomy, remote management, gateways, telemetry, and edge identity.

THE COMPLETE DATA AND TRUST PATH

When is a migration actually complete?

The DoW strategy rejects a narrow endpoint view. Vulnerable algorithms and protocols must be deprecated across the data path, lifecycle, and supply chain.

DECISION RULE

A confidentiality-only cutover is incomplete if classical authentication, signatures, code signing, firmware, certificates, management channels, supplier interfaces, or recovery paths can still establish trust or reintroduce vulnerable cryptography.

01

CREATE AND SIGN

Data, code, firmware, credentials, and commands originate under an authenticated identity and approved signing process.

02

TRANSPORT

Endpoints, gateways, relays, tunnels, satellite communications (SATCOM), radios, application programming interfaces, and mission partners negotiate and preserve protection.

03

STORE AND USE

Databases, devices, logs, archives, backups, analytics, and applications preserve confidentiality, integrity, and authenticity.

04

RECOVER AND RETIRE

Keys, certificates, media, rollback images, disaster recovery, verification, and decommissioning preserve the final state.

05

TECHNICAL ACCEPTANCE

Confirm approved algorithms, profiles, interoperability, performance, failure handling, key lifecycle, rollback, logging, and repeatable test results.

06

OPERATIONAL ACCEPTANCE

Prove the mission thread under nominal and degraded conditions, including latency, jamming, bandwidth, disconnected operations, failover, coalition use, recovery, and maintenance.

NATIONAL SECURITY SYSTEMS GOVERNANCE AFTER NSPM-12

One federal enterprise - two authority lanes

MISSION TAKEAWAY

Classify the authority lane before applying a migration date, profile, reporting obligation, or exception process. Civilian federal requirements and NSS requirements are related but not interchangeable.

01 CNSS GOVERNANCE

CNSS is re-established to coordinate and issue directives and complementary standards for NSS. Its chair is a member of the National Security Council staff.

02 NATIONAL MANAGER

The Director of NSA serves as National Manager for NSS, including cryptologic authority, technical advice, emergency directives, evaluation, and government-wide posture assessment.

03 BINDING NSS DIRECTION

Agencies that own or operate NSS shall comply with CNSS directives and complementary standards. NIST baselines apply as a minimum unless CNSS provides otherwise.

04 NSS / CNSA LANE

National Security Systems follow CNSS policy, CNSA 2.0 profiles, National Manager guidance, high-assurance requirements, and mission-specific authorization.

05 NON-NSS FEDERAL LANE

Federal Civilian Executive Branch systems follow OMB, NIST, CISA, FIPS, and agency authorization requirements; EO 14412 excludes NSS from its HVA/high-impact transition directive.

06 EXCEPTION DISCIPLINE

NSPM-12 rescinds NSM-8 and directs harmonization of related directives. Do not rely on superseded NSM-8 agency-disregard language; identify current CNSS, agency, and authorizing authority for any exception.

NSS ALGORITHM PROFILE

CNSA 2.0 at a glance

CNSA 2.0 is a selected suite and transition framework for National Security Systems - not a generic label for every PQC implementation.

MISSION TAKEAWAY

For NSS, use the exact algorithm, parameter, protocol, implementation, evaluation, and transition requirements established by NSA and the applicable capability package or protection profile.

KEY ESTABLISHMENT.

Applicable NSA guidance selects ML-KEM-1024 under FIPS 203 for relevant NSS uses. Protocol, implementation, evaluation, and transition requirements still apply.

DIGITAL SIGNATURES.

Applicable NSA guidance selects ML-DSA-87 under FIPS 204 for relevant post-quantum authentication and signature functions.

SYMMETRIC ENCRYPTION.

AES-256 protects data after key establishment. Modes, key custody, lifecycle, implementation assurance, and mission integration remain critical.

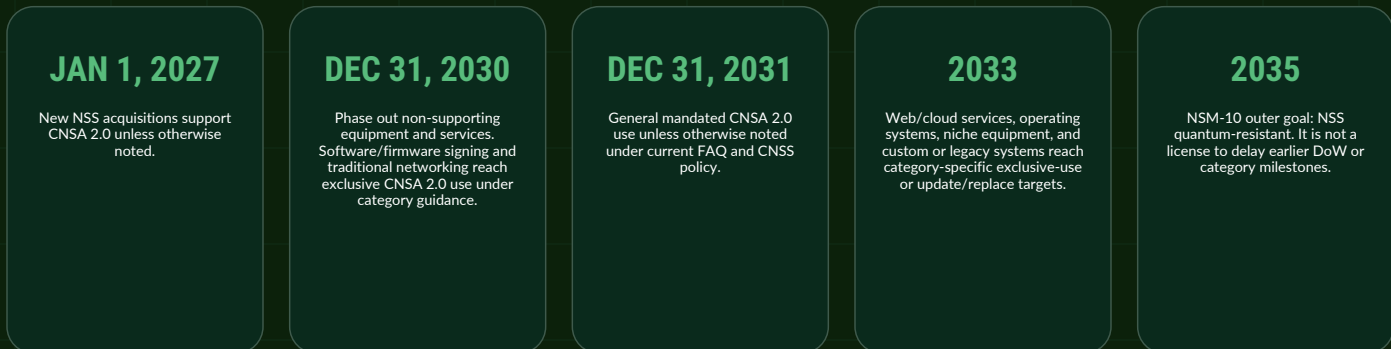
HASH AND SUPPORTING FUNCTIONS.

Use the hash functions, output strengths, randomness, key-derivation, and protocol requirements specified by the applicable NSA profile or capability package.

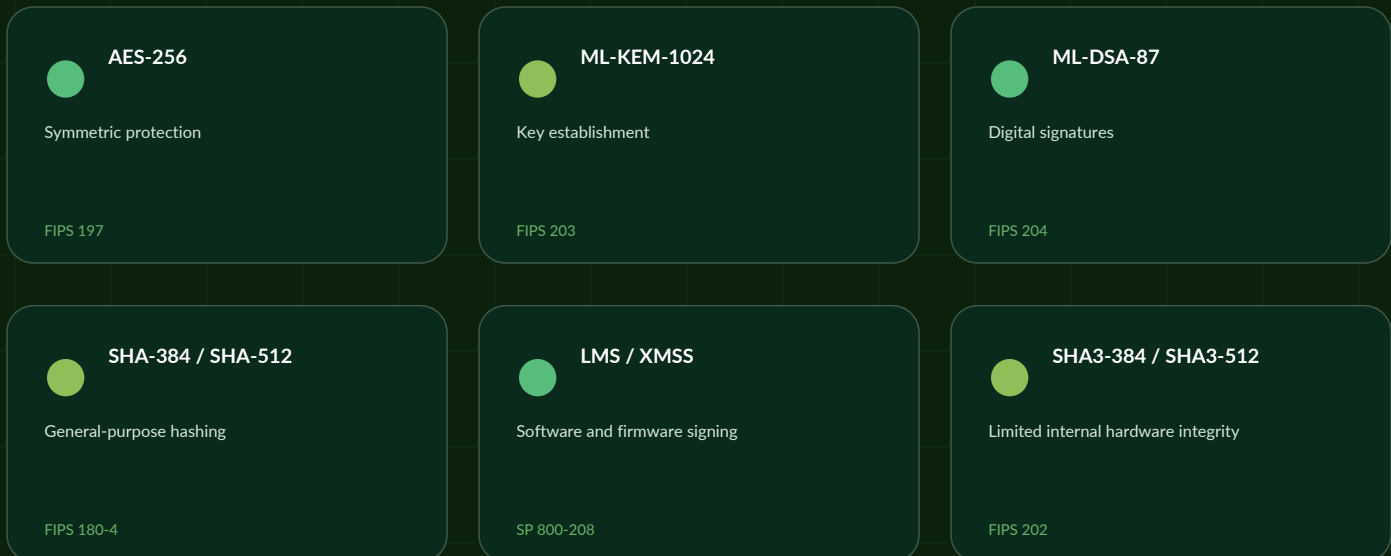
NSS TRANSITION CONTROL PLANE

CNSA 2.0: three timing layers, one NSS transition

The general acquisition and use gates, category-specific exclusive-use dates, and the 2035 national outer goal must be read together. The Department of War 2031 requirement remains the harder operational date for DoW systems.



CNSA 2.0 FOUNDATION



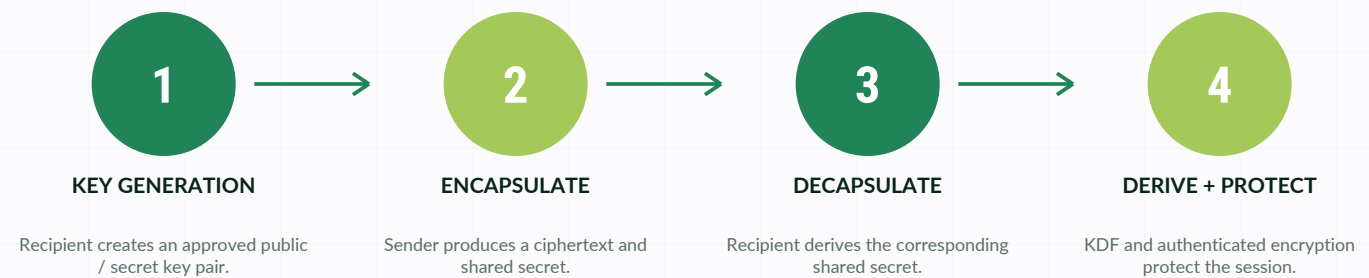
CRITICAL DISTINCTION

CNSA 2.0 does not approve SLH-DSA for NSS use. Category-specific 2033 dates do not defer the DoW requirement to use PQC by December 31, 2031, unless otherwise noted.

POST-QUANTUM KEY ESTABLISHMENT

NIST FIPS 203: ML-KEM

ML-KEM establishes a shared secret. It is a foundation for secure channels - not a complete channel by itself.

**PROFILE**

The controlling profile selects parameter set and assurance requirements.

COMPOSITION

Authentication, transcript binding, KDF use, downgrade resistance, and error handling remain security-critical.

IMPLEMENTATION

Randomness, side channels, validation, provider interfaces, memory handling, and failure behavior require testing.

Treat KEM adoption as protocol engineering - not a search-and-replace of RSA calls.

POST-QUANTUM AUTHENTICITY

NIST FIPS 204 and 205: two signature standards

ML-DSA and SLH-DSA provide distinct post-quantum signature foundations. Selection follows the approved profile, assurance, performance, and lifecycle.

ML-DSA

FIPS 204

Lattice-based signatures

Primary standardized signature for many approved use cases.

SLH-DSA

FIPS 205

Hash-based signatures

Signature diversity with different key, signature-size, and performance trade-offs.

Inventory signature use before choosing a replacement

- Root and intermediate CAs
- Leaf certificates and identity
- Code and firmware signing
- Secure boot and device trust
- Messages, tokens, and logs
- Data provenance and archives
- Emergency recovery and rollback
- Long-term validation and timestamping

Confidentiality-only migration is incomplete if classical signing still controls trust.

NIST INTERNAL REPORT 8547

NIST's transition logic

National Institute of Standards and Technology (NIST) Internal Report 8547 describes a staged deprecation and disallowance path for quantum-vulnerable public-key mechanisms; the cited source remains an initial public draft.

COMMANDER'S TAKEAWAY

Stop creating long-lived dependencies on quantum-vulnerable public-key cryptography, introduce approved post-quantum cryptography support, and plan for eventual disallowance with evidence-based exception handling.

01**2024 DRAFT DIRECTION**

The draft transition direction identifies deprecation targets for selected quantum-vulnerable mechanisms.

02**ONGOING EVOLUTION**

Profiles, standards, validation programs, protocols, products, and implementation guidance continue to evolve.

03**FIPS 203, 204, AND 205**

These Federal Information Processing Standards establish the first principal NIST post-quantum cryptography standards.

04**DISALLOWANCE TARGETS**

Draft direction identifies eventual disallowance targets for selected quantum-vulnerable public-key uses.

05**ORGANIZATION ACTION**

Inventory quantum-vulnerable cryptography, prioritize systems and data, test implementations, and build cryptographic agility.

06**DRAFT STATUS MATTERS**

IR 8547 remains an initial public draft in the cited source. Treat dates and details as planning direction subject to revision; final FIPS standards remain authoritative.

NIST CSWP 39-UPD1

Crypto agility is an operational capability

Agility means the ability to replace and adapt cryptography without losing security or ongoing operations.

DECISION RULE

A mission system is crypto-agile only when policy, architecture, interfaces, implementations, testing, inventory, suppliers, operations, recovery, and authority can execute a controlled change - not merely when an algorithm identifier is configurable.

01 GOVERN — Policy and decision rights.

Approved algorithms and profiles, exception authority, change thresholds, ownership, funding, risk acceptance, evidence standards, and deadlines.

02 DESIGN — Abstraction and modularity.

Versioned interfaces, algorithm negotiation, key and signature agility, provider isolation, protocol extension, configuration control, and reduced hard-coding.

03 OBSERVE — Inventory and telemetry.

Authoritative records of deployed algorithms, keys, certificates, libraries, protocols, devices, owners, dependencies, data lifetime, and configuration drift.

04 CHANGE — Deployment and rollback.

Automated rollout, compatibility windows, hybrid transition, staged cutover, safe failure, rollback, recovery, key rotation, certificate replacement, and supplier coordination.

05 PROVE — Validation and sustainment.

Interoperability, performance, security testing, degraded-mode exercises, evidence packages, authorization impact, continuous reassessment, and retirement of vulnerable paths.

ACCELERATED FEDERAL MIGRATION - JUNE 2026

Executive Order 14412 and OMB M-26-15

The June actions turn post-quantum migration into a dated agency, contractor, CBOM, and vulnerability-disclosure program.

WHY THIS MATTERS TO THE DEFENSE INDUSTRIAL BASE

The order creates procurement and evidence requirements before the migration deadlines. Covered contractors face a proposed FAR path to December 31, 2030 compliance.



90 DAYS | SEP 20, 2026

OMB guidance: review high-value and high-impact systems excluding NSS; plan PQC key establishment by 2030 and digital signatures by 2031.



180 DAYS | DEC 19, 2026

Proposed FAR rule for covered contractors to comply by December 31, 2030 with applicable FIPS incorporating PQC; CMVP acceleration and a NIST pilot also begin.



270 DAYS | MAR 19, 2027

Public CBOM minimum-elements guidance must enable automated cryptographic-asset assessment; proposed VDP rules must cover cryptographic vulnerabilities.



NUMBERING + AUTHORITY

Federal Register: EO 14412, 91 FR 38483, FR Doc 2026-12909. Some DoW materials and coverage use 14409. Civilian EO/OMB actions do not replace NSS or DoW authorities.

PREPARE BEFORE YOU PROCURE

CISA's quantum-readiness roadmap

CISA, NSA, and NIST guidance emphasizes roadmaps, inventory, risk assessment, vendor engagement, and supply-chain preparation.

MISSION TAKEAWAY

The first deliverable is not a purchase order. It is a quantum-readiness roadmap that names leadership, scope, data and system priorities, inventory methods, supplier questions, target profiles, test plans, and funded migration waves.

Establish ownership.

Designate an executive sponsor, technical lead, security lead, acquisition lead, component representatives, and risk authority. Define how decisions reach mission and program owners.

Build the inventory.

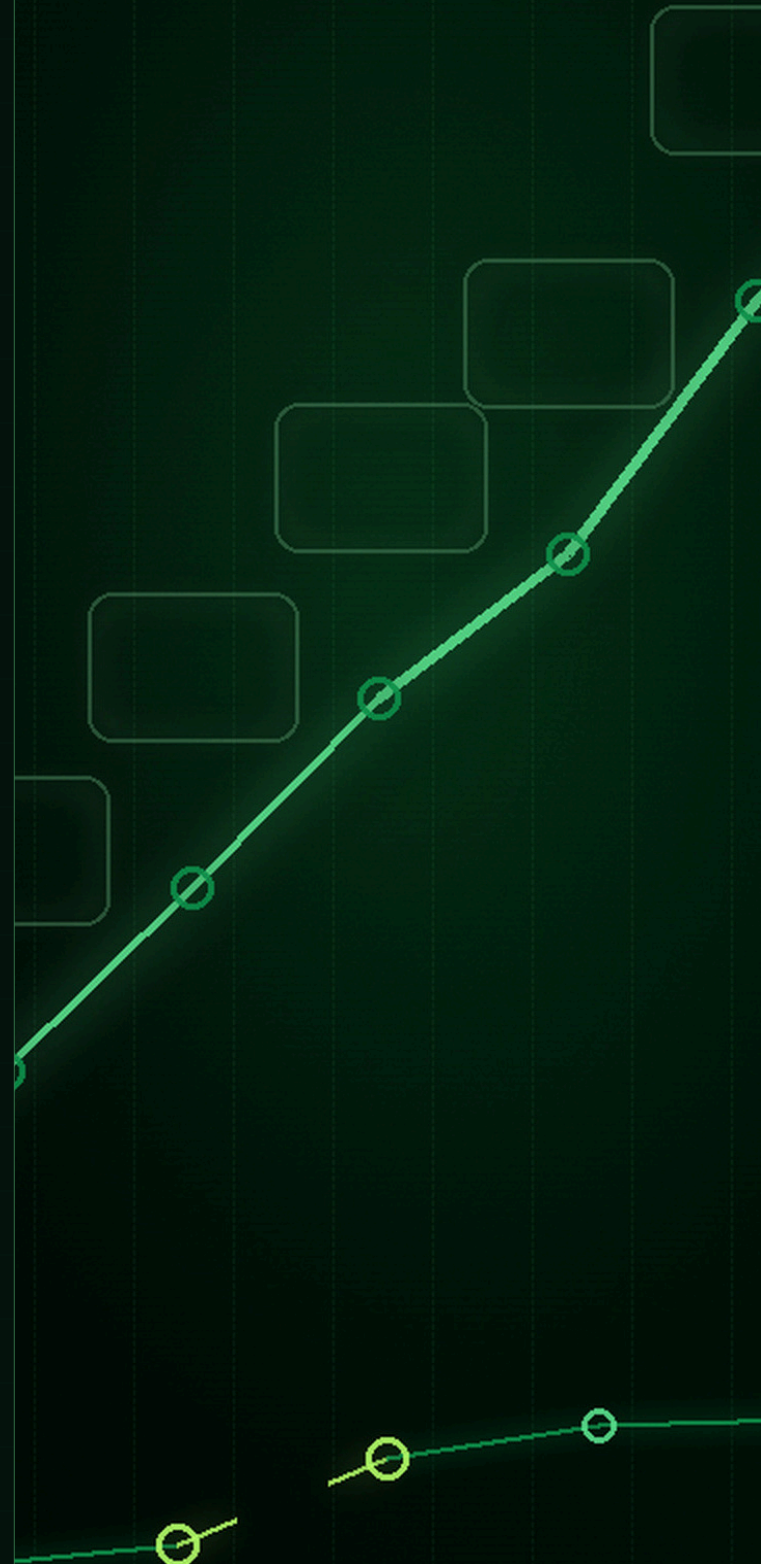
Identify where and how public-key cryptography protects data and systems across hardware, software, firmware, services, protocols, certificates, libraries, and suppliers.

Assess priorities.

Use data lifetime, system criticality, exposure, adversary value, trust function, replacement lead time, dependency depth, and mission consequence.

Engage vendors.

Ask for cryptographic inventories, approved standards support, validation status, algorithm agility, product timelines, performance data, interoperability, update paths, and lifecycle commitments.



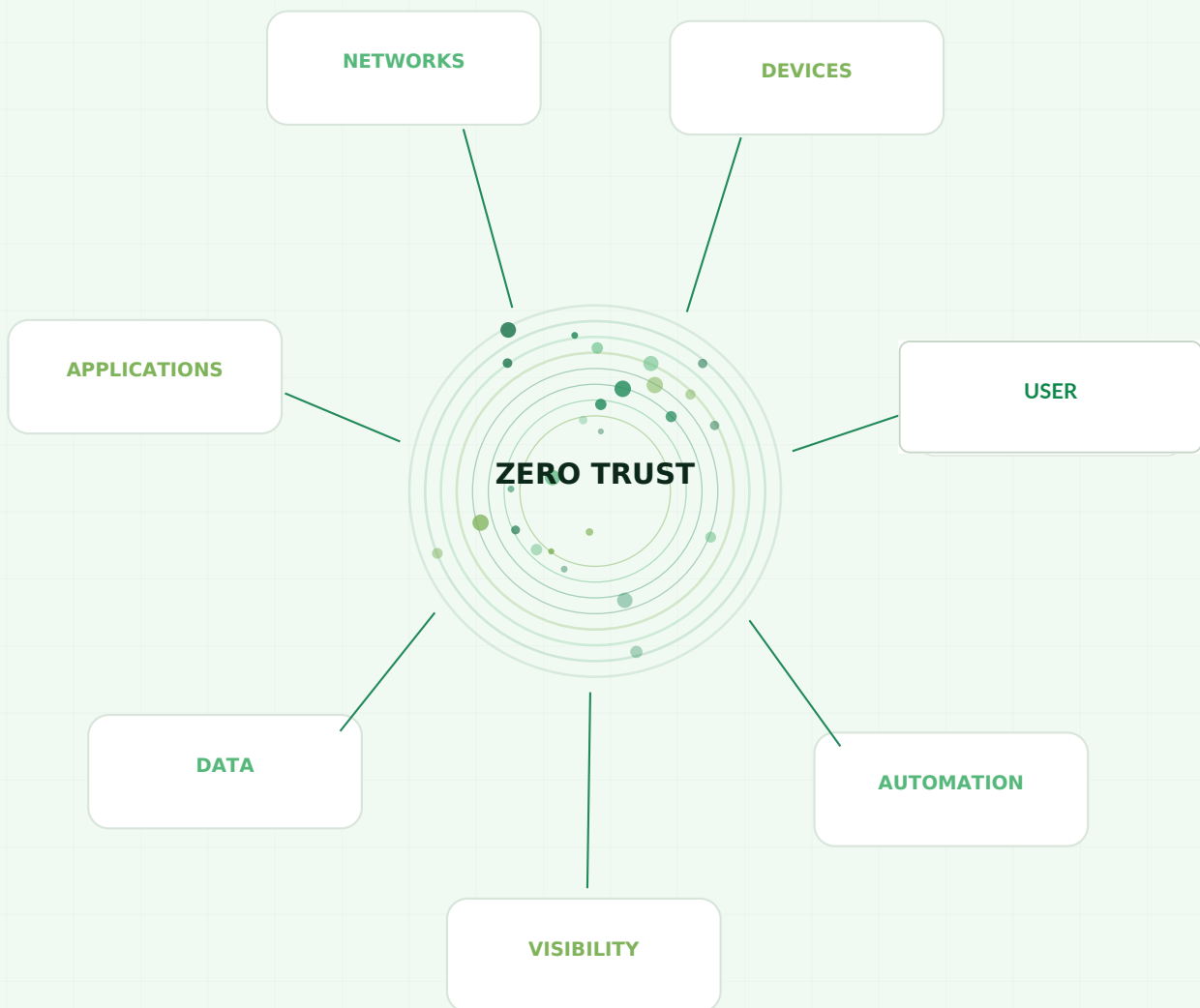
SEVEN PILLARS, ONE TRUST FABRIC

Post-quantum cryptography and Zero Trust reinforce each other

PQC protects selected cryptographic mechanisms; Zero Trust governs who and what may act, on which data, under what conditions, with continuous verification.

DECISION RULE

Do not create a separate quantum enclave. Integrate cryptographic inventory, algorithm posture, certificate health, device capability, workload identity, data lifetime, and migration status into Zero Trust policy and telemetry.



PQC strengthens selected trust mechanisms; Zero Trust governs continuous authorization and policy.

STOP BUYING NEW QUANTUM DEBT

Post-quantum-ready acquisition language

Translate strategy into observable supplier obligations. Tailor every clause to system classification, authority, profile, and acquisition vehicle.

DECISION RULE

A promise to 'support post-quantum cryptography' is not an acceptance criterion. Require exact algorithms and profiles, implementation and validation evidence, update mechanisms, performance results, inventory transparency, transition dates, and remedies.

01

CRYPTOGRAPHIC INVENTORY

Require algorithms, parameters, protocols, certificates, libraries, modules, trust roots, hardware security module / key-management system use, signing paths, interfaces, and dependencies.

02

MACHINE-READABLE EVIDENCE

Require version, owner, confidence, evidence source, architecture mapping, reconciliation process, and export format.

03

APPROVED TRANSITION SUPPORT

Name required NIST, CNSA 2.0, or capability-package support by product version and date, including hybrid behavior and negotiation rules.

04

TESTABLE IMPLEMENTATION

Require standards mapping, validation or evaluation status, configuration evidence, protocol capture, performance, failure handling, and supplier roadmap.

05

CRYPTOGRAPHIC AGILITY

Require abstraction, update path, configuration control, algorithm replacement, certificate and key lifecycle, rollback, telemetry, and compatibility policy.

06

ACCEPTANCE AND REMEDIES

Define test gates, documentation, delivery dates, deficiency correction, upgrade rights, data return, end-of-support, and nonconformance remedies.

ILLUSTRATIVE RACI

Governance: one accountable owner for each decision

A central PQC office can set standards and aggregate evidence, but it cannot replace mission-owner decisions.

DECISION	ENTERPRISE	MISSION OWNER	ENGINEERING	ACQUISITION	AUTHORIZING	SUPPLIER
Inventory	A	R	C	C	I	C
Priority	C	A	R	C	I	C
Architecture	A	R	R	C	C	C
Exception	R	C	C	C	A	I
Acceptance	A	R	R	C	C	C

Decision rule

Exactly one A per decision. R performs the work; C provides required input; I receives the decision and evidence. Every high-risk trust path needs one accountable owner and one recorded risk authority.

-  A accountable
-  R responsible
-  C consulted
-  I informed

The military mission exposure map



Photo: Maj. Nadine Wiley De Moura / U.S. Air Force / DVIDS | Public domain

IN THIS PART

- Enterprise identity, PKI, and access control
- Cloud, software factories, DIB, and suppliers
- C2, tactical networks, SATCOM, and weapons
- Sensors, ISR, AI, autonomy, and sustainment

KEY TERMS

C2 - command and control | SATCOM - satellite communications | ISR - intelligence, surveillance, and reconnaissance | DIB - Defense Industrial Base | CUI - Controlled Unclassified Information | MPE - Mission Partner Environment

MISSION DOMAIN 01

Enterprise identity, PKI, and access control

Identity is the common control plane connecting people, machines, workloads, devices, facilities, data, and administrative authority.

MISSION TAKEAWAY

Prioritize trust anchors and identity systems by blast radius. A vulnerable or poorly migrated root, signing service, device identity, or federation bridge can affect thousands of systems even when individual applications use strong encryption.

PEOPLE — User and privileged identity.

PIV/CAC and derived credentials, administrative certificates, MFA, federation, privilege, remote access, email, signing, and recovery.

MACHINES — Non-person entities.

Servers, endpoints, workloads, containers, services, APIs, devices, radios, sensors, robots, gateways, and automated agents with certificates or keys.

TRUST — PKI and roots.

Roots, intermediates, enrollment, validation, revocation, HSMs, trust stores, templates, policy, cross-certification, and coalition interoperability.

ACCESS — Authorization context.

Identity alone is insufficient. Device posture, workload state, data sensitivity, mission, location, behavior, and risk must shape access decisions.

MISSION DOMAIN 02

Tactical command and control

C2 depends on authentic data, trusted identity, resilient transport, software integrity, time, and the ability to operate through disruption.

MISSION TAKEAWAY

The highest-consequence quantum failure in C2 may be forged or rejected trust - not bulk decryption. Model how a compromised signature, certificate, firmware image, key service, or federation path could deny, delay, deceive, or redirect command.

Command authenticity.

Orders, messages, tracks, fires data, mission plans, software configurations, and operational updates may depend on signatures, certificates, message authentication, and trusted time.

Transport protection.

Tactical networks combine line-of-sight, beyond-line-of-sight, terrestrial, SATCOM, cellular, Wi-Fi, mesh, gateway, and coalition paths. Each negotiation and relay can preserve legacy cryptography.

Identity at the edge.

Disconnected and intermittently connected forces still need device, user, workload, and mission-partner identity. Revocation, time drift, trust-store updates, and emergency access become harder.

Data fusion and provenance.

C2 confidence depends on the origin and integrity of sensor, intelligence, logistics, and partner data. Post-quantum signatures and provenance can be as important as confidentiality.



MISSION DOMAIN 03

Tactical-edge constraint matrix

A cryptographic design that works in a laboratory may fail under bandwidth, compute, power, latency, and sustainment constraints.

DECISION RULE

Benchmark the complete mission handshake and message flow under representative impairment. Average-case server performance is not evidence for a radio, sensor, unmanned platform, or intermittent tactical link.



BANDWIDTH

Measure handshake and signature bytes, fragmentation, retransmission, and over-the-air burden.

REQUIRED EVIDENCE - NOT A SCORE



LATENCY

Measure end-to-end mission timing, timeout behavior, and degraded-link recovery.

REQUIRED EVIDENCE - NOT A SCORE



POWER

Measure CPU, memory, energy, battery, thermal, and duty-cycle impact.

REQUIRED EVIDENCE - NOT A SCORE



DISCONNECTED

Test offline authentication, revocation behavior, key rollover, recovery, and stale-state handling.

REQUIRED EVIDENCE - NOT A SCORE



HARDWARE

Record cryptographic library, accelerator, memory, lifecycle, update path, and supply constraints.

REQUIRED EVIDENCE - NOT A SCORE



CERTIFICATION

Define safety, airworthiness, interoperability, test authority, evidence, and acceptance gates.

REQUIRED EVIDENCE - NOT A SCORE

No universal bars or scores are shown. Each constraint must be measured against representative mission conditions and an approved acceptance threshold.

MISSION DOMAIN 04

Tactical radios and data links

Radio security is an ecosystem of key management, waveform behavior, device trust, embedded software, gateways, and operational procedures.

MISSION TAKEAWAY

Do not evaluate PQC only as an IP-layer handshake. Determine where the radio, waveform, gateway, fill device, key-management infrastructure, embedded module, and mission application establish or consume cryptographic trust.

● Waveform and protocol limits.

Message size, fragmentation, link establishment, timing, retransmission, anti-jam behavior, header constraints, duty cycle, multicast, group keying, and backward compatibility can shape the viable profile.

● Key distribution.

Electronic key management, over-the-air rekey, fill devices, local generation, coalition keys, emergency keys, compromise response, and disconnected operations need a PQC transition path.

● Embedded trust.

Secure boot, firmware signing, FPGA images, configuration, maintenance laptops, debug interfaces, vendor tools, update servers, and supply-chain provenance may remain classical after transport changes.

● Mixed-force operations.

PQC-capable and legacy units will coexist. Define gateway trust, downgrade rules, route selection, key domains, data release, operational indicators, and a retirement schedule.



MISSION DOMAIN 05

SATCOM and the space-ground-user trust chain

Space systems combine long-lived platforms, remote update, cross-border infrastructure, shared providers, constrained links, and high-consequence command trust.

MISSION TAKEAWAY

Map cryptography across the space segment, ground segment, user segment, inter-satellite and terrestrial links, provider control plane, software supply chain, and mission data lifecycle. A secure link does not compensate for vulnerable command or firmware signing.

SPACE — Satellite platform and payload.

Command authentication, telemetry, secure boot, firmware and FPGA updates, payload control, inter-satellite links, keys, time, and long replacement cycles.

GROUND — Control and gateway infrastructure.

Mission control, provider networks, ground stations, cloud services, APIs, operator identity, remote administration, databases, monitoring, and supplier access.

USER — Terminals and tactical integration.

Terminal identity, firmware, management, keying, local networks, applications, gateways, coalition use, mobility, physical exposure, and disconnected operation.

LINKS — Communications and routing.

Uplink, downlink, crosslink, terrestrial backhaul, tunneling, traffic steering, encryption, authentication, jamming response, failover, and provider boundaries.

MISSION DOMAIN 06

Weapons systems and embedded cryptography

Long platform life, safety, certification, constrained hardware, proprietary interfaces, and supplier depth make weapons migration a portfolio engineering problem.

MISSION TAKEAWAY

Start with mission and safety functions, then map every cryptographic dependency and replacement constraint. The decisive work may be redesigning roots of trust, update chains, interfaces, modules, and sustainment contracts years before a fielded cutover.

Secure boot and firmware.

Platform controllers, mission computers, sensors, effectors, processors, radios, FPGAs, maintenance devices, and test equipment may trust classical signatures rooted in long-lived hardware.

Embedded key establishment.

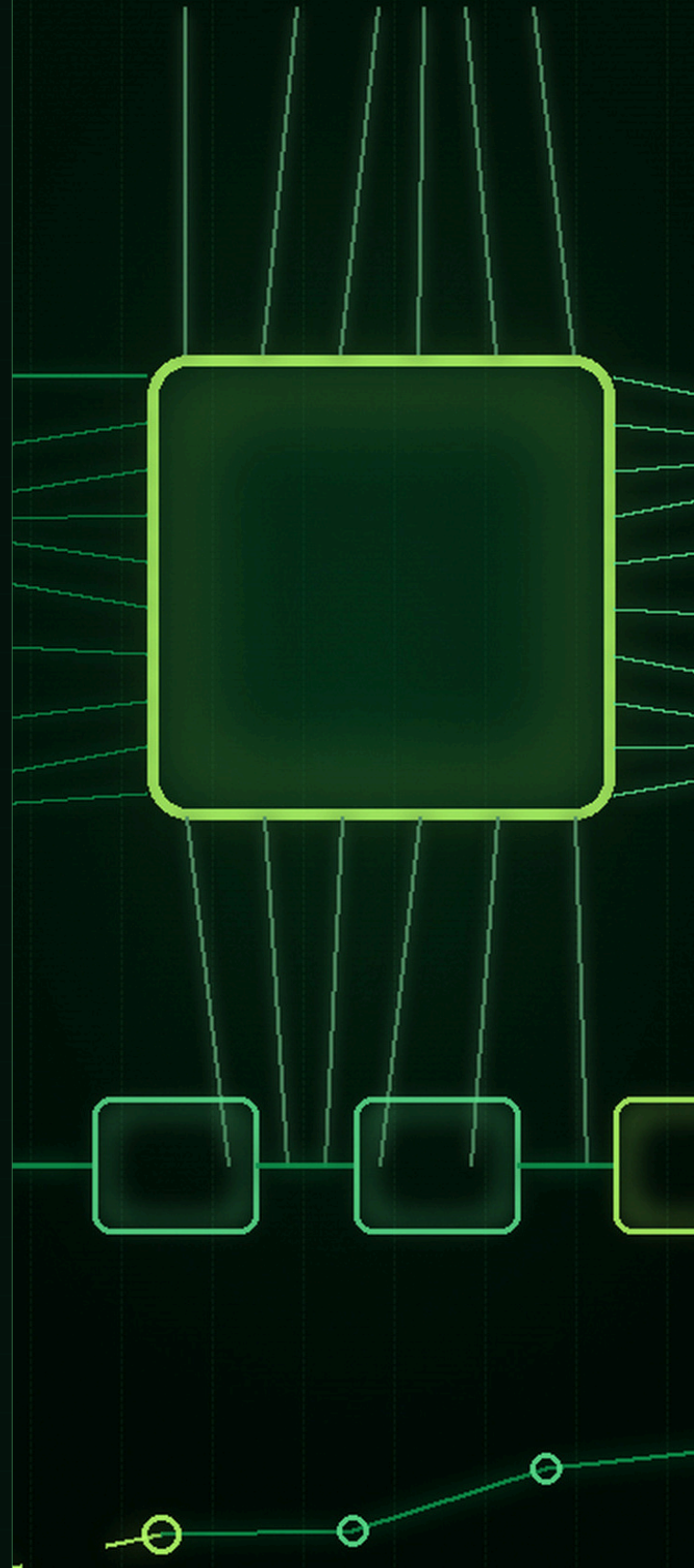
Proprietary protocols, line-replaceable units, internal buses, remote maintenance, data loaders, diagnostic tools, and support equipment can hide RSA or ECC dependencies.

Safety and certification.

Algorithm changes can affect timing, resource use, deterministic behavior, software baselines, hardware qualification, airworthiness, weapons safety, interoperability, and authorization evidence.

Sustainment reality.

Obsolescence, diminishing manufacturing sources, source-code access, vendor viability, export controls, depot tooling, spares, technical orders, and training determine migration feasibility.



MISSION DOMAIN 07

Operational technology and industrial control systems

OT supports installations, logistics, energy, environmental control, manufacturing, test, maintenance, and mission systems - often with long lifecycles and safety constraints.

MISSION TAKEAWAY

Do not introduce PQC into OT through an enterprise mandate without asset-level engineering. Availability, deterministic control, vendor support, maintenance windows, serial and proprietary protocols, safety, and fallback govern the migration sequence.

Hidden cryptography.

Remote access, VPNs, engineering workstations, vendor portals, firmware signing, device certificates, wireless links, historians, APIs, backup systems, and cloud analytics may use public-key cryptography.

Availability first.

A security improvement that disrupts process control, safety, power, environmental conditions, or mission support can create unacceptable operational risk. Validate timing and failure modes.

Vendor dependency.

Many controllers and appliances cannot change algorithms without firmware, replacement, or vendor services. Inventory model, version, support status, update path, and supplier roadmap.

Segmentation is temporary risk reduction.

Gateways, isolation, application proxies, one-way transfer, access restriction, and monitoring can reduce exposure but do not erase vulnerable internal trust or long-lived data.

MISSION DOMAIN 08

Cloud, software factories, and DevSecOps

Modern software delivery concentrates cryptographic trust in identities, APIs, build systems, artifacts, secrets, service meshes, cloud control planes, and automated policy.

MISSION TAKEAWAY

The fastest way to stop new quantum debt is to instrument software delivery. Detect vulnerable libraries and protocols before release, require signed provenance, use agile cryptographic interfaces, and keep deployment evidence synchronized with the inventory.

SOURCE — Repositories and dependencies.

Developer identity, commit and tag signing, package provenance, third-party libraries, cryptographic APIs, secrets, dependency graphs, and branch protections.

BUILD — Pipeline and signer.

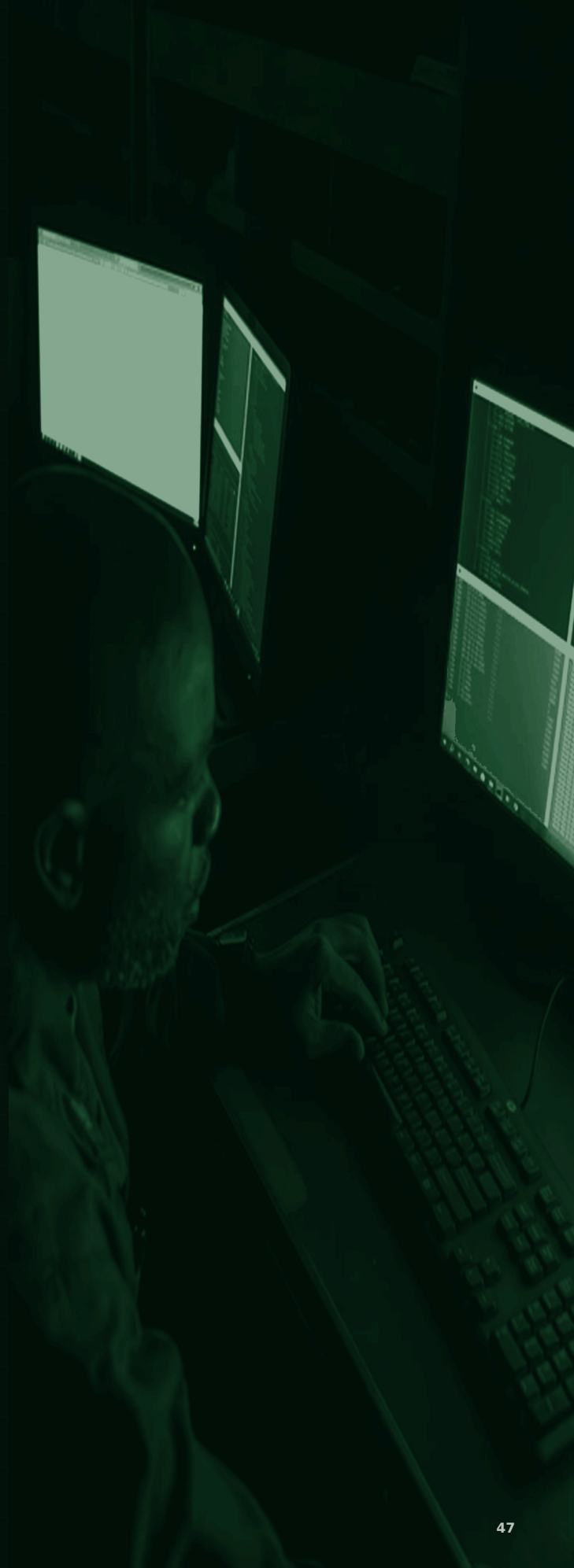
Workload identity, CI/CD services, build isolation, artifact signing, key custody, HSM/KMS, reproducibility, SBOM/CBOM, attestations, and policy gates.

REGISTRY — Artifacts and supply chain.

Images, packages, firmware, manifests, signatures, provenance, scanning, replication, retention, promotion, quarantine, and revocation.

RUNTIME — Applications and service identity.

TLS, service mesh, certificates, APIs, database connections, secrets, tokens, workload identity, sidecars, gateways, and crypto-provider versions.



MISSION DOMAIN 09

Code signing, firmware, and the software trust chain

The ability to forge or bypass software trust can create persistent mission effects below the application layer.

MISSION TAKEAWAY

Treat signing roots and verification code as Tier 0 assets. A post-quantum signing migration must cover key generation, custody, certificate or public-key distribution, signer access, build provenance, verification, rollback, revocation, archival validation, and emergency recovery.

AUTHORIZE.

A person or workload is explicitly permitted to produce a release under controlled identity, role, and policy.

BUILD AND ATTEST.

The system creates a reproducible artifact with dependency, environment, approval, and provenance evidence.

SIGN AND DISTRIBUTE.

A controlled signer binds integrity and origin; registries, repositories, and delivery channels preserve the evidence chain.

VERIFY AND EXECUTE.

Bootloaders, devices, platforms, applications, and operators enforce trust, reject invalid states, support rollback, and preserve audit evidence.

MISSION DOMAIN 10

Long-lived data and archive exposure

The archive problem combines future confidentiality, present collection, old encryption, backup proliferation, key retention, and the need to preserve integrity for decades.

MISSION TAKEAWAY

Inventory data sets and cryptographic envelopes together. Re-encryption priorities should consider sensitivity lifetime, copy count, exposure, access, key custody, legal and intelligence requirements, operational need, and the feasibility of verifiable transformation.

REQUIRED LIFETIME.

Inventory data sets and cryptographic envelopes together. Record how long confidentiality, integrity, authenticity, and evidentiary value must survive.

COPY PROLIFERATION.

Include backups, replicas, removable media, cloud archives, partner copies, legal holds, disaster recovery, data lakes, exports, and encrypted traffic captures.

COLLECTION EXPOSURE.

Evaluate where adversaries, insiders, suppliers, partners, or compromised services could obtain material today.

RE-ENCRYPTION FEASIBILITY.

Prioritize sensitivity, copy count, access, key custody, legal and intelligence requirements, operational need, and the feasibility of verifiable transformation.





Photo: Lt. Col. Victoria Hight / U.S. Space Force / DVIDS | Public domain

MISSION DOMAIN 11

Coalition and allied interoperability

Coalition operations depend on shared trust, releasability, identity federation, gateways, approved algorithms, common profiles, and synchronized transition windows.

MISSION TAKEAWAY

A unilateral migration can create mission failure if partners, gateways, radios, certificates, message formats, or policy domains cannot interoperate. Treat coalition transition as an operational design problem with explicit coexistence and retirement rules.

Common profile.

Agree on algorithms, parameters, protocols, certificate policy, identity assurance, message formats, validation expectations, and exception authority for the specific mission environment.

Federated identity.

Map cross-certification, federation metadata, trust anchors, device and workload identity, attribute release, revocation, partner onboarding, and emergency access under mixed cryptographic states.

Gateway concentration.

Mission partner gateways, guards, translators, relays, cross-domain systems, and cloud exchange points can become blast-radius amplifiers or downgrade chokepoints.

Releasability and data policy.

A quantum-safe channel does not authorize release. Data labels, nationality, need-to-know, mission role, handling rules, and provenance must remain enforceable.

MISSION DOMAIN 12

The Defense Industrial Base and CUI trust chain

The DoW strategy extends PQC transition into the DIB because military mission systems inherit supplier cryptography, software, services, technical data, and operational dependencies.

MISSION TAKEAWAY

The prime contractor's perimeter is not the system boundary. Map cryptography and data movement through subcontractors, cloud and SaaS providers, engineering environments, software supply chains, remote support, manufacturing, logistics, and archives.

CONTRACT — Requirements and flow-down.

Named profiles, inventory evidence, crypto agility, implementation dates, validation, notification, subcontractor obligations, remedies, and data-return or exit requirements.

ENGINEERING — Technical data environments.

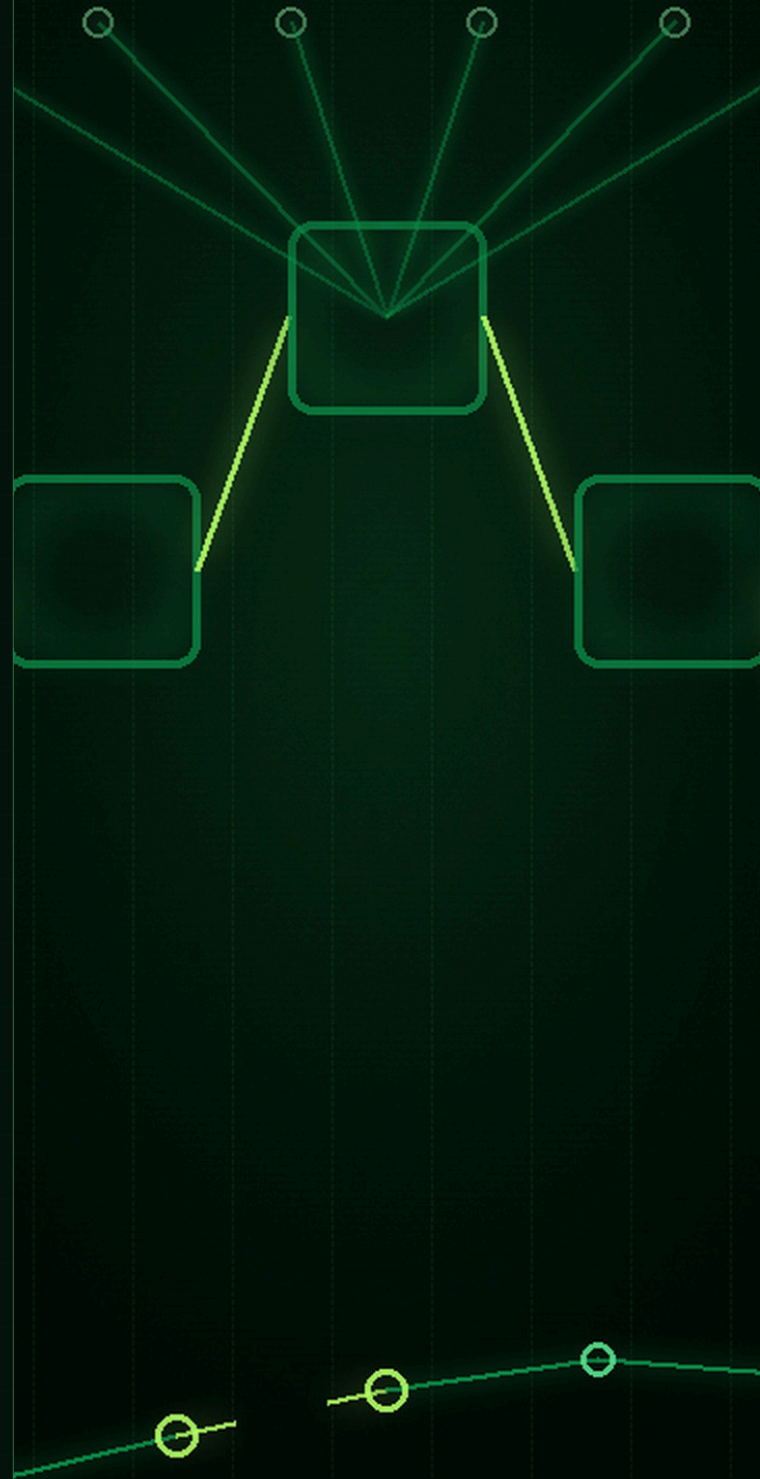
CUI repositories, PLM/CAD, source code, build pipelines, collaboration, email, remote access, backups, key management, certificates, and long-lived weapon-system information.

PRODUCT — Delivered hardware and software.

Embedded libraries, protocols, roots of trust, firmware signing, secure boot, update paths, HSMs, appliances, radios, sensors, test equipment, and support tools.

SERVICE — Managed and remote operations.

SaaS, cloud, help desk, remote maintenance, telemetry, update servers, identity federation, subcontractor access, service accounts, and shared-responsibility boundaries.



MISSION DOMAIN 13

Physical access, PIV/CAC, and facility trust

Physical access systems combine credentials, certificates, readers, panels, controllers, networks, visitor systems, identity proofing, and emergency procedures.

MISSION TAKEAWAY

Migration must preserve life safety, continuity, offline operation, visitor handling, revocation, anti-passback, emergency access, and interoperability across facilities. Replacing the badge certificate alone is not the full system change.

Credential lifecycle.

Issuance, derived credentials, lost-card response, revocation, expiration, certificate updates, PIN and biometric factors, personalization, and trust-anchor distribution.

Reader and controller estate.

Firmware, embedded crypto, secure channels, device identity, management interfaces, local caches, time, offline behavior, physical tamper, and replacement constraints.

Back-end integration.

Identity sources, visitor systems, HR/personnel data, access policy, logging, analytics, federation, APIs, network segmentation, and certificate validation services.

Emergency operations.

Fire and life-safety modes, lockdown, continuity during CA or network outage, manual override, incident command, audit, and recovery require explicit test cases.

MISSION DOMAIN 14

Unmanned systems and autonomous platforms

Autonomy expands the number of non-person identities, remote update paths, sensor trust relationships, control links, models, and machine-to-machine decisions.

MISSION TAKEAWAY

The quantum concern is not only encrypted control traffic. Authentication of commands, mission data, navigation, software, models, sensors, swarms, maintenance tools, and recovery states can determine whether an autonomous system acts for the right authority.

IDENTITY — Platform and component identity.

Vehicle, payload, sensor, controller, radio, maintenance tool, operator, workload, and mission-package identities with scalable issuance and revocation.

CONTROL — Command, telemetry, and data links.

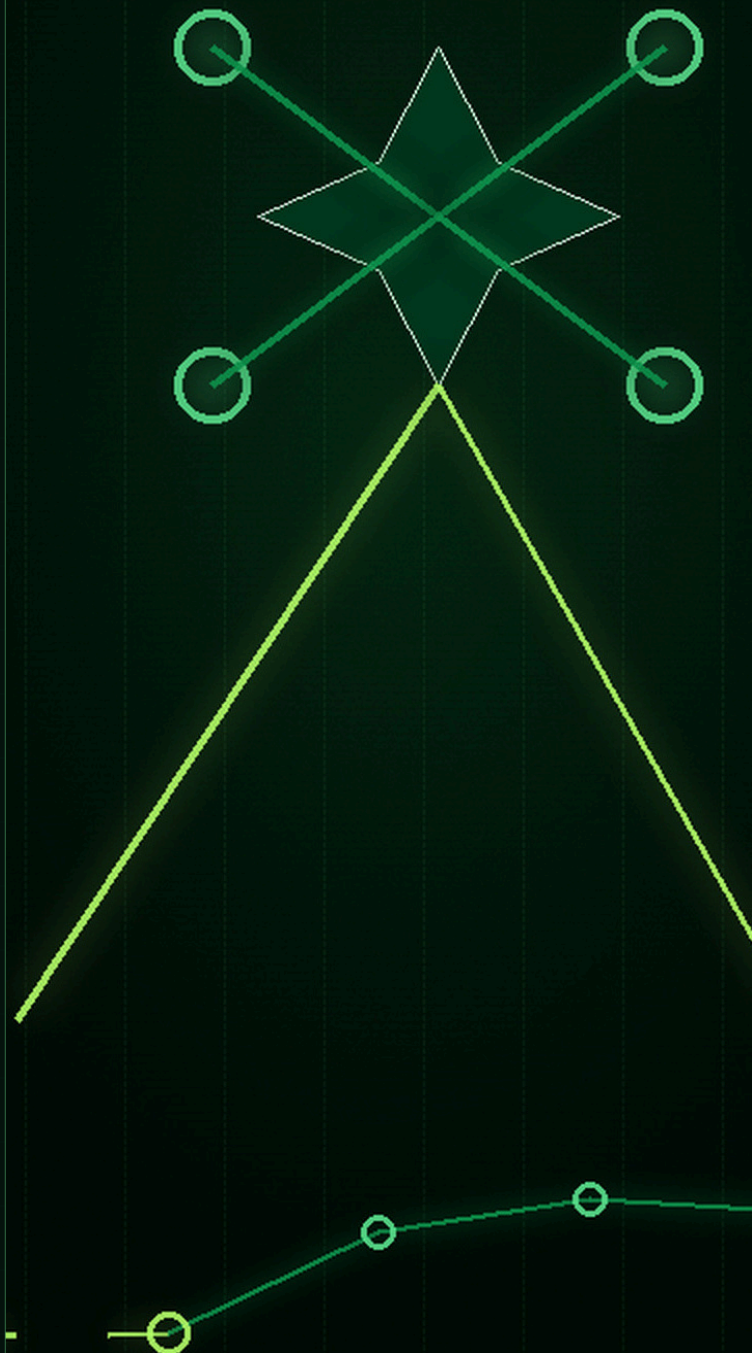
Authenticated control, mission updates, telemetry, group keying, swarm communications, relay, gateway trust, loss, latency, jamming, and disconnected behavior.

SOFTWARE — Boot, firmware, applications, and models.

Signed boot chains, remote update, model provenance, configuration, rollback prevention, third-party components, mission data, and emergency recovery images.

SENSING — Navigation and data provenance.

Sensor identity, timestamp, calibration, fusion, GNSS alternatives, data signing, anti-spoofing, trusted time, and confidence in machine-generated observations.



MISSION DOMAIN 15

Sensors, ISR, and data provenance

Intelligence, surveillance, and reconnaissance depends on confidence in source, time, location, calibration, transformation, dissemination, and analytic lineage.

MISSION TAKEAWAY

PQC can help preserve authenticity and confidentiality, but only a provenance architecture can show who or what generated the observation, how it changed, which models touched it, and whether the mission consumer should trust it.

Sensor identity.

Every sensor, payload, gateway, processing node, analytic service, and human release authority may require a machine or user identity with an auditable lifecycle.

Time and location.

Signed timestamps, clock sources, location assertions, calibration, synchronization, and anti-spoofing influence whether data can support targeting, warning, or attribution.

Data-in-motion.

Tactical links, SATCOM, gateways, relays, cloud ingestion, cross-domain transfer, coalition sharing, and dissemination each introduce cryptographic and policy dependencies.

Data-at-rest and archive.

Raw collections, derived products, labels, metadata, backups, models, and analyst work may retain value for years and face HNDL exposure.

MISSION DOMAIN 16

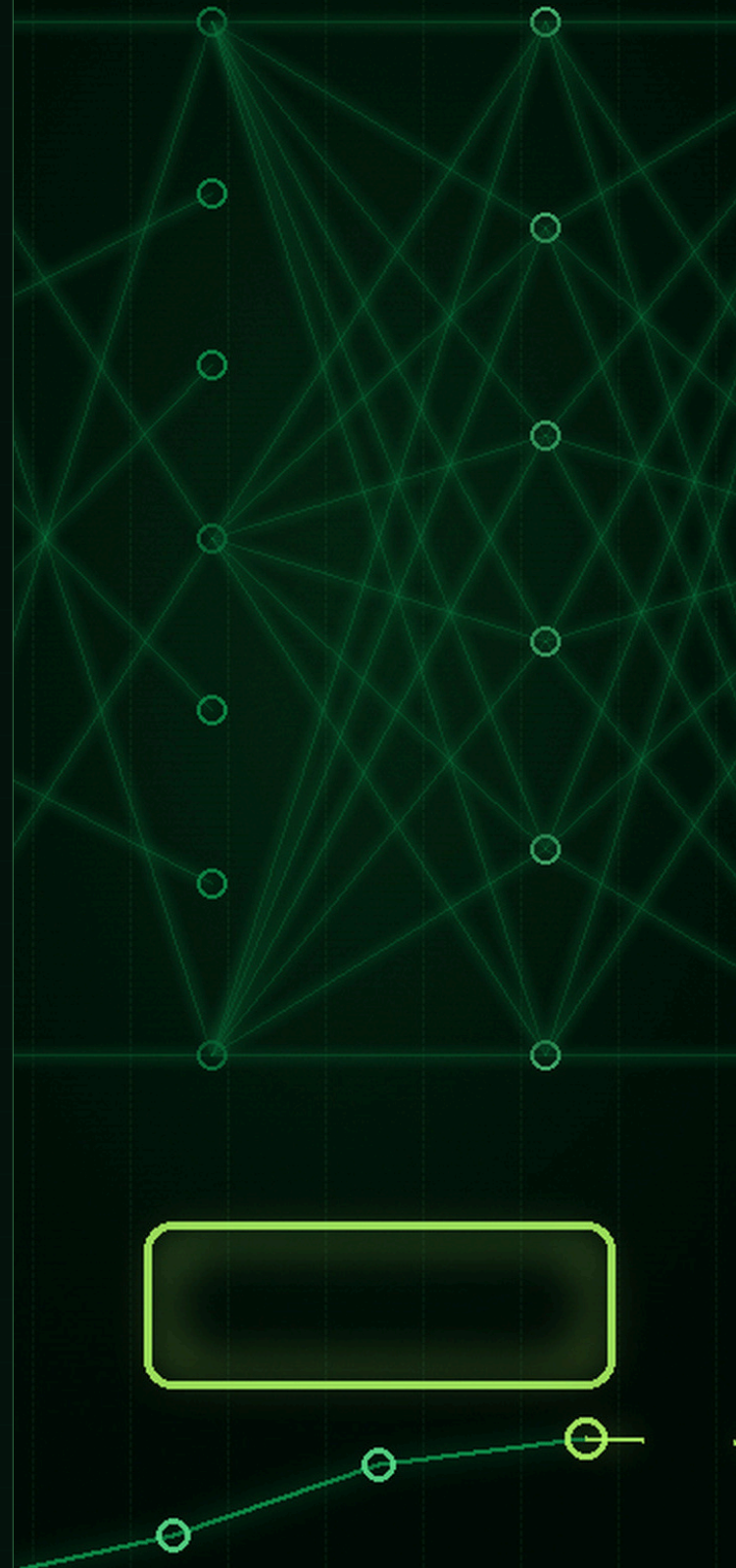
AI and machine-learning pipelines

AI systems inherit cryptographic dependencies from data, models, software, infrastructure, identities, APIs, updates, and autonomous action.

MISSION TAKEAWAY

A quantum-ready AI pipeline needs trustworthy data and model provenance, protected service and agent identities, signed artifacts, agile transport, secure key management, and controls over what machine actors may do.

- **DATA — Training and operational inputs.**
Source identity, labels, rights, integrity, confidentiality lifetime, lineage, storage, transfer, cross-domain release, poisoning detection, and access control.
- **MODEL — Weights, prompts, policies, and provenance.**
Signing, hashing, registry, version, approvals, evaluation results, fine-tuning lineage, rollback, intellectual property, and long-lived sensitive content.
- **SERVICE — APIs, workloads, and agents.**
Workload identity, certificates, tokens, secrets, tool authorization, service mesh, model endpoints, agent actions, non-person entities, and least privilege.
- **DELIVERY — Build and deployment.**
Repositories, pipelines, dependencies, containers, artifact signing, policy gates, environment promotion, HSM/KMS, configuration, and software supply chain.



MISSION DOMAIN 17

Logistics, maintenance, and sustainment

Sustainment systems connect suppliers, depots, transport, inventory, predictive maintenance, technical data, software updates, identity, and physical operations.

MISSION TAKEAWAY

Quantum migration succeeds only when sustainment can support it: replacement parts, firmware, certificates, keys, technical orders, training, depots, test equipment, vendor access, and funding must match the fielded configuration.

Technical data.

Maintenance manuals, engineering drawings, software, vulnerabilities, configurations, serial numbers, mission data, and parts information may require long confidentiality and integrity lifetimes.

Asset and supplier identity.

Parts, devices, vendors, technicians, service accounts, tools, and logistics systems rely on credentials, signatures, certificates, barcodes, APIs, and provenance.

Remote maintenance.

Vendor tunnels, diagnostic portals, maintenance laptops, removable media, cloud analytics, telemetry, and update services create high-value trust paths.

Configuration control.

The authoritative inventory must know which algorithm, library, firmware, certificate, trust anchor, and hardware revision is actually installed on each fielded configuration.

FIELD COMMUNICATIONS | SUSTAINMENT

Photo: 1st Sgt. Sharon Mock / U.S. Navy / DVIDS | Public domain

MISSION DOMAIN 18

5G, private wireless, and edge compute

Private wireless and edge architectures combine subscriber identity, device certificates, core-network trust, orchestration, APIs, cloud-native software, slicing, and supplier ecosystems.

MISSION TAKEAWAY

Map cryptography across the radio access network, transport, core, management, orchestration, edge workloads, device enrollment, roaming or partner interfaces, and software supply chain. A PQC tunnel at one layer does not secure the full system.

Subscriber and device trust.

SIM/eSIM credentials, device certificates, enrollment, attestation, user identity, mission roles, revocation, roaming, and non-person identities.

Network functions.

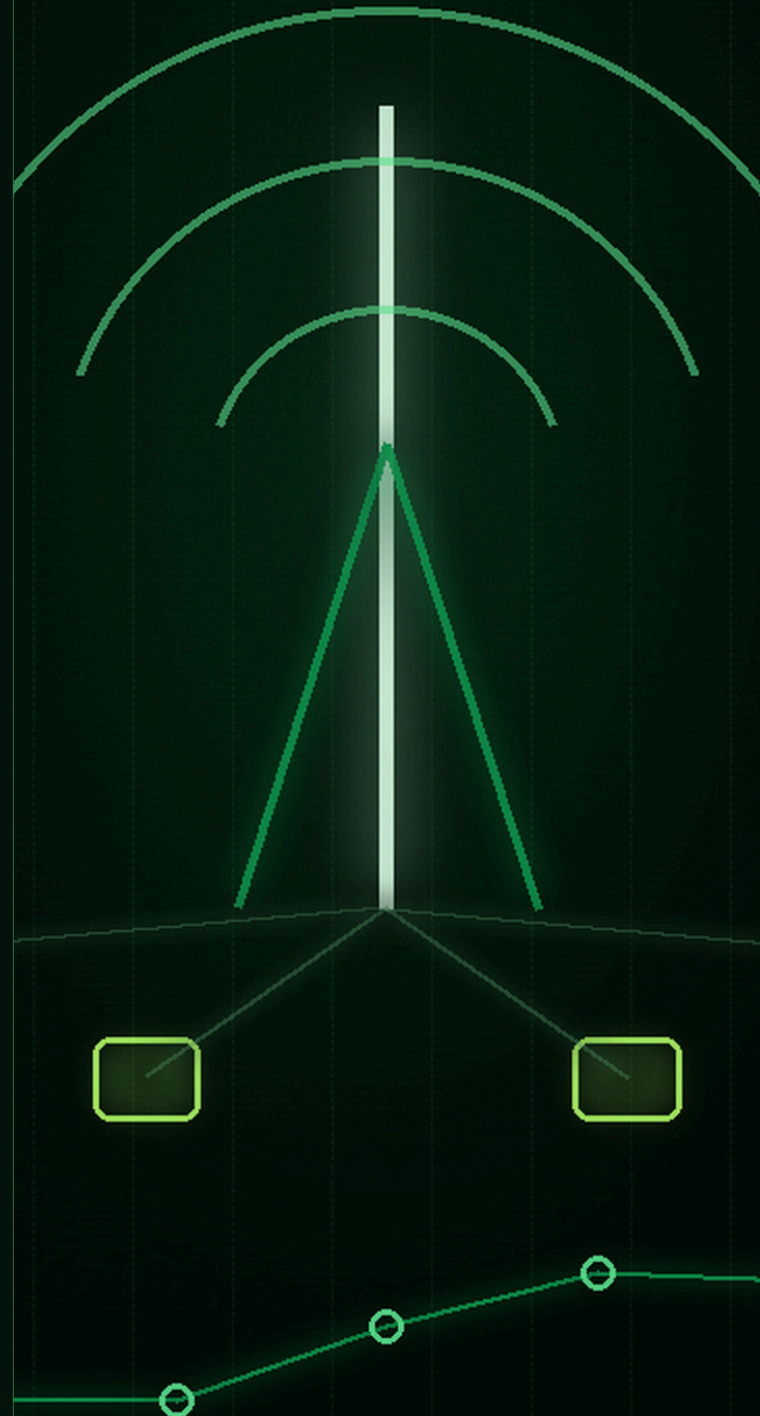
Virtualized and containerized core functions, service mesh, APIs, certificates, secrets, orchestration, management planes, images, and artifact signing.

Edge applications.

Mission workloads, sensors, AI services, databases, message buses, gateways, and local KMS/HSM dependencies may use separate cryptographic stacks.

Transport and backhaul.

Fiber, microwave, SATCOM, IPsec, TLS, vendor tunnels, synchronization, and redundant paths can negotiate or preserve legacy algorithms.



MISSION DOMAIN 19

Mission Partner Environments

MPEs aggregate identity, network, data, cloud, gateway, coalition, policy, and releasability dependencies under time pressure.

MISSION TAKEAWAY

A post-quantum MPE needs a shared cryptographic profile, partner onboarding and evidence model, trusted gateways, identity federation, data policy enforcement, coexistence rules, and a joint test event before mission use.

PARTNERS — Identity and trust federation.

Partner roots, federation, certificate policy, device and workload identity, assurance levels, attributes, revocation, onboarding, departure, and emergency access.

NETWORK — Transport and gateways.

Tunnels, gateways, cloud exchange, SATCOM, tactical links, routing, segmentation, inspection, cross-domain transfer, and negotiation or downgrade behavior.

DATA — Labels, release, and provenance.

Nationality, classification, releasability, mission role, origin, integrity, retention, translation, transformation, and policy enforcement across domains.

SERVICES — Shared applications and cloud.

Collaboration, C2, data services, identity providers, APIs, workloads, service mesh, PKI, KMS, signing, logs, and supplier-managed capabilities.

MISSION DOMAIN 20

Cross-domain solutions and high-assurance gateways

Cross-domain systems concentrate parsing, policy, identity, signatures, data labeling, inspection, release, and trusted transfer between security domains.

MISSION TAKEAWAY

PQC changes can affect both transport and the trusted computing base. Treat guards, filters, transfer protocols, signing, validation, policy updates, management, audit, and fail-safe behavior as one high-assurance migration.

Trusted path.

Identify cryptography at endpoints, transfer applications, guards, one-way devices, gateways, inspection services, data-labeling systems, management channels, and audit repositories.

Signature verification.

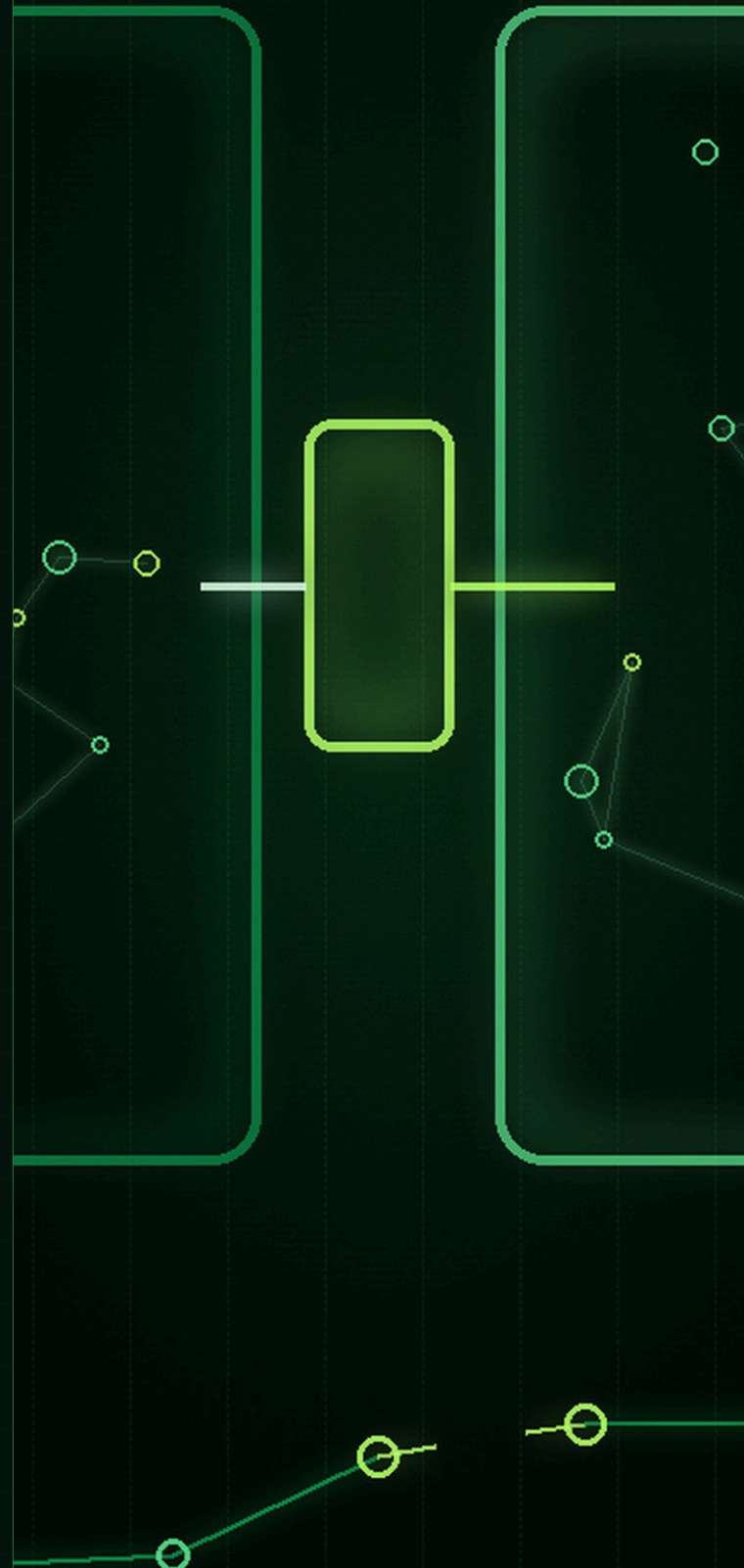
Cross-domain release may rely on origin, integrity, approval, sanitization, and provenance signatures. Verify that the complete signing and validation chain can transition.

Protocol and parser impact.

Larger certificates, keys, signatures, and handshake messages can affect buffers, schemas, message limits, parser behavior, transfer latency, and failure modes.

High-assurance change.

Updates may require specialized evaluation, regression, configuration control, hardware or firmware changes, accreditation evidence, and carefully controlled fielding.



COVERAGE BEFORE RANKING

Twenty mission domains - one evidence-screening map

This is a coverage map, not a universal priority ranking. Every mission owner re-scores the domains from local consequence, data and trust lifetime, collection opportunity, supplier lead time, replacement friction, and evidence confidence.

P.40 Enterprise identity, PKI, and access control Screen first for: roots, credentials, machine identity	P.50 Coalition and allied interoperability Screen first for: profiles, releasability, shared trust
P.41 Tactical command and control Screen first for: degraded operations, command trust	P.51 Defense Industrial Base and CUI Screen first for: supplier evidence, contracts, data flow
P.42 Tactical-edge constraints Screen first for: latency, bandwidth, power, disconnection	P.52 Physical access and PIV/CAC Screen first for: credentials, readers, controllers, recovery
P.43 Tactical radios and data links Screen first for: waveforms, keys, negotiation, recovery	P.53 Unmanned and autonomous systems Screen first for: identity, update, control, safety
P.44 SATCOM and space-ground-user trust Screen first for: gateway, terminal, telemetry, update	P.54 Sensors, ISR, and provenance Screen first for: source, time, location, lineage
P.45 Weapons and embedded cryptography Screen first for: secure boot, firmware, long life	P.55 AI and machine-learning pipelines Screen first for: data, model, service, deployment
P.46 Operational technology and control Screen first for: safety, vendor access, legacy protocols	P.56 Logistics and sustainment Screen first for: technical data, spares, maintenance
P.47 Cloud and software factories Screen first for: control plane, CI/CD, secrets, services	P.57 5G, private wireless, and edge Screen first for: subscriber identity, transport, orchestration
P.48 Code signing and software trust Screen first for: roots, artifacts, firmware, rollback	P.58 Mission Partner Environments Screen first for: federation, coalition, shared services
P.49 Long-lived data and archives Screen first for: retention, copies, re-encryption	P.59 Cross-domain and high assurance Screen first for: labels, guards, release, evidence

P.xx denotes the linked page number - never priority, severity, or rank.

Evidence screen: mission consequence | data and trust lifetime | collection opportunity | replacement lead time | evidence confidence. Prioritize only after local scoring and accountable-owner review.

IV

Discovery and cryptographic risk intelligence

You cannot protect what you cannot see. The product job is to turn approved scope into evidence, materiality, ownership, and the next decision.

IN THIS PART

- Why cryptographic inventories fail
- Evidence fusion and CBOM structure
- HNDL priority and confidence
- QScout Gold and QScout Pulse

KEY TERMS

ACDI - automated cryptography discovery and inventory | CBOM - cryptographic bill of materials | CMDB - configuration management database | HSM - hardware security module | KMS - key-management system or service

ROOT CAUSES

Why cryptographic inventories fail

Most organizations possess fragments: certificate lists, scanner output, CMDB records, source scans, cloud inventories, spreadsheets, and vendor statements. They do not yet possess a decision-grade cryptographic estate.

MISSION TAKEAWAY

A useful inventory must answer where cryptography is used, what trust function it performs, who owns it, what mission and data it protects, how it was observed, how confident the finding is, what depends on it, and what action closes the risk.

Asset-centric instead of crypto-centric.

A CMDB may know a server exists but not the certificates, libraries, protocols, embedded keys, signing relationships, cloud services, or data lifetimes that create quantum exposure.

One tool, one surface.

Network scanners, source scanners, PKI tools, cloud APIs, SBOMs, HSM inventories, and vendor questionnaires each see different evidence. None should be treated as complete alone.

No mission or data linkage.

A list of RSA certificates does not reveal whether they protect a public website, a weapons update path, a root CA, long-lived intelligence, or an obsolete lab system.

No provenance or confidence.

Findings without evidence source, collection time, method, scope, parser or tool version, corroboration, and confidence cannot support risk acceptance or audit.

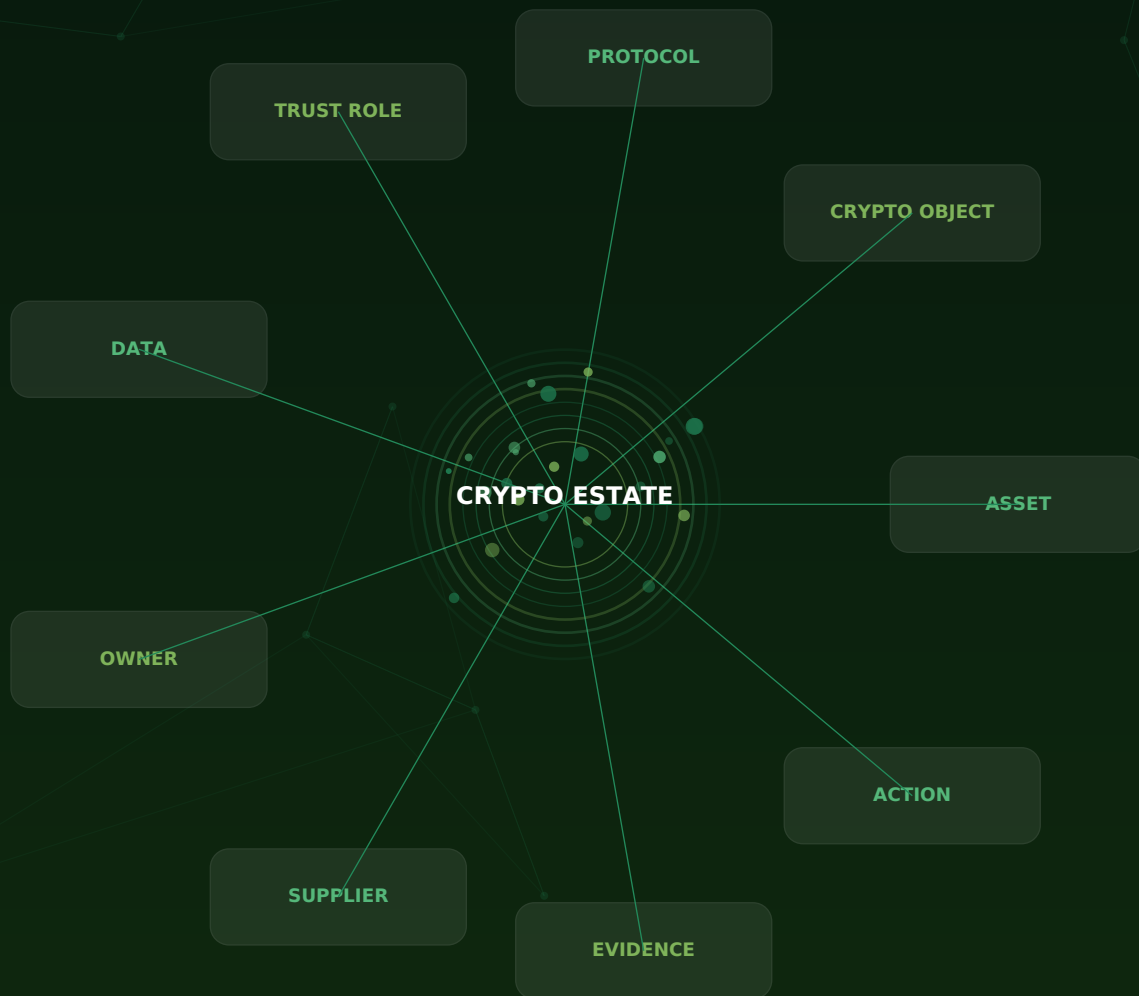
WHAT MUST BE INVENTORIED

The cryptographic estate taxonomy

Use a common schema across enterprise, tactical, embedded, cloud, software, physical, coalition, and DIB environments.

DECISION RULE

Inventory cryptographic objects and their relationships, not only algorithms. The same RSA or ECC mechanism has different risk depending on function, data, owner, exposure, trust role, replacement lead time, and downstream dependency.



COLLECT, CORRELATE, RECONCILE

Discovery is a multi-source evidence fusion problem

Authoritative inventory emerges from combining evidence sources with different coverage, confidence, cost, and operational risk.

DECISION RULE

Start with low-impact evidence, then deepen access where mission value justifies it. Preserve raw evidence and distinguish observed, inferred, declared, and validated facts.

NETWORK

coverage + confidence

CODE

coverage + confidence

CLOUD

coverage + confidence

PKI

coverage + confidence

KMS/HSM

coverage + confidence

CMDB

coverage + confidence

TELEMETRY

coverage + confidence

OWNER

coverage + confidence

CORRELATE | RECONCILE | PROVENANCE | OWNER REVIEW

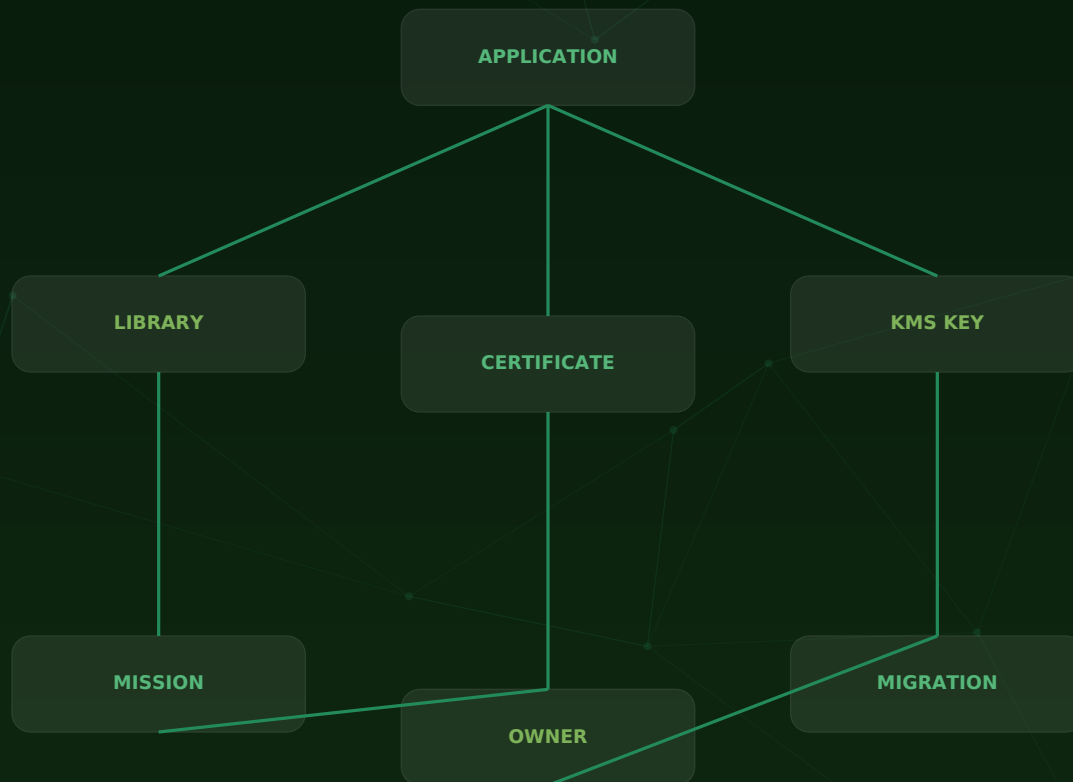
CRYPTOGRAPHIC BILL OF MATERIALS

A CBOM becomes useful when it is relational

A flat list of algorithms is not enough. A decision-grade CBOM links cryptographic objects to components, services, data, mission, owners, evidence, dependencies, and migration actions.

DECISION RULE

Use a machine-readable representation where practical, but preserve the operational semantics: why the cryptography exists, what it protects, who can change it, which profile controls it, and what proves closure.



A relational CBOM connects cryptography to consequence, ownership, evidence, and action.

LOW-FRICTION ENTRY POINT

External attack-surface discovery

External observation can rapidly identify internet-facing cryptographic posture and likely ownership questions without installing software or requesting internal credentials.

MISSION TAKEAWAY

External discovery is powerful for prioritization and owner engagement, but it cannot prove the absence of internal, embedded, disconnected, proprietary, classified, or supplier-managed cryptography. State the boundary visibly.

Domain and service mapping.

Domains, subdomains, DNS, certificate transparency, IP and ASN relationships, exposed ports, services, redirects, edge providers, and likely ownership boundaries.

TLS and certificate posture.

Protocol versions, offered suites, key exchange, signature algorithms, certificate chains, validity, key size, trust, host coverage, and observed negotiation behavior.

Public code and secrets indicators.

Public repositories, dependency files, configurations, documentation, accidental secrets, certificate material, endpoints, and cryptographic library indicators where lawfully observable.

Quantum-vulnerable exposure.

Observed RSA/ECC use, protocol dependencies, certificate and signature posture, externally visible legacy support, and likely migration questions.

WHERE QUANTUM DEBT IS CREATED

Source code and dependency discovery

Repositories and build systems can reveal hard-coded algorithms, provider APIs, protocol settings, certificate handling, key use, signing, dependencies, and migration friction before deployment.

MISSION TAKEAWAY

Make cryptographic discovery a software-delivery control. Detect vulnerable and non-agile patterns in code and dependencies, link them to released artifacts, then verify the deployed configuration rather than assuming source equals runtime.

Cryptographic API calls.

Key generation, encryption, decryption, KEM, signing, verification, hashing, KDF, random generation, certificate validation, trust stores, and provider selection.

Hard-coded policy.

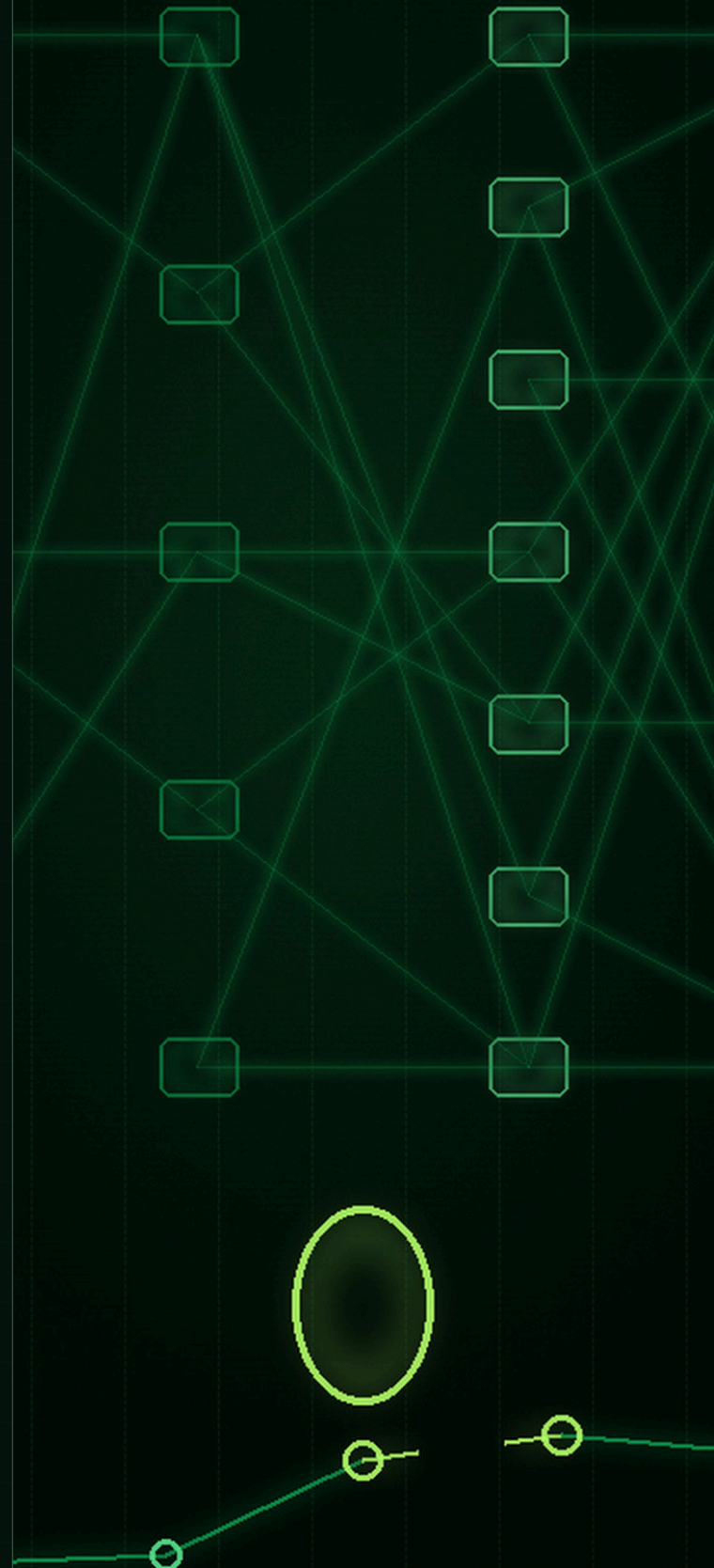
Algorithm names, key sizes, cipher suites, protocol versions, certificate pins, OIDs, provider-specific assumptions, serialized formats, message limits, and fallback behavior.

Dependencies.

Direct and transitive libraries, language runtimes, OS providers, containers, firmware SDKs, hardware APIs, open-source packages, and supplier components.

Build and signing.

Commit identity, artifact signing, HSM/KMS integration, manifests, attestations, SBOM/CBOM generation, key custody, release authorization, registry, and verification.



CONTROL-PLANE EVIDENCE

Cloud, KMS, HSM, PKI, and secrets discovery

Cloud control planes and platform services contain cryptographic objects, identities, policies, trust paths, and provider-specific evidence that network scanning alone cannot establish.

MISSION TAKEAWAY

Inventory the consuming trust path, not only the KMS key. A strong key in an HSM does not make a vulnerable certificate, protocol, signer, application, secret distribution path, or recovery process quantum ready.

CLOUD CONTROL PLANE.

Inventory account, subscription, project, region, policy, identity, network, workload, logging, and managed-service relationships through authorized APIs and exports.

PKI AND CERTIFICATES.

Map certificate authorities, roots, intermediates, leaf certificates, trust stores, enrollment, revocation, validation, expiry, ownership, and renewal paths.

KMS AND HSM.

Record key type, algorithm, purpose, owner, custody, rotation, exportability, backing hardware, policy, grants, aliases, replication, audit, and recovery.

SECRETS AND MACHINE ACCESS.

Identify API keys, tokens, passwords, SSH keys, certificates, service accounts, rotation, workload identity, delivery, use, audit, and emergency access.

FROM CRYPTO OBJECT TO MISSION RISK

Classify data lifetime and HNLD priority

Cryptographic posture becomes a priority only after it is linked to data value, trust function, exposure, adversary interest, mission consequence, migration lead time, and evidence confidence.

DECISION MODEL - NO UNIVERSAL SCORE

PRIORITY = IMPACT x URGENCY x EXPOSURE x FRICTION, moderated by evidence confidence. Weights and thresholds are engagement-specific and must be approved before results are known.

01

DATA / TRUST LIFETIME

How long must confidentiality, integrity, authenticity, provenance, or non-repudiation remain reliable?

02

COLLECTION EXPOSURE

Can an adversary obtain ciphertext, signed artifacts, software, telemetry, archives, or trust material now?

03

MISSION CONSEQUENCE

What fails if the protected decision, identity, command, update, sensor, or data flow cannot be trusted?

04

ADVERSARY INTEREST

Who benefits from collection, decryption, forgery, downgrade, impersonation, or delayed exploitation?

05

MIGRATION LEAD TIME

How long do discovery, procurement, suppliers, integration, certification, fielding, and retirement actually take?

06

EVIDENCE CONFIDENCE

What is observed, inferred, modeled, or unverified - and what would disprove the current priority?

OUTPUT

A ranked, evidence-linked decision record: what must move first, why, who owns it, what remains uncertain, and what validation or migration action closes the gap.

SCORE THE DECISION, NOT THE DRAMA

A defensible quantum-risk scoring model

A score orders work and exposes assumptions. It is not a measured probability that a quantum computer breaks a system on a specific date.

PRIORITY = IMPACT x URGENCY x EXPOSURE x FRICTION

IMPACT

Mission consequence, trust blast radius, and loss of command, confidentiality, integrity, or availability.

URGENCY

Data lifetime, policy deadline, adversary value, and the time remaining to close the path.

EXPOSURE

Collection opportunity, reachable path, observed condition, and confidence in the evidence.

FRICTION

Lead time, supplier depth, integration, testing, certification, accreditation, and operational disruption.

Publish factors, weights, normalization, confidence, sensitivity, raw evidence, and a correction path.

The result should be challengeable by the mission owner and reproducible from the evidence set.

TRUST THE FINDING

Evidence confidence and provenance

Decision-makers need to distinguish what was directly observed, what was inferred, what an owner declared, and what was reproduced under controlled validation.

DECISION RULE

Every material finding should carry a provenance record: source, time, scope, method, raw artifact, tool and version, transformation, analyst judgment, confidence, corroboration, owner response, and validation status.

DIRECTLY OBSERVED

runtime or authoritative metadata

REPRODUCED

controlled test or replay

CORRELATED

multiple independent evidence sources

DECLARED

owner or supplier statement

INFERRED

analytical conclusion requiring review

WHAT IT IS - AND IS NOT

QScout: explicit product boundary

QScout is Qtonic Quantum's risk and vulnerability intelligence layer for cryptographic discovery, evidence, prioritization, and executive decision support.

MISSION TAKEAWAY

QScout identifies cryptography, evidence, mission urgency, and sequence. It complements PKI, CLM, HSM/KMS, remediation, QStrike, and Qsolve.

QScout Surface.

An agentless external assessment of observable domains, certificates, TLS, services, attack-surface indicators, and public evidence. It requires no customer-installed software or internal credential by default.

Deeper scoped evidence.

Gold engagements may add approved repository access, customer exports, platform APIs, scoped credentials, documentation, interviews, or a customer-run collector when the statement of work authorizes them.

What it produces.

Normalized findings, evidence references, quantum-vulnerable dependencies, risk factors, ownership questions, CBOM-oriented records, migration priorities, executive and technical reports, and work-ready actions.

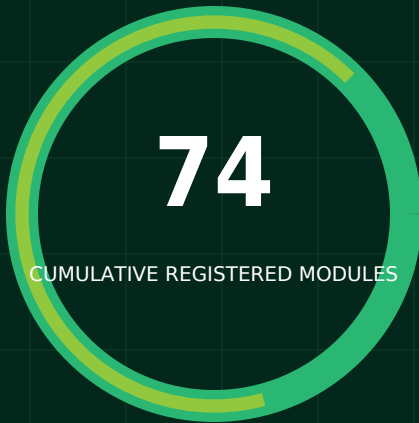
What it cannot prove alone.

Absence of internal or embedded cryptography, exploitability, production impact, classified mission context, supplier internals, secure implementation, or completed remediation without additional evidence and validation.

FIND | PRIORITIZE | ASSIGN

QScout Gold: governed breadth, defined

Gold is the deep QScout assessment tier for authorized, multi-source evidence fusion, trust-path mapping, owner assignment, and executive closeout.



WHAT COUNTS AS A MODULE?

A module is a discrete, registered QScout capability that performs a defined discovery, analysis, validation, evidence, or reporting function and produces a governed result or explicit disposition.

CUMULATIVE TIER CATALOG

SURFACE	SILVER	GOLD
46	57	74

DISCOVER

Public, application, dependency, cloud, platform, certificate, and exposure evidence.

PROVE

Provenance, confidence, evidence manifests, and operator review.

PRIORITIZE

HNDL, data lifetime, trust blast radius, mission consequence, and friction.

SCOPE AND FAIL-CLOSED RULE

Not every module runs against every target. Applicable modules execute according to authorized scope, access, asset class, dependencies, and reachability. Inapplicable, unavailable, or blocked modules do not silently inflate coverage; they fail closed or are explicitly dispositioned in the evidence record.

Buyer test: ask for the module registry, applicability rules, executed-module list, skipped-module reasons, release identity, and evidence manifest.

ALWAYS-ON CRYPTOGRAPHIC-RISK INTELLIGENCE

QScout Pulse: 24/7/365 continuity

Management-confirmed operating state. Pulse continuously monitors the approved external surface and configured evidence sources across QScout Surface, Silver, and Gold.

OPERATING STATE

24 / 7 / 365

CONTINUOUS EXTERNAL MONITORING

1 BASELINE

Start from approved scope, evidence thresholds, ownership, and an accepted baseline.

2 MONITOR

Continuously observe authorized TLS, certificate, public-surface, HNDL, and configured evidence signals.

3 EXPLAIN DRIFT

State what changed, why it matters, what is observed, what is inferred, and what remains unknown.

4 ESCALATE

Route material change into QStrike, QSolve, owner review, remediation, or a documented exception.

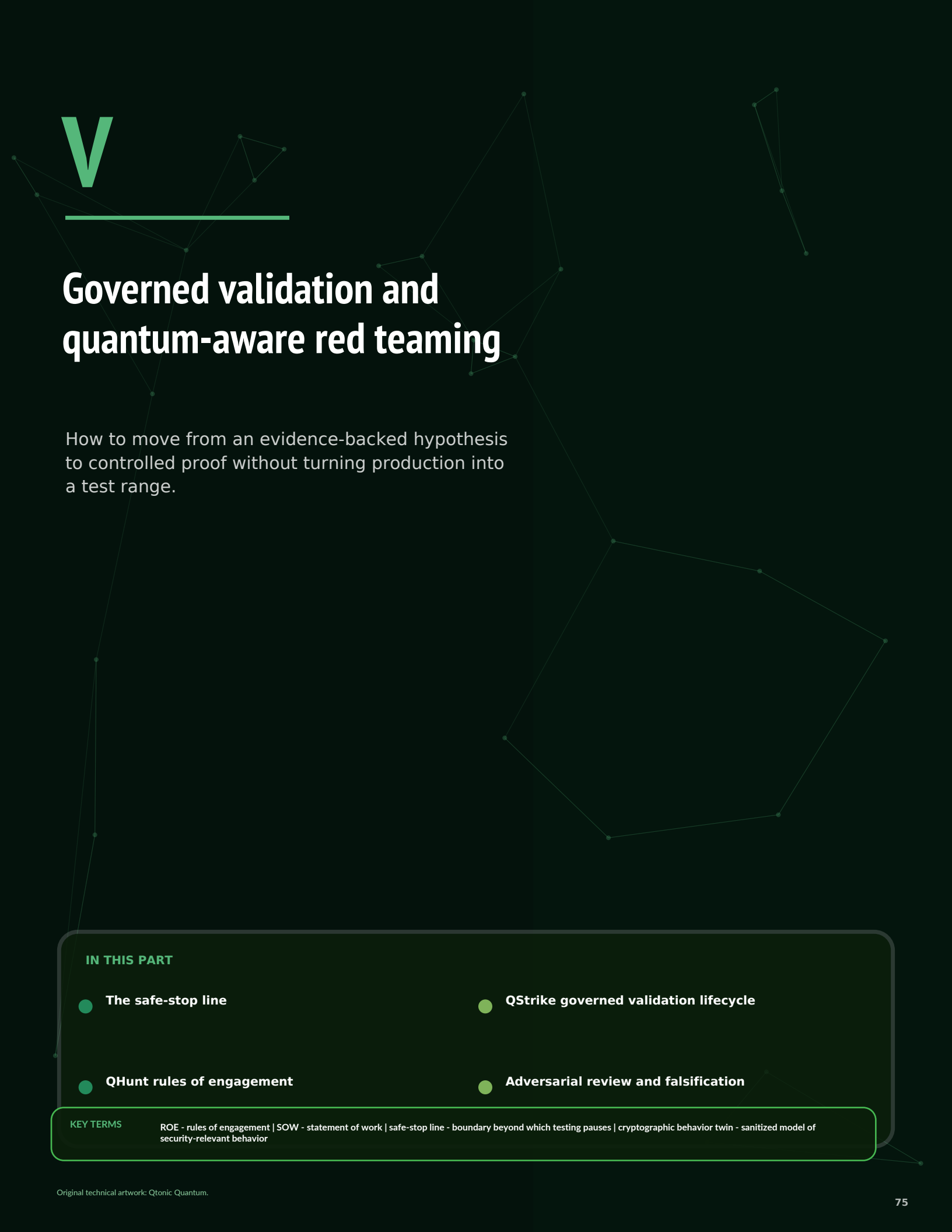
SUPPORTED OPERATING MODEL

- 24/7/365 monitoring of the authorized external surface
- Event-driven updates and posture-history comparison
- Evidence-backed cryptographic and certificate drift
- Leadership-ready posture and urgency summaries
- Escalation into QStrike validation or QSolve migration

CREDIBILITY BOUNDARY

- Not a SOC, endpoint detection, or incident-response platform
- No automatic access to private customer systems without authorization
- No universal completeness beyond approved scope and evidence sources
- No unconditional 100% uptime SLA is represented by the 24/7/365 operating cadence
- Does not replace PKI, CLM, HSM/KMS, vulnerability management, QStrike, or QSolve

Buyer test: define the observed surface, evidence sources, alert path, retention, ownership, escalation, and service-level terms in the engagement.



V

Governed validation and quantum-aware red teaming

How to move from an evidence-backed hypothesis to controlled proof without turning production into a test range.

IN THIS PART

- The safe-stop line
- QStrike governed validation lifecycle
- QHunt rules of engagement
- Adversarial review and falsification

KEY TERMS

ROE - rules of engagement | SOW - statement of work | safe-stop line - boundary beyond which testing pauses | cryptographic behavior twin - sanitized model of security-relevant behavior

PROOF WITHOUT MISSION HARM

The safe-stop line and test authority

A test is credible only when the boundary is as explicit as the hypothesis. QStrike and QHunt stop at the least-invasive action that proves or disproves the approved claim.

BEFORE ACTIVITY

01

AUTHORITY

Named sponsor, target, purpose, governing lane.

02

SCOPE

Systems, identities, data, suppliers, environments.

03

METHOD

Allowed tests, credentials, fixtures, and observers.

04

RECOVERY

Rollback, halt authority, incident path, and evidence release.

THE STOP LINE

01

NO UNCONTROLLED WRITES

No persistence, privilege extension, or state change beyond approved proof.

02

NO MISSION DISRUPTION

No uncontrolled loss of availability, safety, command, or protected function.

03

NO PROTECTED-DATA EXFILTRATION

Use synthetic or minimized fixtures; retain only authorized evidence.

04

NO CLAIM BEYOND THE EVIDENCE

State scope, confidence, alternative explanations, and avoided action.

RELEASE EVIDENCE, NOT THEATRICALS

The closeout records authorization, hypothesis, safe method, evidence hash, timestamp, proof level, stop line, avoided action, limitations, alternative explanations, mission consequence, remediation gate, and retest path.

NO AUTHORITY = NO ACTIVITY

REPRODUCE SECURITY-RELEVANT BEHAVIOR

Build a cryptographic behavior twin before testing the mission system

A digital twin for quantum-security validation is not a copy of all production data. It is a versioned model of the assets, trust, protocol, identity, data-flow, configuration, and failure behavior needed to test the approved hypothesis.

DECISION RULE

The twin must be certified for scope coverage, fidelity, traceability, secret exclusion, freshness, replay conformance, graph integrity, and deterministic rebuild before its results are treated as evidence about a mission path.

01**EVIDENCE PLANE
— Approved
source state.**

QScout Gold evidence, architecture, inventories, certificates, trust stores, policies, protocol captures, code and build metadata, configurations, telemetry, device exports, supplier evidence, and owner declarations.

02**MODEL PLANE —
Canonical asset,
identity, trust.**

Normalize provider-specific evidence into typed objects and relationships with provenance, confidence, version, ownership, mission context, data lifetime, and explicit unknowns.

03**SANITIZATION PLANE
— Synthetic secrets
and minimized
content.**

Exclude live private keys, passwords, bearer tokens, unnecessary payloads, and protected customer content. Replace operational secrets and records with controlled fixtures that preserve test behavior.

04**REPLAY PLANE —
Protocols, workflows,
failures, and attack
paths.**

Reproduce negotiation, authentication, signing, validation, update, recovery, revocation, fallback, key-compromise, malformed-input, overload, latency, and loss-of-service conditions relevant to the hypothesis.

05**ASSURANCE PLANE
— Acceptance gates
and signed manifest.**

Measure completeness, fidelity, traceability, reproducibility, isolation, control coverage, evidence integrity, rebuild, test limits, and differences from production; sign the release manifest and preserve it with results.

A REVIEWABLE CHAIN OF REASONING

From hypothesis to attack-path evidence

A useful validation result shows exactly why an observed cryptographic condition can or cannot become a mission-relevant failure.

DECISION RULE

Do not jump from 'legacy algorithm present' to 'mission compromised.' Connect preconditions, reachable path, observed behavior, affected trust or data, consequence, scope, confidence, alternatives, and reproducible evidence.

01

HYPOTHESIS

State the exact claim, protected function, adversary capability, prerequisite access, affected version, and expected observable result.

02

TEST DESIGN

Choose the least-invasive valid method, environment, fixtures, measurements, control case, stop conditions, and evidence to retain.

03

OBSERVATION

Capture configuration, inputs, outputs, logs, traces, timing, errors, state changes, identities, signatures, hashes, and environmental conditions.

04

ADJUDICATION

Challenge causation, test alternatives, reproduce, bound scope and consequence, assign confidence, map remediation, and define the retest gate.

05

EVIDENCE UNIT

A controlled record identifies the target, authorization, hypothesis, method, environment, versions, inputs, outputs, timestamps, hashes, analysts, limitations, and review disposition.

06

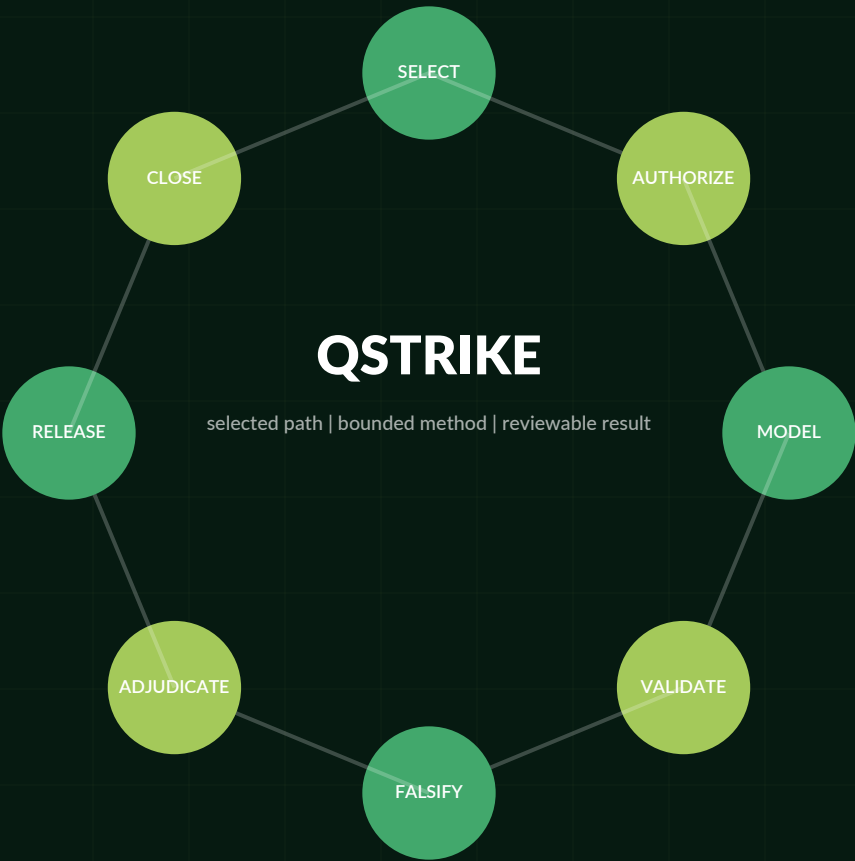
MISSION UNIT

The owner sees the affected mission thread, security effect, duration, detectability, recovery path, dependencies, and operational workaround.

SELECT | PROVE | FALSIFY | CLOSE

QStrike governed validation lifecycle

QStrike is the controlled proof layer for selected findings that require more than discovery evidence.



The test ends at the authorized stop line. The result shows the hypothesis, method, evidence, reproducibility, alternative explanations, avoided action, and remediation acceptance criteria.

WHAT CAN BE PROVEN SAFELY

QStrike validation test classes

Select a test class because it closes a mission decision, not because it is visually impressive.

DECISION RULE

Each test identifies the protected function, authoritative requirement, threat model, preconditions, least-invasive method, evidence, expected result, mission consequence, stop condition, remediation, and retest criterion.

01

CONFIGURATION

Cryptographic settings, policy, downgrade behavior, negotiation, and provider state.

02

TRUST PATH

Roots, signatures, identities, gateways, certificates, and authorization chains.

03

REPLAY

Protocol and artifact behavior under controlled, reproducible inputs.

04

PERFORMANCE

Latency, size, compute, memory, bandwidth, and constrained-device effects.

05

FAILURE

Invalid input, error handling, fallback, randomness, side channels, and unsafe state.

06

CLOSURE

Prove remediation, residual risk, acceptance authority, and retest criteria.

LAUNCHING AT TECHNET AUGUSTA 2026

Q Hunt

Qtonic Quantum's most powerful quantum-aware cyber risk and vulnerability red-team intelligence capability for warfighters.

Non-destructive by default. Any active, destructive, or disruptive method requires explicit written authorization, isolation, stop conditions, recoverability, governance, and mission-safety controls.

● MISSION-THREAD INTELLIGENCE

Combine cryptography, identity, software supply chain, trust, data lifetime, supplier access, and operational constraints.

● ADVERSARY EMULATION

Challenge the assumptions that could create false confidence across C2, tactical edge, SATCOM, OT, software factories, and the DIB.

● CREDENTIALLED OPERATIONS

Authenticated traversal, controlled writes, payload-safe exploitation, session interaction, and multi-stage penetration only within the rules of engagement.

● EVIDENCE TO ACTION

Replayable proof, safe-stop receipts, owner decisions, remediation handoff, and a reviewable evidence package.

This superlative is scoped only to Qtonic Quantum's product portfolio; no independent universal market-leadership certification is represented.

FEDERAL AND MILITARY USE CASES

Where Q Hunt can create decision value

The strongest Q Hunt engagements are framed around a mission decision, a contested assumption, and an evidence gap - not a generic request to 'hack the network.'

MISSION TAKEAWAY

Select a small number of consequential mission threads, define the decision and authorization, build the evidence baseline, then use a red team to attack the assumptions that could create false confidence.

- **C2 and tactical edge.**
Challenge trust establishment, identity, degraded operations, intermittent links, algorithm negotiation, downgrade, credential compromise, update, latency, recovery, and mixed coalition states.
- **Software factory and update chain.**
Challenge source dependency, build identity, signing, manifests, artifact repositories, provenance, verification, deployment authorization, rollback, emergency release, and supplier compromise assumptions.
- **SATCOM and space ground systems.**
Challenge command and telemetry trust, gateway identity, provisioning, remote update, long-lived mission data, crosslinks, constrained terminals, jamming resilience, failover, and recovery evidence.
- **OT, facilities, and weapons support.**
Challenge vendor access, engineering workstations, signing, remote maintenance, serial and proprietary protocols, safety boundaries, spares, offline recovery, unsupported components, and life-extension decisions.

THE NON-NEGOTIABLE CONTROL SET

QHunt rules of engagement

A red-team plan is incomplete until authority, safety, evidence, and recovery are as explicit as the technical objective.

AUTHORITY

named sponsor, target, purpose

SCOPE

systems, identities, data, suppliers

METHOD

allowed tests and stop line

SAFETY

isolation, rollback, observers

EVIDENCE

custody, hashes, release rules

RECOVERY

halt, restore, incident path

NO AUTHORITY = NO ACTIVITY

TEST ASSUMPTIONS, NOT SCIENCE FICTION

Quantum-aware red-team scenario library

Use scenarios to reveal interacting trust, migration, operational, and supplier weaknesses while keeping present and future adversary capabilities distinct.

DECISION RULE

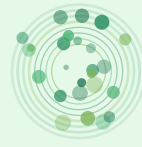
A scenario is valuable when it exposes a decision gap that can be observed and closed now. It is not valuable merely because it contains the word quantum.

**HNDL PATH**

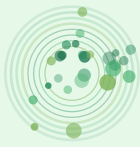
collection to long-lived data

**SIGNING FAILURE**

update and artifact trust

**DOWNGRADE**

fallback to vulnerable protocol

**SUPPLIER GAP**

migration blocked by dependency

**EDGE FAILURE**

latency, size, power, disconnect

**COALITION BREAK**

interoperability and releasability

MAKE THE RESULT REVIEWABLE AND REUSABLE

The validation evidence package

A demonstration without a disciplined evidence package is difficult to reproduce, remediate, audit, authorize, or defend during acquisition and operational review.

DECISION RULE

Release a compact signed decision package and preserve a controlled technical record. The package must make clear what is fact, inference, assumption, customer declaration, analyst judgment, limitation, and future target state.

01 SCOPE & AUTHORITY

reviewable | reproducible | attributable

02 HYPOTHESIS

reviewable | reproducible | attributable

03 EVIDENCE MANIFEST

reviewable | reproducible | attributable

04 REPLAY / RECEIPTS

reviewable | reproducible | attributable

05 FALSIFICATION

reviewable | reproducible | attributable

06 MISSION IMPACT

reviewable | reproducible | attributable

07 REMEDIATION GATE

reviewable | reproducible | attributable

08 SIGNED CLOSEOUT

reviewable | reproducible | attributable

THE RED TEAM MUST ALSO RED-TEAM ITS OWN RESULT

Adversarial review and falsification

The most credible program attempts to disprove its preferred conclusion before publishing a finding or declaring a migration successful.

DECISION RULE

A high-severity finding should survive independent challenge. A closure decision should survive an attempt to reproduce the original path, create an equivalent path, trigger fallback, exploit an exception, or invalidate the evidence.

PREFERRED EXPLANATION

What the finding appears to show

?

ALTERNATIVE

What else could produce the evidence

≠

DISPROVE PATH

What test would falsify the conclusion

×

ADJUDICATION

Human review and confidence statement

✓

VI

Migration and program execution

Sequence dependencies, field approved patterns, retire vulnerable paths, and prove sustained readiness.

IN THIS PART

- Transition architecture patterns
- Migration waves ordered by trust
- 1,000-day target operating plan
- QSolve governance and acceptance

KEY TERMS

RFI - request for information | RACI - responsible, accountable, consulted, informed | CBOM - cryptographic bill of materials | NSS - National Security System | DIB / CUI - Defense Industrial Base / Controlled Unclassified Information

THERE IS NO SINGLE MIGRATION MECHANISM

Transition architecture patterns

A portfolio will use multiple patterns according to mission, standards profile, platform support, data lifetime, trust role, performance, interoperability, supplier, accreditation, and replacement lead time.

DECISION RULE

Select a target pattern for each cryptographic dependency and record the exit condition. Hybrid modes and compensating controls can reduce transition risk, but they become permanent debt unless their purpose, security property, owner, test, and retirement date are explicit.

01 Direct standards-based replacement.

Replace vulnerable key establishment or signature with an approved PQC mechanism where the platform, profile, performance, validation, interoperability, and mission test are ready.

02 Hybrid key establishment or authentication.

Combine classical and PQC mechanisms so security can survive failure of one component when the construction and profile are approved. Test composition, negotiation, downgrade, size, latency, and lifecycle.

03 Cryptographic abstraction and service.

Move algorithm selection, policy, keys, certificates, signing, validation, rotation, telemetry, and upgrade behind governed APIs or platforms where architecture and assurance permit.

04 Gateway or overlay transition.

Use an approved boundary service to protect a path while endpoints lag. Record what it does and does not protect, trust concentration, visibility, availability, performance, key lifecycle, and retirement.

05 Re-protect or re-sign data and artifacts.

Decrypt and re-encrypt, wrap, re-sign, timestamp, re-issue, migrate trust, or preserve verifiable provenance for long-lived data, archives, software, firmware, identities, and records.

06 Replace, isolate, constrain, or retire.

For embedded, unsupported, safety-critical, proprietary, or uneconomic components, use replacement, segmentation, reduced data lifetime, one-way transfer, operational control, limited exposure, or retirement with approved residual risk.

DoW CAVEAT

PQC proxy solutions should be avoided in place of actual upgrades. Treat gateways and overlays only as approved, time-bounded transitions with a named owner, evidence, and retirement gate.

SEQUENCE THE DEPENDENCIES

Migration waves ordered by trust and mission consequence

The order of migration matters because roots, signers, identity, update paths, common infrastructure, and supplier capabilities enable or block downstream systems.

DECISION RULE

Begin enabling work early for long-lead platforms even when fielding comes later. A wave plan should combine technical dependency, mission consequence, data lifetime, supplier readiness, acquisition cycle, test capacity, and deprecation deadlines.

01

WAVE 0 — Governance, profiles, inventory, and test capacity.

Authority, component POCs, target profiles, schema, discovery, ownership, risk method, supplier clauses, lab and digital-twin capacity, workforce, budget, exception policy, evidence, and reporting cadence.

02

WAVE 1 — Roots, identity, signing, and common crypto.

Enterprise and mission PKI, trust anchors, code and firmware signing, KMS/HSM, secrets, directories, federation, time and timestamping, service identity, CI/CD, artifact trust, gateways, and platform crypto libraries.

03

WAVE 2 — Long-lived data and high-value mission threads.

Strategic intelligence, plans, designs, weapons and logistics data, C2 identity, SATCOM command trust, high-value applications, cloud data paths, mission partner exchange, and DIB/CUI dependencies.

04

WAVE 3 — Broad application, infrastructure, and supplier rollout.

Enterprise applications, APIs, service mesh, endpoints, network devices, remote access, messaging, databases, backups, observability, facility systems, suppliers, managed services, and routine acquisition refresh.

05

WAVE 4 — Tactical, embedded, OT, legacy.

Constrained edge, radios, sensors, unmanned systems, weapons support, OT, physical access, offline systems, spares, field service, unsupported products, exceptions, classical fallback removal, archival proof, and residual-risk acceptance.

WHY QTONIC QUANTUM

One evidence system across the decision lifecycle

Choose Qtonic Quantum when the buyer needs an independent decision layer spanning quantum-specific priority, continuous external intelligence, controlled validation, and vendor-neutral migration.

01

MISSION-SPECIFIC URGENCY

HNDL, data and trust lifetime, mission consequence, collection opportunity, replacement lead time, and evidence confidence.

02

GOVERNED EVIDENCE

CycloneDX 1.7 CBOM output, provenance, confidence, asset and trust relationships, owner/action mapping, and versioned closure.

03

PROOF WITHOUT UNCONTROLLED RISK

QStrike and OHunt use explicit authorization, digital twins, safe stops, bounded methods, falsification, and reviewable evidence.

04

REMEDiation NEUTRALITY

QSolve sequences approved technologies and providers without requiring one PKI, HSM, KMS, network, cloud, or certificate platform.

THE COMPLEMENTARY ECOSYSTEM

PKI and certificate-lifecycle platforms, HSM/KMS products, network crypto-agility solutions, cloud controls, primes, integrators, and implementation partners remain complementary. Qtonic Quantum supplies the evidence, quantum-specific priority, controlled proof, and accountable decision record that tells the buyer what must move first and why.

Best fit: decisions that must survive mission-owner, engineering, cyber, acquisition, legal, audit, and executive review. Selected references and engagement examples are available under NDA.

ACCEPTANCE GATES BY PHASE

The 1,000-day target operating plan

A bounded planning target, not a universal guarantee. Each phase ends with evidence an executive, authorizing official, acquisition lead, operator, and auditor can examine.



Completion means the approved PQC profile operates across the complete protected path and lifecycle, vulnerable fallback is removed or explicitly accepted, and mission performance, recovery, and evidence are proven.

THE CUSTOMER NAMED THE REQUIREMENT

ACDI: automated cryptography discovery and inventory

DoW LOE 2 explicitly calls for investigation of ACDI tools. OMB M-26-15 says manual approaches are often insufficient and directs agencies toward automation for discovery, enforcement, compliance, and CBOM maintenance.

"automated cryptography discovery and inventory (ACDI) tools"

DoW PQC Strategy, LOE 2

PROCUREMENT-READY CAPABILITY LANGUAGE

01

DISCOVER

Applications, code, dependencies, endpoints, PKI, cloud, protocols, KMS/HSM, firmware, and suppliers.

02

NORMALIZE

Algorithm, use, key size, certificate chain, protocol, owner, data lifetime, provenance, confidence, and freshness.

03

RECONCILE

Change after releases, renewal, architecture, supplier, incident, waiver, or policy events.

04

EXPORT

Machine-readable CBOM, evidence manifest, exception record, leadership dashboard, and migration handoff.

05

GOVERN

Authorization, scope, operator review, evidence thresholds, release rules, and correction path.

QScout is the governed discovery and evidence layer; QStrike validates selected hypotheses; QSolve sequences migration.

PROCUREMENT GUARDRAIL

Do not buy the wrong quantum answer

The DoW strategy names approaches that are not considered fully quantum resistant, establishes a 2030 phase-out for specified cases, and directs Components not to test, pilot, use, or procure specified commercial solutions for quantum resistance.

01

QKD AND QUANTUM NETWORKING

Do not use as the security mechanism for confidentiality, data or entity authentication, key distribution, or non-local randomness generation.

02

NON-LOCAL QUANTUM RANDOMNESS

The strategy does not accept it as a quantum-resistance security solution.

03

LONGER RSA / ECC KEYS

Larger parameters on CRQC-vulnerable public-key algorithms are not fully quantum resistant.

04

SYMMETRIC KEY ESTABLISHMENT / AGREEMENT / DISTRIBUTION

For non-High Assurance quantum resistance, these approaches are not considered fully quantum resistant.

05

PSK-BASED QUANTUM RESISTANCE

Not accepted for non-High Assurance use when not provisioned through NSA KMI for High Assurance devices.

06

PQC PROXIES IN PLACE OF UPGRADES

The strategy says proxy solutions should be avoided in favor of actual upgrades to PQC.

ACTIONABLE SWEEP

Identify these patterns across procurement, pilots, architecture, supplier claims, and deployed systems. Route each to approved replacement, explicit exception, time-bounded transition, or retirement.

Exception note: legacy symmetric-key distribution in use before 2010 receives a narrow strategy exception; asymmetric PQC migration should still be investigated.

INSIDE A QSCOUT EVIDENCE PACKAGE

What decision-grade output looks like

Sanitized illustrative excerpt - no customer data. The actual package is governed by approved scope, evidence sources, operator review, and release rules.

EXAMPLE MISSION THREAD			
Tactical C2 identity, software trust, and long-lived mission data			
OBJECT	OBSERVED CRYPTOGRAPHY	EVIDENCE	DECISION
Mission gateway	RSA-2048 TLS certificate	CT log, handshake, chain	HNDL priority; validate renewal path
Firmware signer	ECDSA P-256	Build manifest, signer metadata	QStrike hypothesis; QSolve migration wave
Identity root	ECC P-256 trust anchor	Certificate path, policy, owner	Owner and exception decision
Supplier API	TLS 1.2 / ECDHE	Endpoint evidence, dependency map	Contract evidence request and sequence

DELIVERABLE ARTIFACTS

- CycloneDX 1.7 CBOM
- Evidence manifest
- Asset and trust graph
- HNDL and data-lifetime priority
- Owner and action map
- Delta and closure record

VERIFICATION CHAIN



A signature can protect artifact integrity. It does not by itself prove discovery completeness, classification correctness, or customer acceptance.

FROM PRIORITY TO ACCEPTED CHANGE

Qsolve: vendor-neutral migration governance

Qsolve turns prioritized findings into architecture, policy, supplier decisions, migration waves, implementation plans, and acceptance evidence.

OPERATING PRINCIPLE

Sequence the customer decision and acceptance record without locking remediation to one technology provider.

01**POLICY**

Approved profiles and exception process.

02**ARCHITECTURE**

Target patterns and dependencies.

03**SUPPLIER**

Request for information (RFI), evidence, contract obligations, and remedies.

04**WAVES**

Sequence by trust path, mission, dependency, and readiness.

05**ACCEPTANCE**

Tests, owner signoff, residual risk, and evidence release.

06**SUSTAIN**

Metrics, change review, recertification, exception aging, and operational transfer. Customer-selected public key infrastructure, certificate lifecycle management, hardware security module, key-management, network, cloud, library, hardware, or integration partners remain vendor-neutral.

ENTERPRISE DELIVERY AND DILIGENCE

Security and delivery posture

Qtonic Quantum's public posture is defined by Azure-aligned delivery, explicit scope boundaries, and a refusal to convert inherited provider controls into unsupported company-held certifications.

01

AZURE-HOSTED DELIVERY

Delivery is aligned to applicable Microsoft Azure inherited controls. The exact architecture, tenant, region, evidence flow, and responsibility matrix are defined for the engagement.

02

CONTROL-INHERITANCE BOUNDARY

Inherited Azure controls do not make Qtonic Quantum FedRAMP Authorized, CMMC certified, SOC 2 certified, or ISO 27001 certified. No such company-held status is claimed here.

03

DATA-HANDLING TERMS

Data residency, approved evidence sources, access, retention, deletion, release, and any customer-hosted components are documented in the statement of work or Azure Marketplace private offer.

04

AUTHORIZATION AND ACCESS

No private-system access, credentials, active method, or persistent collection is assumed. Scope, methods, credentials, stop conditions, and evidence release require explicit authorization.

05

BUYING ROUTES

Purchase through Microsoft Azure Marketplace or through a direct agreement with Qtonic Quantum. No additional public contract vehicle is claimed here.

06

PAST PERFORMANCE

Selected references and engagement examples are available under NDA. This publication does not substitute an illustrative sample for verified customer evidence.

No public price is published. Scope, commercial terms, data-handling requirements, and service levels are provided through an Azure Marketplace private offer or a direct proposal.

COMMAND JUDGMENT. OPERATOR ACCOUNTABILITY.

Leadership accountable to the mission

Mission standards, enterprise and cyber execution, allied readiness, doctrine, and national policy - with specialist capacity scoped only when an engagement requires it.

 GOVERNS Mark E. Weatherington Chairman, Defense Innovation Council Mission-assurance standards for continuous post-quantum readiness.	 OPERATES / ADVISES Peter Renner Vice Chairman, Enterprise Technology Enterprise architecture, cloud transformation, and buyer execution.	 OPERATES / ADVISES Eliot Jung Vice Chairman, Cybersecurity Cyber operations, enterprise security, and accountable decisions.
 GOVERNS Roger L. Cloutier Jr. Founding Chair, Allied Defense Council Coalition-readiness standards for allied cryptographic transition.	 OPERATES / ADVISES Milford H. Beagle Jr. Senior Managing Director, Doctrine and Readiness Army force-development and training rigor applied to private-sector mission readiness.	 OPERATES / ADVISES Dr. David Mussington Former Executive Assistant Director for Infrastructure Security, CISA Critical-infrastructure security and national cyber-policy perspective.

These are Qtonic Quantum private-sector leadership and advisory responsibilities. Former military ranks and public roles are omitted from the commercial presentation except where needed to identify a prior public position. No government endorsement, procurement authority, current official role, or use of official position is represented.

HOW TO ENGAGE QTONIC QUANTUM

Turn one mission thread into a buying path.

Bring one consequential mission thread and one contested trust

01

QSCOUT SURFACE

A bounded, authorized external assessment for a defined domain or public surface. Delivered through Azure Marketplace or direct agreement.

02

30-DAY MISSION DECISION

QScout evidence, one selected QStrike or QHunt hypothesis, and a QSolve decision roadmap. Scope-specific Azure private offer or direct proposal.

03

ENTERPRISE TRANSITION

Multi-system discovery, validation, migration governance, acceptance, and sustainment under a custom statement of work.

FEDERAL PROCUREMENT PROFILE

SAM UEI

FRYFAD3GW5W5

CAGE

14E99

BUSINESS

Small Business

NAICS

541512 / 541519

MARKETPLACE

Microsoft Azure Marketplace

COMMERCIAL TERMS

No public price is published. Pricing and service levels are scoped through an Azure private offer or direct proposal. Selected references and engagement examples are available under NDA.

FEDERAL AND MISSION CONTACT

J. Nathaniel Ader

Co-Founder & Chief Innovation Officer

jna@qtonicquantum.com | 305-268-2626

qtonicquantum.com/contact | +1 (866) 4-QTONIC



SCAN TO START

PRIMARY AND OFFICIAL SOURCES

Evidence register

External sources control policy and standards claims. Qtonic Quantum sources control only Qtonic Quantum product boundaries and remain vendor-authored. Click any entry.

D01	DoW Post Quantum Cryptography Strategy dowcio.war.gov	N05	NSA Embracing a Zero Trust Security Model media.defense.gov	C02	CISA Post-Quantum Considerations for OT cisa.gov	A02	TechNet Augusta official FAQ, venue, theme events.afcea.org
D02	DoW CIO: Preparing for Migration to PQC dowcio.war.gov	S01	NIST FIPS 203 - ML-KEM csrc.nist.gov	C03	CISA product categories using PQC standards cisa.gov	Q01	Qtonic Quantum QScout qtonicquantum.com
D03	Department of Defense Zero Trust Strategy dowcio.war.gov	S02	NIST FIPS 204 - ML-DSA csrc.nist.gov	W01	Executive Order 14412 - Federal Register federalregister.gov	Q02	QScout methodology and product boundary qtonicquantum.com
D04	Zero Trust Capability Execution Roadmap v1.1 dowcio.war.gov	S03	NIST FIPS 205 - SLH-DSA csrc.nist.gov	W02	OMB M-26-15 - PQC migration execution whitehouse.gov	Q03	Qtonic Quantum Trust Center qtonicquantum.com
D05	U.S. Army Unified Network Plan 2.0 api.army.mil	S04	NIST SP 800-227 - KEM recommendations csrc.nist.gov	W03	NSM-10 - Quantum leadership and risk govinfo.gov	Q04	Qtonic Quantum QStrike qtonicquantum.com
D06	Army FY2026 tactical-network budget material asafm.army.mil	S05	NIST IR 8547 initial public draft nvlpubs.nist.gov	W04	OMB M-23-02 - Migrating to PQC whitehouse.gov	Q05	QScout market and evidence boundary qtonicquantum.com
D07	Cybersecurity guidance for LEO SATCOM media.defense.gov	S06	NIST CSWP 39upd1 - Crypto agility csrc.nist.gov	W05	NSPM-12 - NSS cybersecurity governance whitehouse.gov	Q06	Q Hunt TechNet Augusta launch and briefing qtonicquantum.com
N01	NSA Post-Quantum Cybersecurity Resources nsa.gov	S07	NIST NCCoE Migration to PQC project nccoe.nist.gov	G01	GAO-26-107759 - Updating the National Strategy gao.gov	Q07	Qtonic Quantum QSolve qtonicquantum.com
N02	CNSA 2.0 and Quantum Computing FAQ v2.1 media.defense.gov	S08	NIST SP 1800-38B preliminary draft nccoe.nist.gov	G02	GAO-25-107703 - Quantum Threat Mitigation Strategy gao.gov	Q08	Qtonic Quantum leadership qtonicquantum.com
N03	CNSS Policy 15, March 2025 nsa.gov	S09	NIST SP 800-208 - Stateful hash signatures csrc.nist.gov	G03	GAO-25-108590 - Cyber Threat Mitigation Testimony gao.gov	Q09	QScout Pulse 24/7/365 launch qtonicquantum.com
N04	NSA Zero Trust Implementation Guideline Primer media.defense.gov	C01	CISA/NSA/NIST Quantum-Readiness guide cisa.gov	A01	TechNet Augusta 2026 official conference site events.afcea.org		

Authentic operational photography is public-domain U.S. military visual information sourced via DVIDS; each added image is used once and credited on its page. Leadership portraits identify approved private-sector roles. The appearance of U.S. Department of War (DoW) visual information does not imply or constitute DoW endorsement.

No depicted person, service, unit, AFCEA, or TechNet Augusta endorsement is implied.

SECURE THE MISSION. CONTROL THE TRANSITION.

Find with QScout. Sustain with QScout Pulse. Prove with QStrike and QHunt. Fix with QSolve.



QSCOUT

FIND



QSCOUT PULSE

SUSTAIN 24/7/365



QSTRIKE + QHUNT

PROVE



QSOLVE

FIX

**Bring one mission thread.
Leave with a decision path.**

Azure Marketplace or direct | References available under NDA



TECHNET AUGUSTA 2026

QHunt launches at TechNet Augusta 2026. QScout Pulse operates continuously, 24/7/365, across the approved external surface and configured evidence sources. Engagement methods remain governed by authorization, scope, and mission safety.

J. Nathaniel Ader | jna@qtonicquantum.com | 305-268-2626

qtonicquantum.com/contact | Independent vendor publication; no government or AFCEA endorsement implied.