QTONIC QUANTUM
POST QUANTUM READY

QUANTUM CYBERSECURITY FOR THE U.S. MILITARY

Mission assurance in a post-quantum world

108-PAGE EXECUTIVE FIELD GUIDE | MISSION-PROFILE EVIDENCE

TWO OUTCOMES. ONE MISSION.

2030

SUPPORT PQC
OR PHASE OUT

2031

USE PQC

DoW strategy targets,
unless otherwise noted.
Authority and scope: pp.27-35.

EVIDENCE INCLUDED

4 measured studies + bandwidth model
1 supplier-neutral acceptance sheet
Methods and hashes: pp.101-108

SEPTEMBER 9, 2026 EDITION

QSCOUT | QSCOUT GOLD PULSE | QSTRIKE | QSOLVE
QHUNT FOR THE WARFIGHTER | MISSION AND OT ASSESSMENT

MISSION-PROFILE RESEARCH EDITION

EVIDENCE BEFORE ASSERTION

What this edition establishes

Research cutoff: September 9, 2026. Facts, estimates, analysis and company statements have different evidentiary weight.

01 EXTERNAL REQUIREMENT

Official documents control scope, dates and profiles. Drafts, guidance and proposed rules are identified as such.

02 CURRENT RESEARCH

Resource estimates, experiments and vendor reports are distinguished. None is represented as a demonstrated break of military encryption.

03 COMPANY-PROVIDED FACT

Qtonic Quantum statements identify the service and delivery boundary. A company statement is not independent validation.

04 ENGAGEMENT EVIDENCE

Methods, access, acceptance and deliverables follow the agreed scope. Illustrations are not customer results.

05 NO ENDORSEMENT

Company team portraits are used with permission. Roles are private-sector responsibilities. No government, service, conference or depicted-person product endorsement is implied.

06 COMPANY-REPORTED STATE

Qtonic Quantum reports SAFE/29 with QShield v1.0 as built and operating. This edition records that company statement. It does not treat an engineering specification alone as proof of a particular release or deployment.

EDITION RECORD

September 9, 2026 revision. Eight research and procurement pages extend the field guide. Fresh ML-KEM-1024 / ML-DSA-87 measurements, six TLS configurations and a transport-budget model accompany the unchanged earlier evidence.

Fresh studies + budget: pp.105-107 | Acceptance: p.103 | Evidence files: pp.104,108. Company team portraits remain used with permission; no new portrait or operational-photo substitutions in this revision.

LETTER FROM THE CO-FOUNDER

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

EVIDENCE
OWNERSHIP
ACCEPTANCE

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 connects discovery to a mission decision. QScout finds and prioritizes cryptographic evidence. QScout Gold Pulse tracks change across the agreed external scope. QStrike validates selected hypotheses, and QSolve sequences migration with owners and acceptance criteria. QHunt, announced August 19, extends this work into authorized mission and operational-technology environments. The September evidence reinforces the practical task: protect long-lived data and the complete chain of trust, then verify the result.

J. Nathaniel Ader

Co-Founder and Chief Innovation Officer | Qtonic Quantum Corp

THE ENTIRE REPORT IN ONE PAGE

Executive command brief

The immediate decision is which mission dependencies must change, who owns them, and what evidence will establish readiness.

01 **2030 | SUPPORT OR PHASE OUT**

DoW strategy: support quantum-resistant cryptography or phase out affected systems by December 31, 2030. Read the applicable scope and exceptions.

02 **2031 | USE PQC**

DoW strategy: use quantum-resistant algorithms by December 31, 2031, unless otherwise noted. A capable endpoint alone does not complete a mission path.

WHAT CHANGED SINCE THE AUGUST BASELINE

G7 guidance connects migration to inventories and purchasing. New research changes modeled resource requirements. Current OT attacks reinforce the need to address present access weaknesses in parallel.

01 **NAME THE MISSION**

Choose long-lived data, a critical trust function and the accountable owner.

02 **MAP THE COMPLETE PATH**

Include roots, signers, identities, software, suppliers, gateways and fallback.

03 **BUY MEASURABLE EVIDENCE**

Require exact profiles, versions, validation status, mission tests and acceptance.

04 **START A BOUNDED ENGAGEMENT**

Use QScout evidence, scoped QStrike/QHunt work and a QSolve decision roadmap.

Reader path: new research pp.105-107 | policy pp.27-37 | mission map p.60 | acceptance p.103 | action p.98

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.

Sources: D01, D02, C01, S06

SEPTEMBER 2026 UPDATE

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

SEPTEMBER BRIEFING
Pages 11, 30-31, 34-35 and 46

Report at a glance

Navigate 108 pages in seconds. Acronyms and mission terms: pages 19-20.

MISSION-PROFILE RESEARCH + BUYER TOOLS

New studies + bandwidth pp.105-107 | Earlier studies pp.101-102

Acceptance p.103 | Embedded evidence and hashes pp.104,108

Sources: A01, A02

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

QHunt for the warfighter: scoped cryptographic exposure assessment for mission and OT environments. Connect the approved mission boundary to evidence, unknowns, an accountable owner and a remediation decision.

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

Company team portraits used with permission. Private-sector roles; no government or military-service endorsement implied.

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

Sources: Q01, Q02, Q04, Q06, Q07

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.

DAYS 0-5

AUTHORIZE

Mission owner, scope, systems, data, authority, prohibited actions, and evidence-release rules.

DAYS 6-12

DISCOVER

QScout evidence, cryptographic dependencies, CBOM output where approved, data lifetime, and initial priority.

DAYS 13-20

CHALLENGE

Select the highest-value hypothesis for QStrike or an authorized QHunt engagement.

DAYS 21-30

DECIDE

QSolve migration wave, owner, target pattern, acceptance gate, residual risk, and next investment decision.

The evidence package

01 Authorized scope manifest

02 Cryptographic inventory / CBOM

03 HNDL and mission priority

04 Validation hypothesis and stop line

05 Migration wave and accountable owner

06 Executive decision brief and acceptance criteria

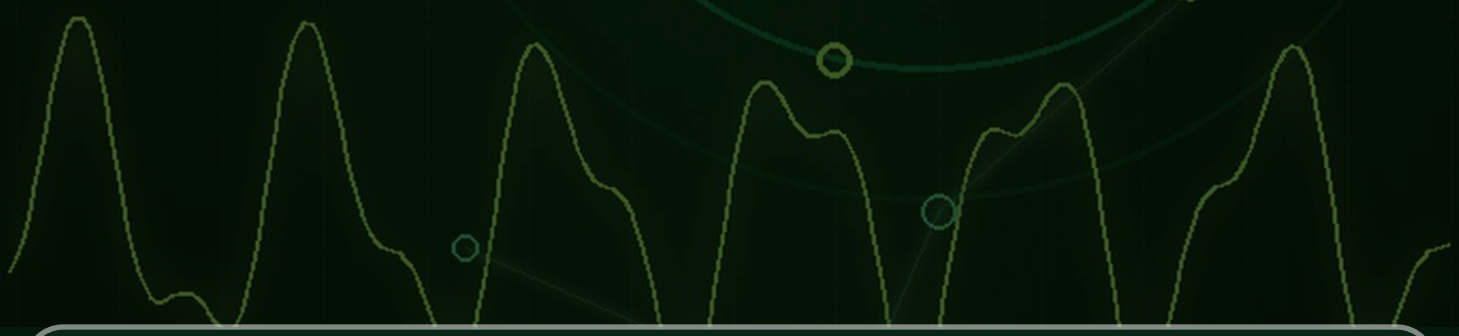
Bring one mission thread. Leave with a decision you can defend.

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

Sources: Q01, Q04, Q07

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
- Shor, Grover, and cryptographic effect
- Harvest-now-decrypt-later timing
- 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

Original technical artwork: Qtonic Quantum.

MISSION ASSURANCE

Protect the whole decision.

DATA

What must remain confidential?

IDENTITY

Who is trusted to act?

SOFTWARE

Which code may execute?

MISSION

What consequence must be prevented?

Cryptography supports each trust decision. Inventory the full dependency path.

ILLUSTRATIVE TRUST PATH

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.

SEPTEMBER RESEARCH BRIEFING

What the latest evidence changes

Two new results illustrate progress at different layers. Neither demonstrates a cryptographically relevant quantum computer.

19,397	25.7	MODELED
PHYSICAL QUBITS	DAYS PER ATTEMPT	NOT DEMONSTRATED

SEPT 4 PREPRINT / SEPT 8 ANNOUNCEMENT | IONQ

A full-stack estimate, with a specific target

The preprint models a proposed fault-tolerant trapped-ion system solving the secp256k1 elliptic-curve discrete logarithm problem. The reported time is for one attempt. It is not a live cryptographic break, a demonstrated production computer or a timetable for breaking military encryption. [R01]

READ THE ASSUMPTIONS

The paper reports about 40.7% end-to-end success from a rigorous algorithmic bound and 63.3% from a heuristic starting point. These estimates concern one curve and architecture; they do not transfer directly to AES-256, RSA-2048 or every ECC system.

AUG 27 | AI-ASSISTED QUANTUM MAINTENANCE

QuEra reports 695 successful laser relocks in 700 trials (99.3%). The final blind test ran a completed deterministic script without an AI agent in the loop. This is a vendor-reported subsystem result, not quantum gate fidelity or whole-machine availability. [R02]

MISSION IMPLICATION | QTONIC QUANTUM ANALYSIS

Track architecture, error correction, runtime and success assumptions together. Refresh risk scenarios when the evidence changes; continue migration without turning a resource estimate into a promised Q-Day.

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

Classical ECDHE forward secrecy protects past sessions from later long-term-key compromise. A future CRQC could recover recorded ephemeral exchanges; classical forward secrecy alone does not prevent quantum decryption.

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.

Sources: S05, G01

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.

Sources: D01, G01

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.

Sources: D01, S01, S02, S03, S05

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.

Sources: S01, S04

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.

Sources: S02, S03, S05

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.

Sources: N01, D01, S06

TIMING AND CONSEQUENCE

HNDL: the decision is about time

Protect information for as long as it must remain confidential. Compare that lifetime with collection exposure and the time needed to migrate.

CONFIDENTIALITY AND AUTHENTICITY ARE DIFFERENT

HNDL means harvesting ciphertext now for possible decryption later. Future signature forgery threatens identity and integrity; it does not require harvesting ciphertext.

ILLUSTRATIVE HIGH-PRIORITY WINDOW

Sensitive data remains valuable beyond the assumed capability window.

Scenario markers are illustrative, not a time scale or forecast.

LOWER-PRIORITY WINDOW

When data loses sensitivity before a plausible collection-and-decrypt window, retain it in the inventory but prioritize higher-consequence exposures. Long migration lead times can still require early work.

SIX QUESTIONS THAT SET PRIORITY

Data sensitivity lifetime	Collection opportunity	Adversary value
Migration lead time	Mission consequence	Evidence confidence

Qtonic Quantum analysis: use early, central and late capability scenarios. Reassess when lifetime, exposure, supplier readiness or migration evidence changes; do not present one forecast as certainty.

ACRONYMS AND MISSION TERMS

Acronyms and mission terms: A-M

Plain-English expansions for policy, systems and mission decisions. Additional terms continue on the next page.

ACDI
Automated cryptography discovery and inventory. Tool-assisted discovery of cryptographic use across approved systems and evidence sources.

AES
Advanced Encryption Standard. Symmetric encryption; CNSA 2.0 specifies AES-256 for applicable NSS use.

AFCEA
Armed Forces Communications and Electronics Association. Organizer of TechNet Augusta; reference does not imply endorsement.

AI / ML
Artificial intelligence / machine learning. Models, data, services, agents, and deployment pipelines with cryptographic dependencies.

API
Application programming interface. A software interface through which services, tools, and systems exchange requests and data.

ASN
Autonomous system number. An identifier used to map Internet routing ownership during authorized external discovery.

C2
Command and control. The people, systems, processes, and communications used to direct forces and missions.

CA
Certificate authority. An entity that issues and signs digital certificates within a public key infrastructure.

CBOM
Cryptographic bill of materials. A structured inventory of cryptographic objects, uses, dependencies, and provenance.

CI/CD
Continuous integration / continuous delivery. Software build, test, signing, and deployment pipelines.

CISA
Cybersecurity and Infrastructure Security Agency. Federal source for civilian and critical-infrastructure migration guidance.

CISO
Chief information security officer. Executive accountable for enterprise cybersecurity risk and operating controls.

CLM
Certificate lifecycle management. Issuance, renewal, rotation, revocation, inventory, and policy for certificates.

CMDB
Configuration management database. A system of record for assets and configuration relationships; one discovery evidence source.

CNSA 2.0
Commercial National Security Algorithm Suite 2.0. NSA algorithm suite and transition profile for National Security Systems.

CNSS
Committee on National Security Systems. Governance body for cybersecurity policy and baseline requirements for NSS.

CRQC
Cryptographically relevant quantum computer. A quantum system capable of defeating currently deployed public-key mechanisms at relevant scale.

CUI
Controlled Unclassified Information. Information requiring safeguarding or dissemination controls under federal policy.

DIB
Defense Industrial Base. Companies, suppliers, and partners supporting military systems, missions, and sustainment.

DoW
Department of War. Departmental authority used throughout the 2026 PQC Strategy and this field guide.

ECC
Elliptic-curve cryptography. Public-key mechanisms based on elliptic-curve discrete logarithms; quantum-vulnerable under Shor.

ECDH
Elliptic-curve Diffie-Hellman. Key-establishment method requiring migration analysis.

ECDSA
Elliptic Curve Digital Signature Algorithm. Classical signature method requiring migration analysis.

EO
Executive order. A presidential directive governing executive-branch action; EO 14412 accelerates federal PQC migration.

FCEB
Federal Civilian Executive Branch. Civilian federal agencies governed through the non-NSS federal policy lane.

FIPS
Federal Information Processing Standards. NIST standards used for federal cryptographic requirements and validation.

FPGA
Field-programmable gate array. Reconfigurable hardware that may embed cryptographic implementations and trust anchors.

GNSS
Global Navigation Satellite System. Positioning and timing services whose identity, integrity, and trust paths require protection.

HNDL
Harvest now, decrypt later. Capture protected data now for possible future decryption.

HSM
Hardware security module. Protected hardware for generating, storing, and using cryptographic keys.

HVA
High-value asset. Federal information system or data whose compromise could materially affect national or agency interests.

IPsec
Internet Protocol Security. A suite protecting IP communications; its key establishment and authentication require migration review.

ISR
Intelligence, surveillance, and reconnaissance. Mission data and systems whose provenance and long-term value drive risk.

KDF
Key-derivation function. Converts shared secrets or key material into cryptographic keys for defined uses.

KEM
Key-encapsulation mechanism. Establishes a shared secret; ML-KEM is the NIST standardized post-quantum KEM.

KMI
Key-management infrastructure. Systems and services governing cryptographic keys, especially in high-assurance environments.

KMS
Key-management system or service. Software or cloud capability for key generation, custody, policy, rotation, and use.

LMS
Leighton-Micali Signature. Stateful hash-based signature approved for CNSA 2.0 software and firmware signing.

LOE
Line of effort. A structured workstream in the DoW PQC Strategy.

ML-DSA
Module-Lattice-Based Digital Signature Algorithm. NIST FIPS 204 post-quantum signature standard.

ML-KEM
Module-Lattice-Based Key-Encapsulation Mechanism. NIST FIPS 203 post-quantum key-establishment standard.

MPE
Mission Partner Environment. Shared coalition or partner environment for exchanging mission information.

Use the full term on first use. Terminology describes functions, not product guarantees.

ACRONYMS AND MISSION TERMS

Acronyms and mission terms: M-Z

Plain-English definitions for policy, technology and mission decisions. Product names are not treated as acronyms.

MFA
Multi-factor authentication. Identity verification using two or more independent factors.

NIAP
National Information Assurance Partnership. Evaluates commercial IT security products against applicable profiles. See 30.

NIST
National Institute of Standards and Technology. Publishes FIPS, technical guidance and migration resources.

NSA
National Security Agency. National Manager for NSS and source of CNSA 2.0 guidance. See 27-30.

NSM-10
National Security Memorandum 10. National quantum leadership and migration risk-reduction policy.

NSPM-12
National Security Presidential Memorandum 12. Re-establishes NSS governance and CNSS. See 27.

NSS
National Security System. A system subject to statutory national-security criteria and the CNSS/NSA authority lane.

OCSP
Online Certificate Status Protocol. Provides certificate-revocation status to relying systems.

OID
Object identifier. Standardized identifier for algorithms, attributes, policies and protocols.

OMB
Office of Management and Budget. Leads civilian-federal migration execution and oversight. See 34.

OPSEC
Operations security. Protects sensitive indicators, plans, capabilities and activities.

OS
Operating system. Its libraries, trust stores, signing and update mechanisms need migration planning.

OT
Operational technology. Systems monitoring or controlling physical processes. See 46.

PEO
Program Executive Officer. Acquisition leader accountable for programs, portfolios and resources.

PIV / CAC
Personal Identity Verification / Common Access Card. Federal and defense identity credentials and their trust chains.

PKI
Public key infrastructure. Certificates, authorities, roots, policy and lifecycle operations. See 17, 40.

PLM / CAD
Product lifecycle management / computer-aided design. Engineering systems that hold sensitive technical data.

PQC
Post-quantum cryptography. Algorithms designed to resist known classical and quantum attacks.

PSK
Pre-shared key. A secret distributed in advance; not a general substitute for approved asymmetric PQC migration.

QKD
Quantum key distribution. A quantum communication mechanism subject to the DoW restrictions described on p.93.

RACI
Responsible, accountable, consulted, informed. A governance model with a named decision owner.

RFI
Request for information. Gathers supplier capabilities and market evidence; it is not a contract award.

RMF
Risk Management Framework. Federal process for selecting, assessing, authorizing and monitoring security controls.

RSA
Rivest-Shamir-Adleman. Public-key cryptography vulnerable to sufficiently capable quantum computation. See 12, 14.

SATCOM
Satellite communications. Includes space, ground, terminal, identity and command trust. See 44.

SBOM
Software bill of materials. An inventory of software components and dependencies; distinct from a CBOM.

SHA
Secure Hash Algorithm. Hash functions used in integrity, signatures and derivation. Profiles set required strengths.

SLH-DSA
Stateless Hash-Based Digital Signature Algorithm. FIPS 205; not in the current CNSA 2.0 suite. See 16, 31.

S/MIME
Secure / Multipurpose Internet Mail Extensions. Certificate-based email encryption and signatures.

SOC
Security operations center. Monitors and responds to security events. QScout Gold Pulse is not a SOC.

SSH
Secure Shell. Remote-access protocol with cryptographic dependencies that need inventory.

TLS
Transport Layer Security. Session protection depends on key establishment, authentication and negotiation.

VPN
Virtual private network. Tunnel protection requires analysis of algorithms, profiles, endpoints and gateways.

XMSS
eXtended Merkle Signature Scheme. Stateful hash-based signing included in CNSA 2.0 software/firmware guidance.

Zero Trust
Security model that continuously evaluates identity, device, policy and context. See 36.

Use the full term on first use. Terms describe the mission function, not a product guarantee.

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.

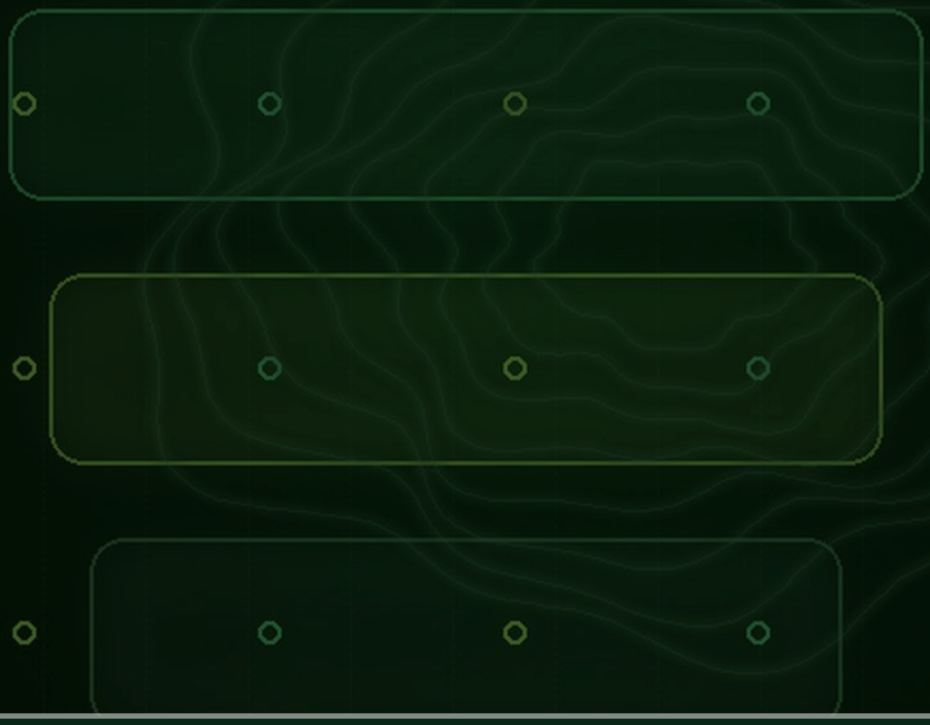
Program test: if a claim cannot name the authority, asset, trust path, evidence, consequence, owner, and next action, it is not yet decision-grade.

Sources: D01, N01, G01, G02

II

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
- CNSA 2.0 profile and milestones
- NIST FIPS 203, 204, and 205
- 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 | ACDI - automated cryptography discovery and inventory

Original technical artwork: Qtonic Quantum.

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

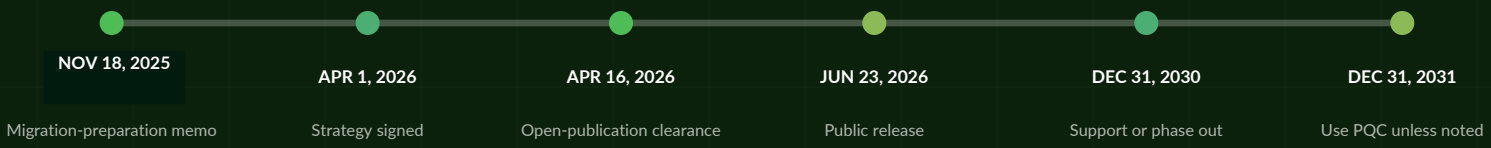
SUPPORT PQC OR PHASE OUT

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.

Sources: D01, D02

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.

Sources: D01

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.

Sources: D01, D02

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.

Sources: D01, S06

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.

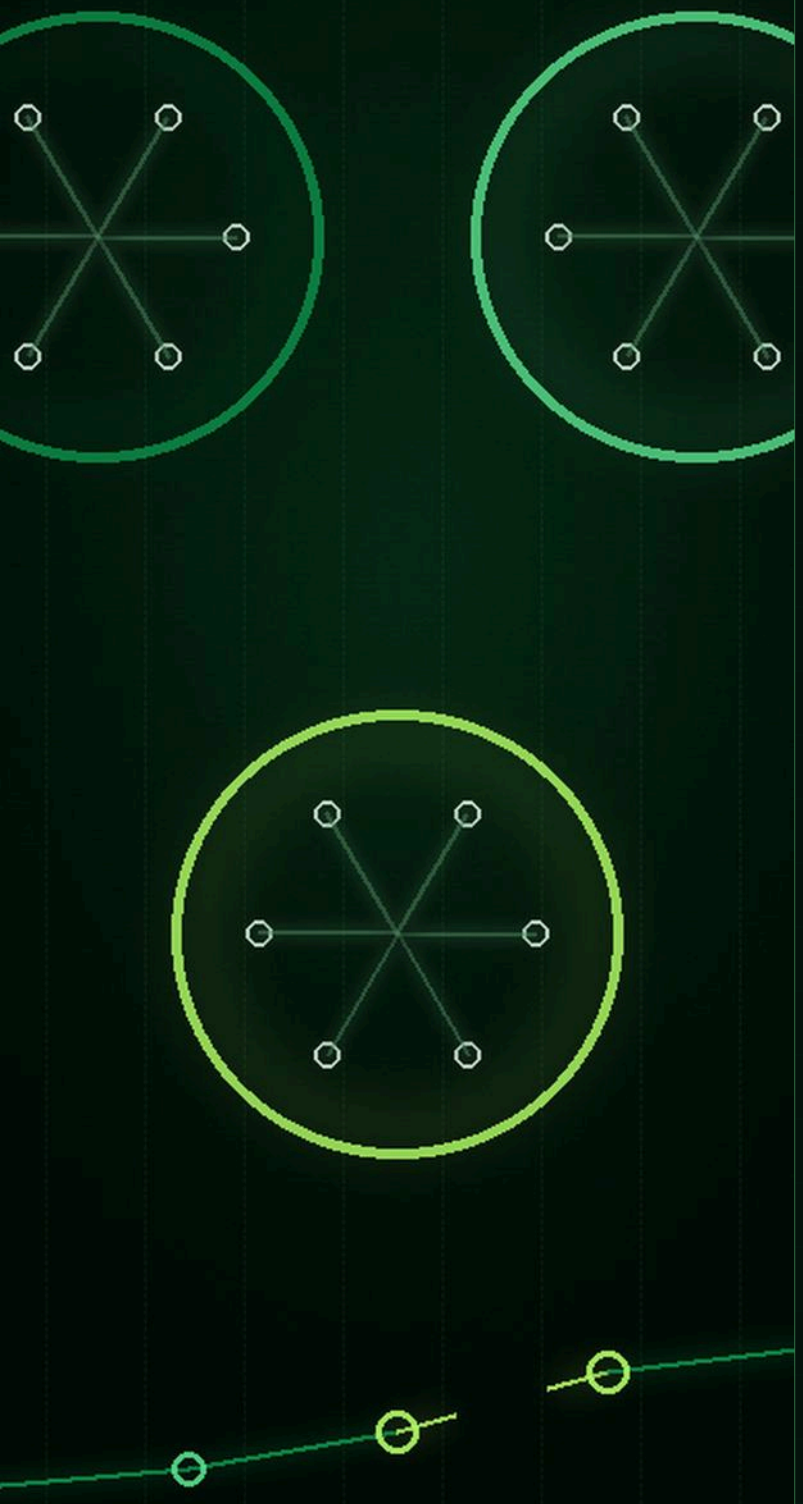
05 NON-NSS FEDERAL LANE

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.

Sources: W05, N01, N03, W02, D01



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.

Original technical artwork: Qtonic Quantum.

NATIONAL SECURITY SYSTEMS

CNSA 2.0: the dates that govern

Use the current policy and the applicable exception authority. NSS, civilian-federal and vendor timelines are distinct.

JAN 1, 2027

NEW NSS ACQUISITIONS

Apply CNSS/NSA policy with the new NIAP implementation guidance (p.30). Identify implemented or updateable PQC, product version and supporting evidence.

DEC 31, 2030

PHASE OUT NON-SUPPORTING SYSTEMS

Phase out equipment and services that cannot support CNSA 2.0 unless otherwise noted. Begin supplier and replacement work before the cutoff.

DEC 31, 2031

MANDATED ALGORITHM USE

CNSA 2.0 algorithm use is mandated unless otherwise noted. Keep applicable exceptions and system-specific guidance visible.

THE ALGORITHM PROFILE IS SPECIFIC

Relevant NSS guidance selects ML-KEM-1024 and ML-DSA-87. AES-256, specified hashes and approved stateful software/firmware signing remain part of the suite. A different FIPS-approved parameter set is not automatically CNSA 2.0 compliant.

Apply the current NSA FAQ, CNSS policy and system authority together. The broader 2035 national goal does not extend these earlier gates. This page uses FAQ v2.1 (December 2024); it does not reproduce the older technology-category timetable.

NEW ACQUISITION EVIDENCE

What buyers must ask suppliers now

A contract promise, an evaluated product and a fielded mission capability are different states. The August 31 policy makes the sequence explicit.

AUGUST 31, 2026 | NIAP POLICY LETTER 33

NSS procurement now faces staged product-readiness tests. The new policy is effective January 1, 2027; it distinguishes contract requirements, evaluation intake and product-list posting.

2027

CONTRACT LANGUAGE

From January 1, government contracts for NSS products must require implemented PQC or the ability to update the product to implement it.

2028

EVALUATION INTAKE

From January 1, products without CNSA 2.0 for every cryptographic function cannot enter NIAP evaluation, subject to the policy's stated exception.

2029

PRODUCT LISTING

From January 1, such products cannot be posted to the Product Compliant List. The date for archiving existing entries remains to be determined.

Products failing CNSA 1.0 face earlier intake (January 1) and listing (July 1) restrictions in 2027. Consult the full policy for certificate restrictions. An AES-128 Bluetooth exception remains pending a standards update. Products with full CNSA 2.0 support receive validation priority.

BUYER ACTION | QTONIC QUANTUM ANALYSIS

Ask the supplier to show the upgrade mechanism, affected cryptographic functions, delivery date and evidence of readiness for the relevant gate.

Sources: N06, N02, N03 | Reviewed September 9, 2026

STANDARDS STATUS | SEPTEMBER 9, 2026

Approved algorithm is only the start

Ask separately what is standardized, what is validated, what profile is required and what the mission owner has authorized.

FINAL | ML-KEM

FIPS 203 establishes key encapsulation. It creates a shared secret; the protocol still needs authentication and secure composition.

FINAL | ML-DSA / SLH-DSA

FIPS 204 and 205 establish signature standards. Selection still follows the applicable security profile; SLH-DSA is not in CNSA 2.0.

IN PROGRESS | FN-DSA / HQC

NIST continues standardization work. Do not present selection or ongoing work as a final FIPS publication.

DRAFT | NIST IR 8547

The cited transition document remains an initial public draft. Proposed dates are planning direction, not universal statutory deadlines.

SEPTEMBER 21-22 | MODULE-VALIDATION TRANSITION

FIPS 140-2 validations remain active through September 21, 2026. From September 22, only FIPS 140-3 validations remain on the active list. Historical modules may continue in existing systems under applicable agency policy.

BUYER CHECK

Record the module certificate, approved mode, version and algorithm coverage. This validation-list transition is not a new PQC migration deadline. A FIPS algorithm standard, a module validation and mission authorization establish different things.

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.

Sources: S01, S02, S03, S05

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.

Sources: S06

EXECUTIVE POLICY | CURRENT IMPLEMENTATION

EO 14412 and OMB M-26-15

Correct authority is part of the evidence. Separate an issued instruction, a forthcoming rule and an enforceable contract requirement.

SOURCE CHECK | THE EXECUTIVE ORDER IS 14412

The Federal Register identifies EO 14412, signed June 22 and published June 25, 2026: 91 FR 38483, FR Doc 2026-12909. Some DoW materials and coverage use 14409. Use the Federal Register identifier when citing this order.

ISSUED JUN 24

AGENCY PLANS: OCT 22, 2026

OMB M-26-15 is already issued. Non-NSS agency plans are due within 120 days of June 24. The EO targets key establishment by 2030 and signatures by 2031.

DEC 19, 2026

PROPOSED FAR RULE

The order directs a proposed covered-contractor rule and specified validation initiatives. It targets applicable contractor PQC compliance by December 31, 2030; a proposed rule is not an effective clause.

MAR 19, 2027

CBOM AND DISCLOSURE WORK

Deadline for public CBOM minimum-elements guidance and proposed cryptographic vulnerability-disclosure rules. A named file format does not establish future compliance.

AUTHORITY BOUNDARY

Civilian EO/OMB actions do not replace NSS or DoW authorities. Apply requirements incorporated into the solicitation and contract; keep the authority, system scope, due date and accepting official together.

COALITION READINESS UPDATE

From migration advice to buying decisions

The latest guidance strengthens the case for a funded transition plan tied to mission dependencies and normal technology renewal.

SEPTEMBER 3, 2026 | G7 CYBERSECURITY WORKING GROUP

Start the transition through inventory and renewal

The G7 call to action asks public and private organizations to begin phased, risk-based PQC migration. It emphasizes critical systems, cryptographic inventories, dependency mapping, transition plans, product renewal and public procurement. The risk includes authentication as well as harvested ciphertext. [C04]

01

INVENTORY

Identify cryptographic assets and their dependencies.

02

PRIORITIZE

Start with critical systems and long-lived sensitive data.

03

PROCURE

Put PQC requirements into renewal and purchasing decisions.

04

VERIFY

Test interoperability and close the complete trust path.

AUGUST 2026 | NATIONAL SECURITY TECHNOLOGY PRIORITIES

The White House National Security Science and Technology Strategy explicitly lists post-quantum cryptography as a critical and emerging technology. This is strategic direction, not a product approval or contract award. [W06]

Qtonic Quantum analysis: align coalition profiles, supplier evidence and purchasing cycles now. The G7 publication creates no new universal U.S. statutory deadline.

Sources: C04, W06; see C01 and C03 | Reviewed September 9, 2026

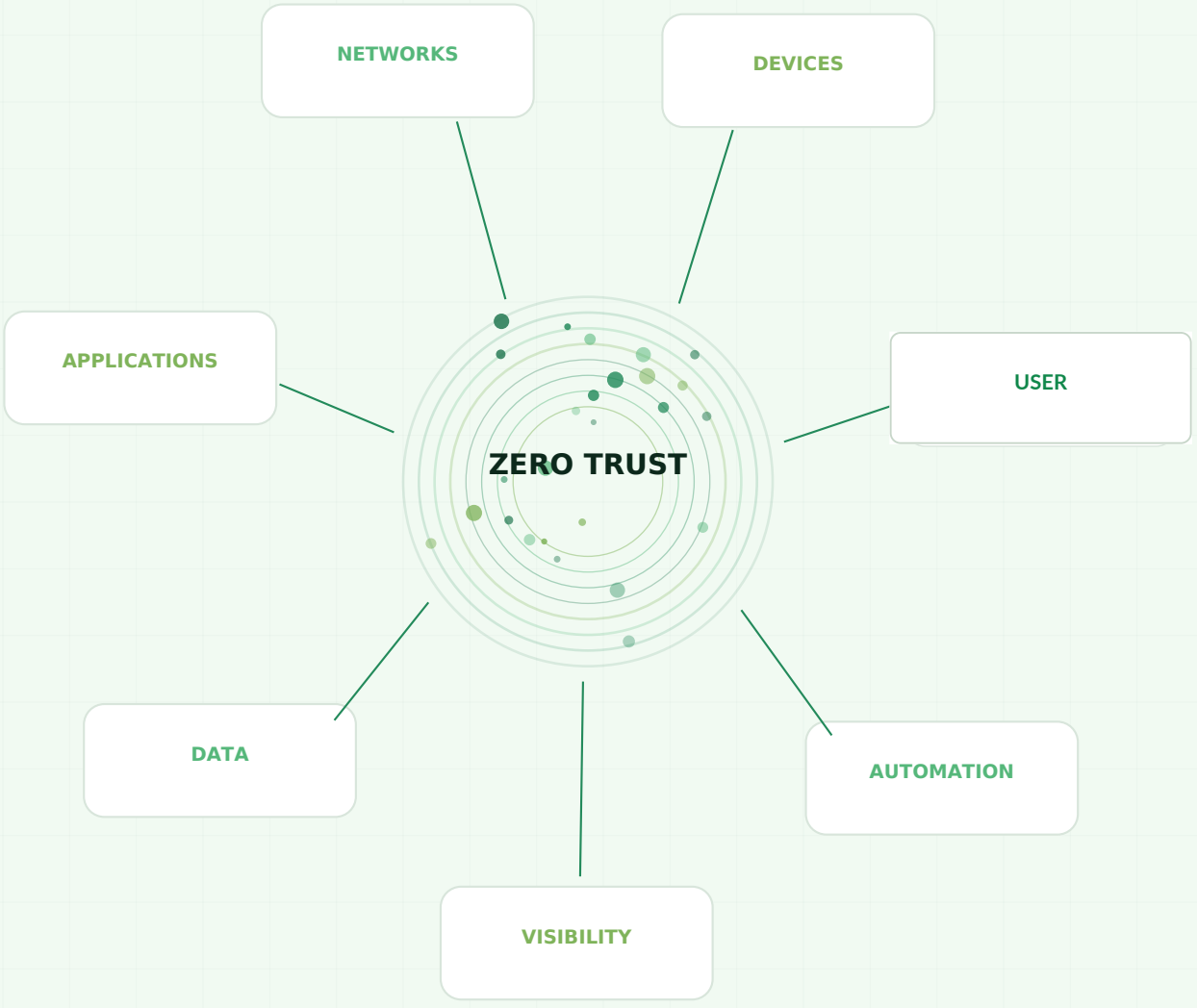
SEVEN PILLARS, ONE TRUST FABRIC

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.

Sources: D03, D04, N03, N04

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.

Sources: D01, D02, C03, S06

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

Sources: D01, D02

III

The military mission exposure map

01 **IDENTITY**

People, devices and workloads

02 **CONNECTIVITY**

C2, tactical networks and SATCOM

03 **PLATFORMS**

Firmware, software and mission systems

04 **PARTNERS**

Coalition, suppliers and gateways

05 **SUSTAINMENT**

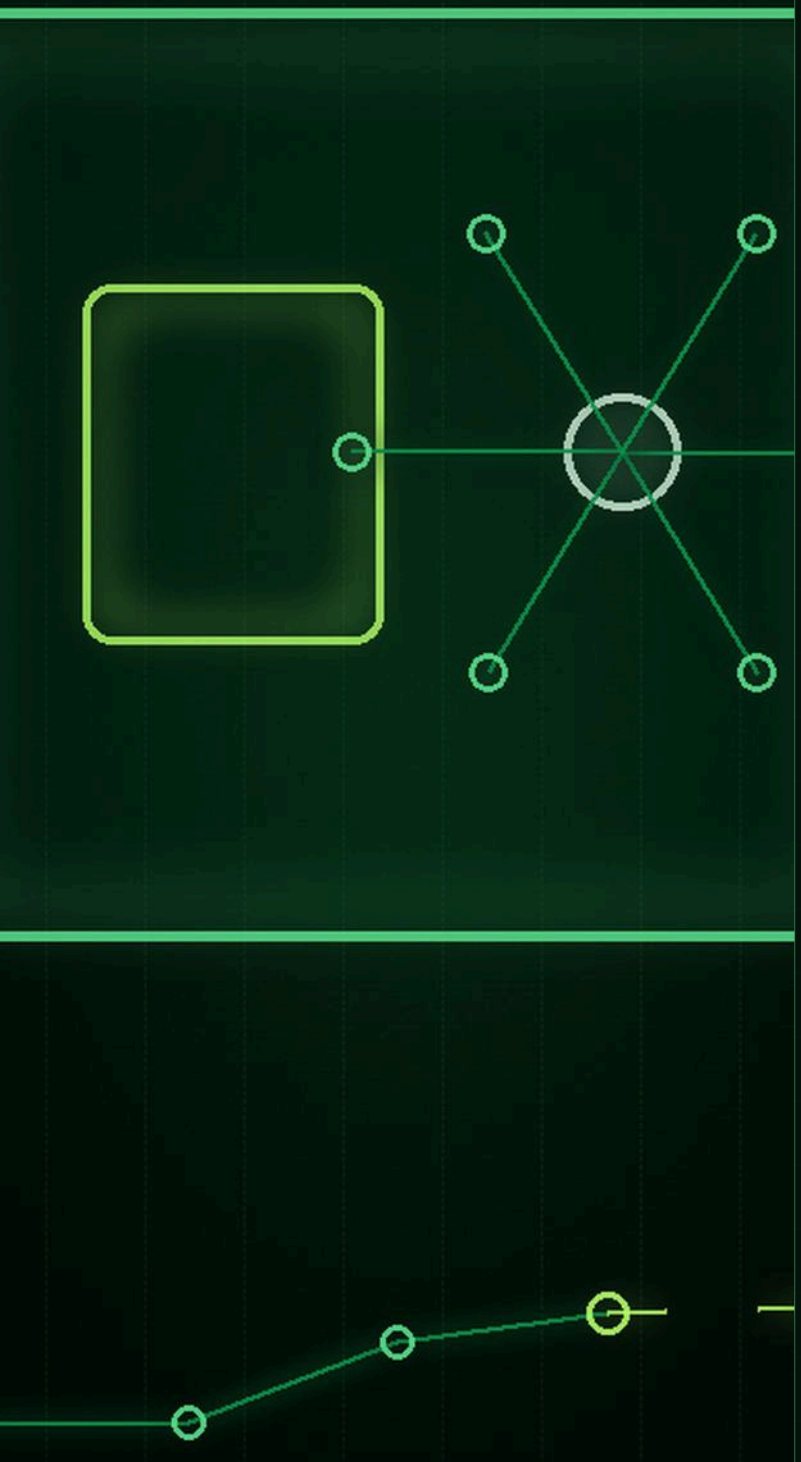
Updates, maintenance and recovery

IN THIS PART

- Enterprise identity, PKI, and access control
- C2, tactical networks, SATCOM, and weapons
- Cloud, software factories, DIB, and suppliers
- 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

Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

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 ASSURANCE

A command is a trust path.

ORIGIN

Authenticate the issuing authority.

TRANSPORT

Protect the agreed communication span.

RECIPIENT

Verify identity, freshness and authorization.

ACTION

Retain the evidence of acceptance.

A secure link does not authorize a command or establish endpoint integrity.

TEST THE COMPLETE EXCHANGE | Observed TLS flights and illustrative bandwidth budget: pp.106-107

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.

Sources: D01, D06

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 ASSURANCE

Beyond the radio link.

TERMINAL

Record software, keys and trust anchors.

LINK

Identify algorithms and negotiated profiles.

GATEWAY

Map relays and trust termination.

MISSION SERVICE

Verify the complete protection boundary.

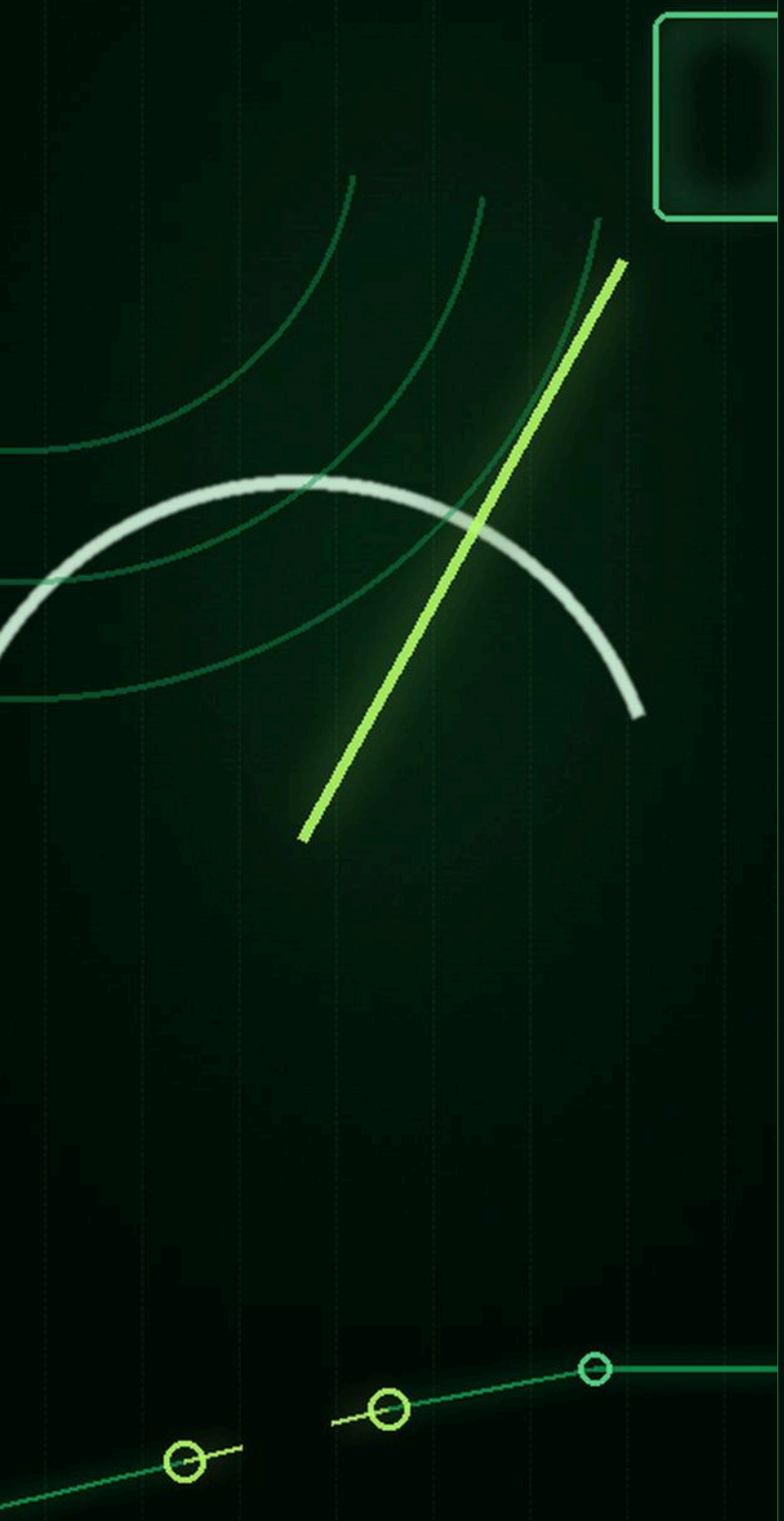
PQC readiness belongs to the complete path and its lifecycle.

TEST THE COMPLETE EXCHANGE | Observed TLS flights and illustrative bandwidth budget: pp.106-107

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.

TEST THE COMPLETE EXCHANGE | Observed TLS flights and illustrative bandwidth budget: pp.106-107

Original technical artwork: Qtonic Quantum.

Sources: D01, D07

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.**

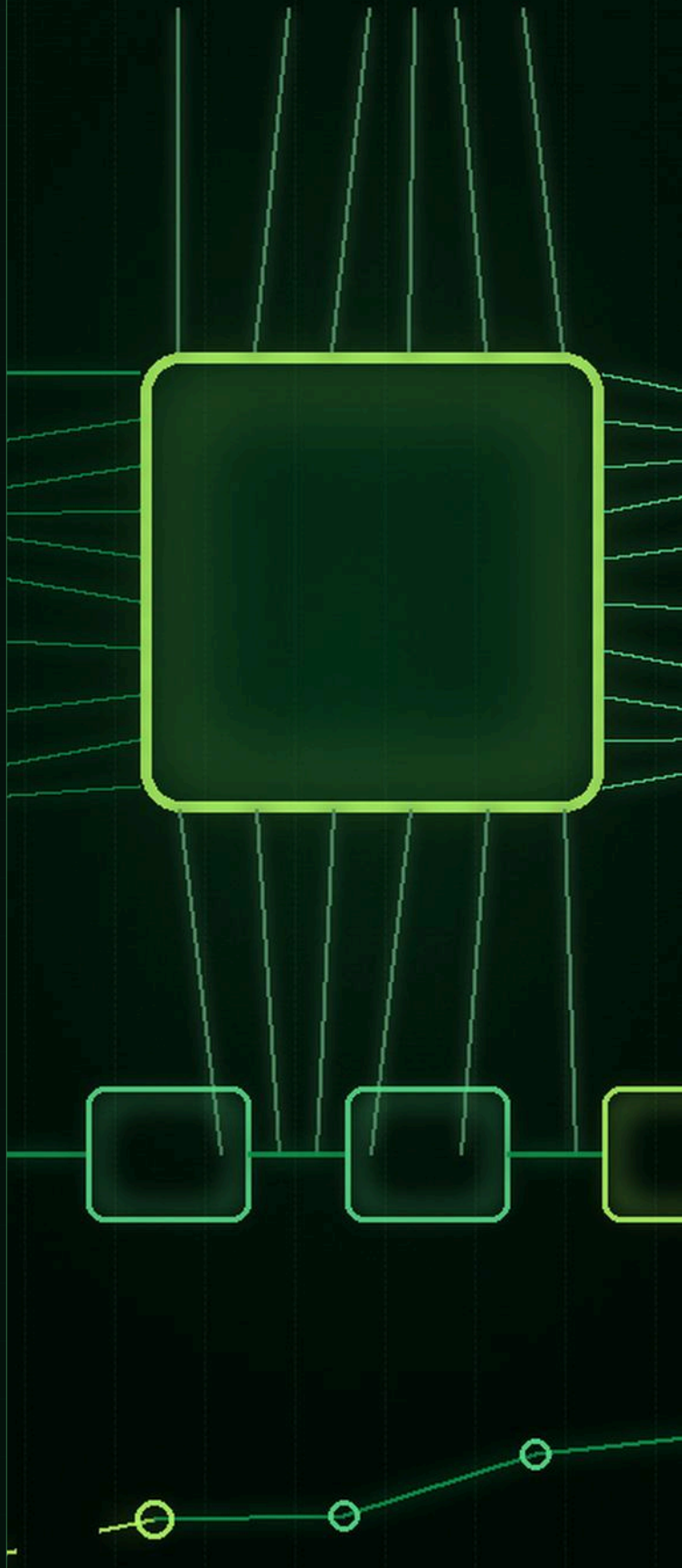
  Proprietary protocols, line-replaceable units, internal buses, remote maintenance, data loaders, diagnostic tools, and support equipment can hide RSA or ECC dependencies.

- **Safety and certification.**

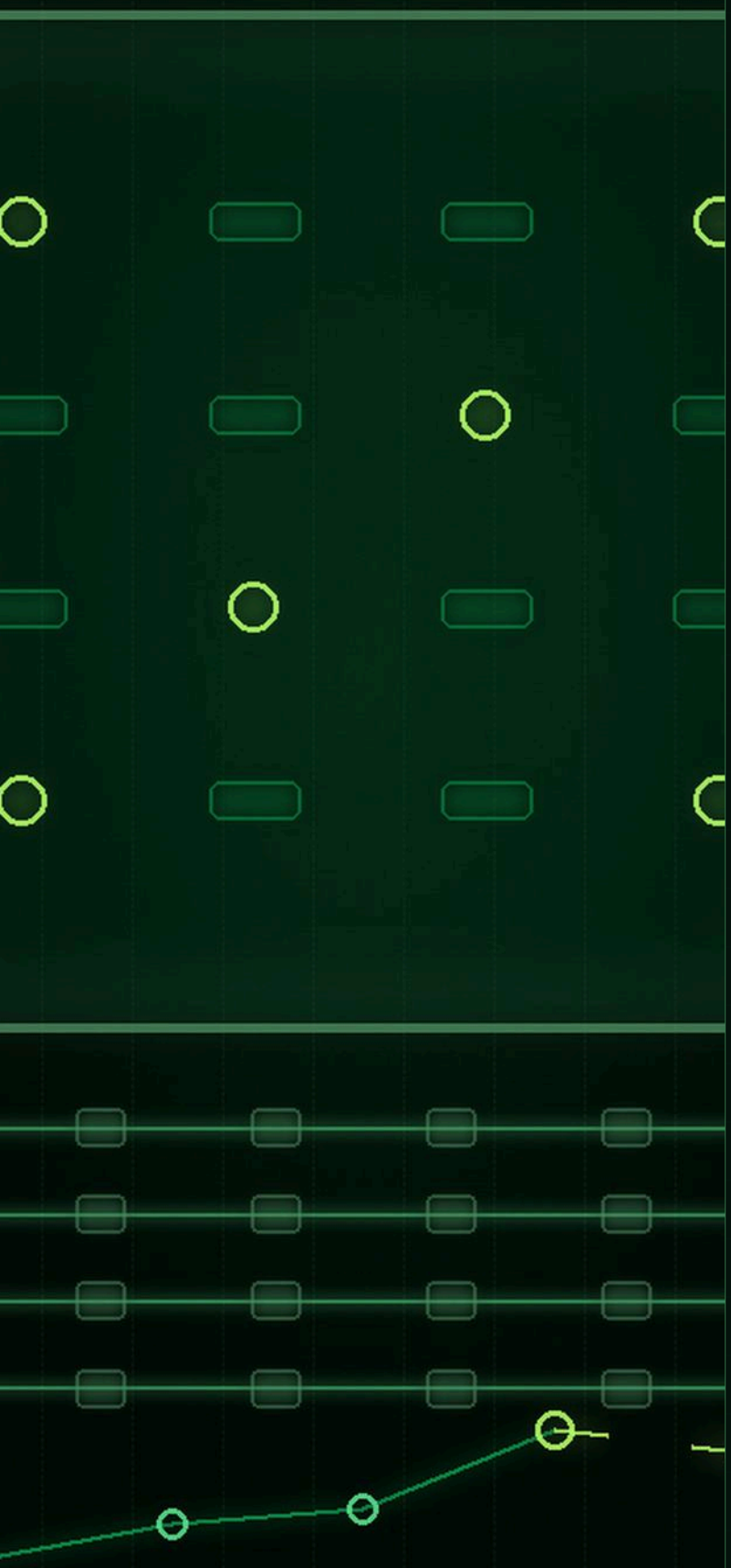
  Algorithm changes can affect timing, resource use, deterministic behavior, software baselines, hardware qualification, airworthiness, weapons safety, interoperability, and authorization evidence.

- **Sustainment reality.**

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



Original technical artwork: Qtonic Quantum.



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.

AUG 19 | ACTIVE OT THREAT

NSA and partners reported targeting of Siemens S7 controllers with AI-generated exploitation scripts presented as monitoring tools. The advisory concerns critical infrastructure; it does not establish compromise of a military installation. [C05]

IMMEDIATE DEFENSIVE PRIORITIES

Reduce exposed access, segment control systems, protect engineering identities, apply tested vendor fixes and verify recovery copies. PQC does not repair weak authorization or an already compromised workstation.

MIGRATION IMPLICATION

Inventory firmware signing, remote maintenance, VPNs and device trust. Schedule cryptographic changes around safety, vendor support and representative process-control testing.

Original technical artwork: Qtonic Quantum.

Sources: D01, C02

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.**

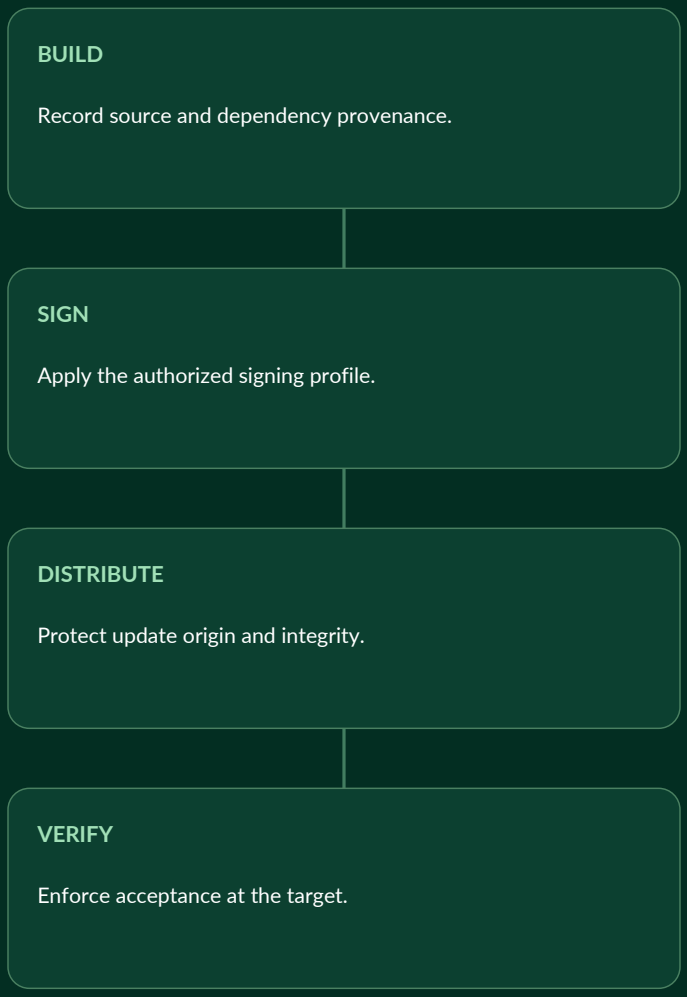
  Images, packages, firmware, manifests, signatures, provenance, scanning, replication, retention, promotion, quarantine, and revocation.

- **RUNTIME — Applications and service identity.**

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

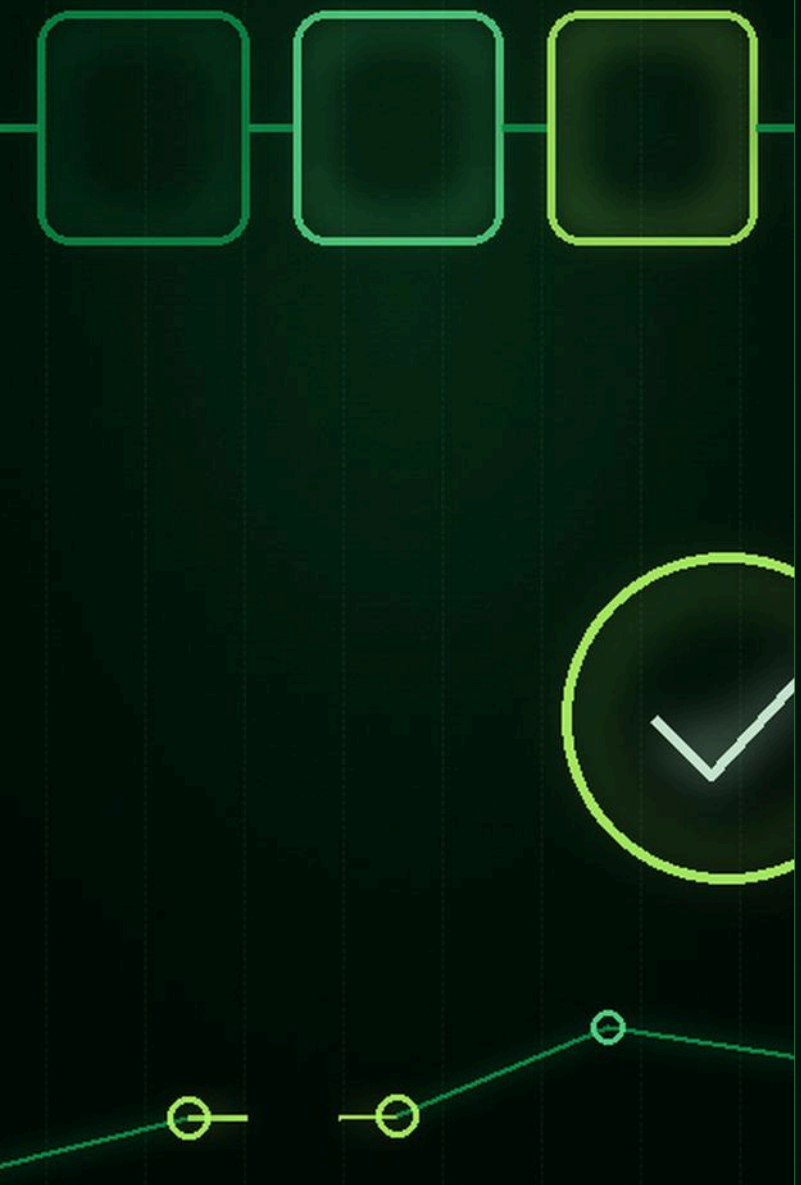
MISSION ASSURANCE

The software trust chain.



Key rotation, revocation and recovery must work in the fielded configuration.

ILLUSTRATIVE TRUST PATH



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.

Original technical artwork: Qtonic Quantum.

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.**

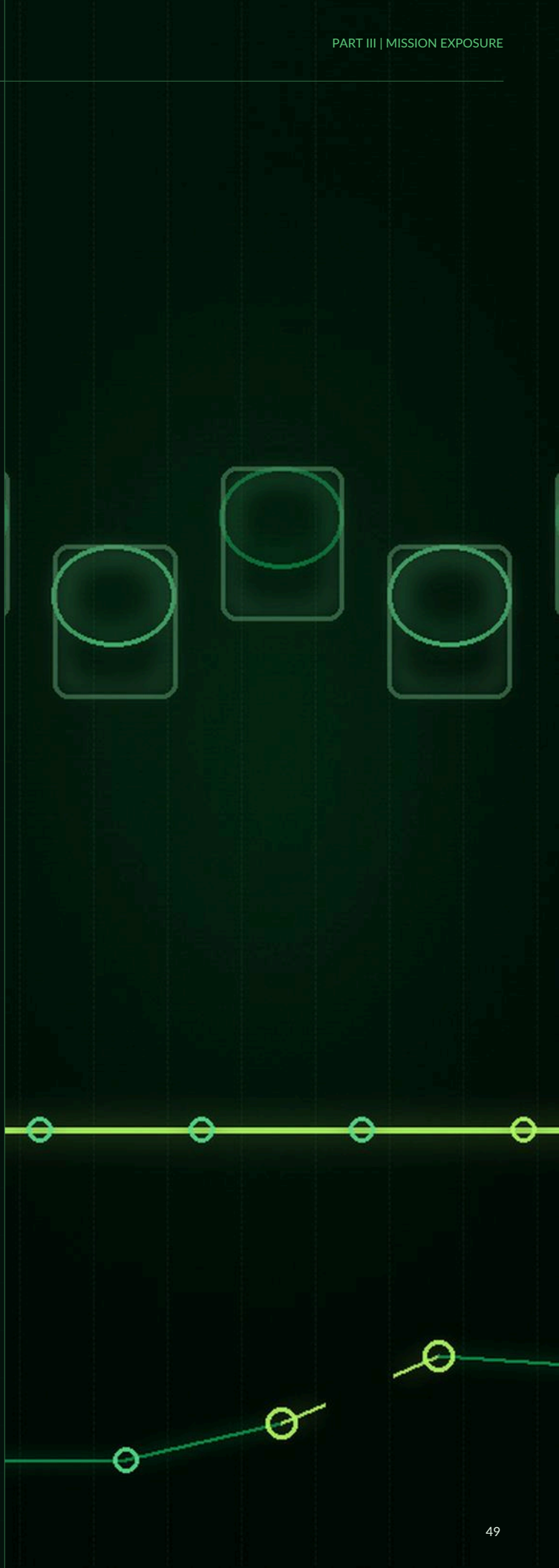
  Include backups, replicas, removable media, cloud archives, partner copies, legal holds, disaster recovery, data lakes, exports, and encrypted traffic captures.

- **COLLECTION EXPOSURE.**

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

- **RE-ENCRYPTION FEASIBILITY.**

  Re-encryption protects future exposure; it cannot erase ciphertext already harvested. Preserve provenance, verify the transformation and account for every retained copy.



Original technical artwork: Qtonic Quantum.

MISSION ASSURANCE

One agreed profile.

PROFILE

Agree parameters and coexistence rules.

PARTNER A

Verify the sending trust boundary.

PARTNER B

Verify the receiving trust boundary.

MISSION

Test interoperability and releasability.

Record shared acceptance evidence and the retirement gate for vulnerable fallback.

ILLUSTRATIVE TRUST PATH

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.**

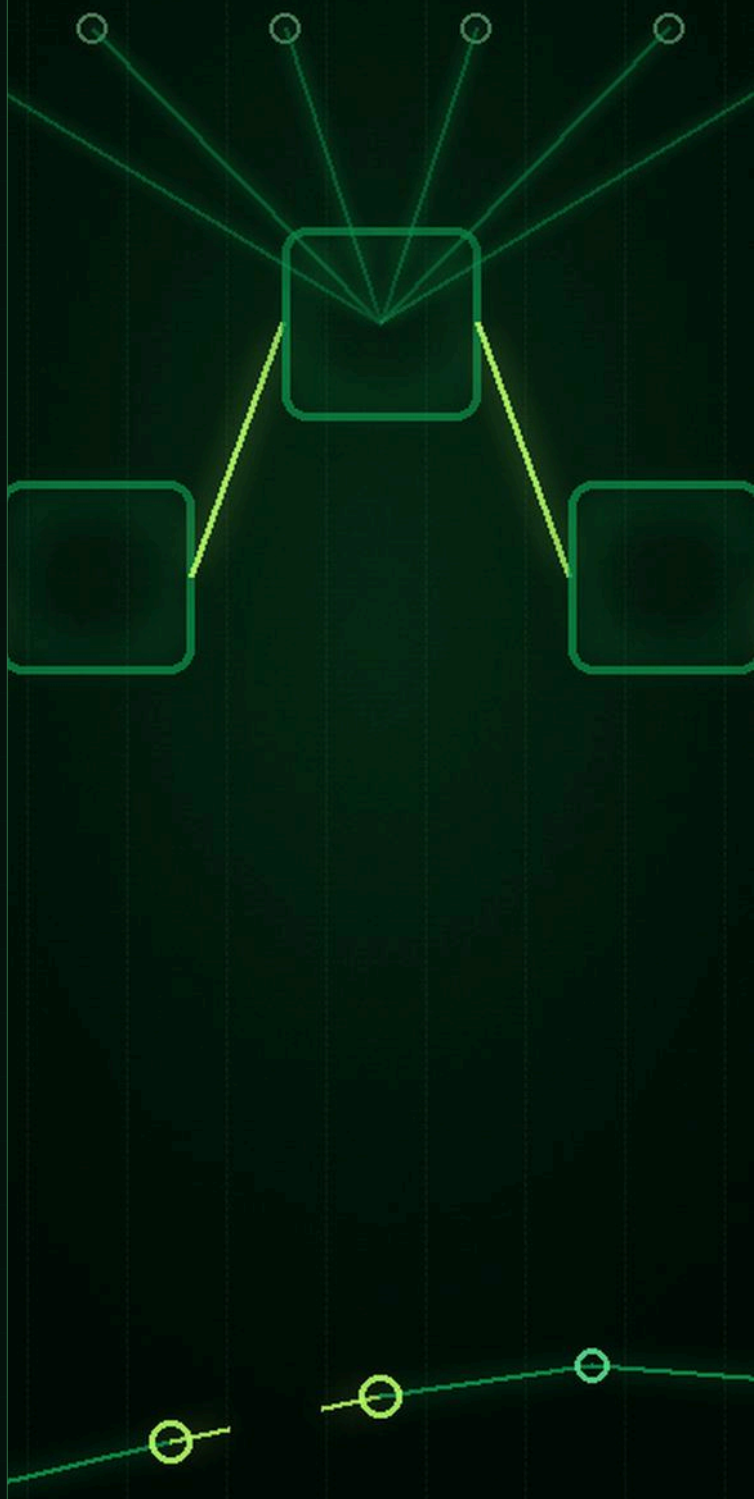
  CUI repositories, PLM/CAD, source code, build pipelines, collaboration, email, remote access, backups, key management, certificates, and long-lived weapon-system information.

- **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.**

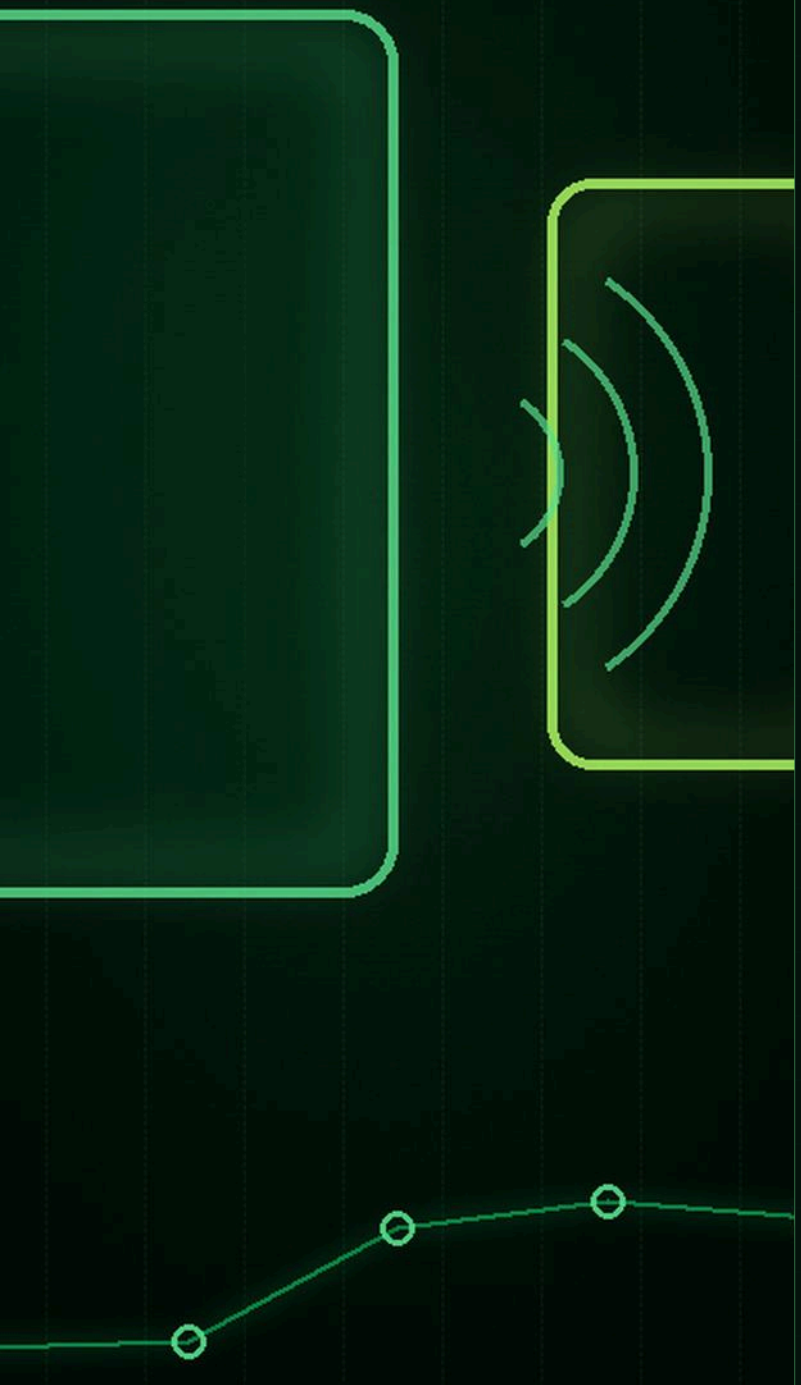
  SaaS, cloud, help desk, remote maintenance, telemetry, update servers, identity federation, subcontractor access, service accounts, and shared-responsibility boundaries.



CMMC STATUS | JULY 13, 2026

DoW suspended Phase II and future rollout milestones; Phase I self-assessments remain. Continuing NIST SP 800-171 obligations and contract terms still matter. This is not a current PQC certification requirement. [D08]

Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

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.**

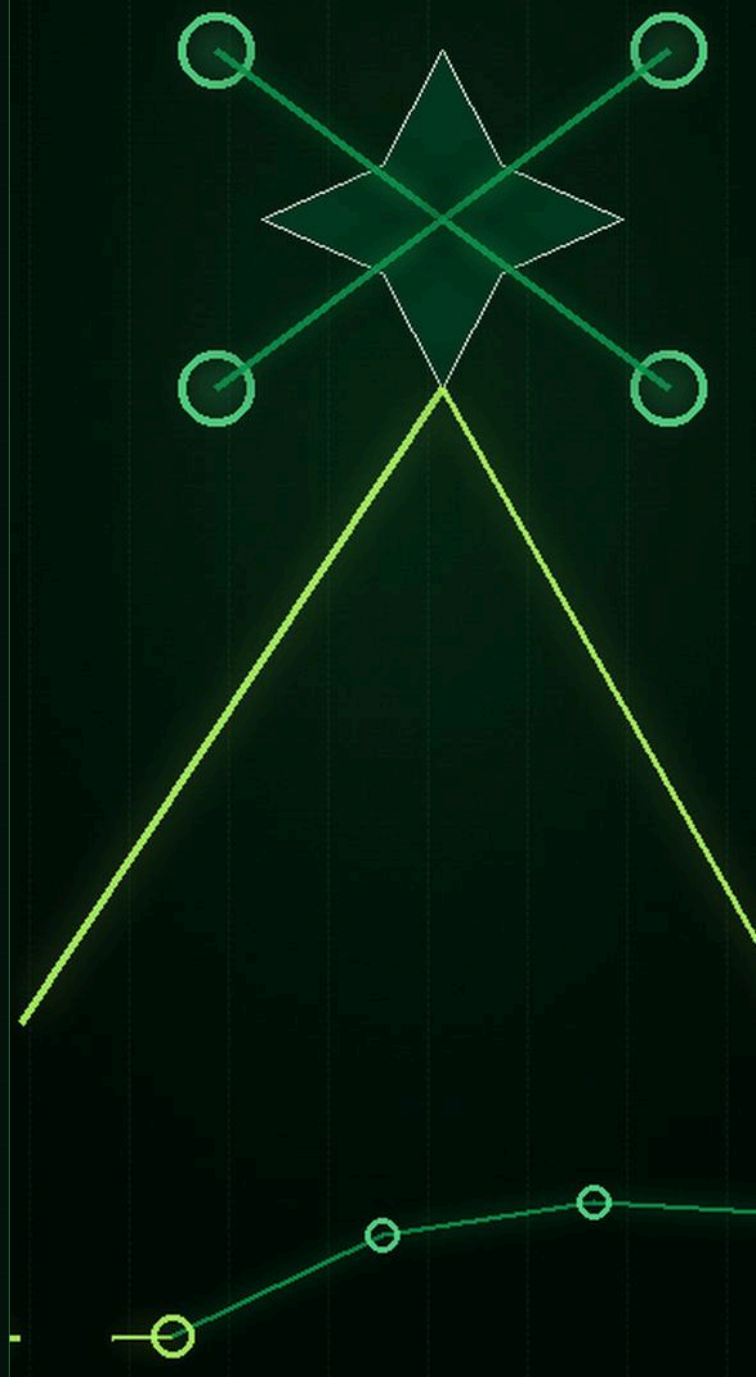
  Authenticated control, mission updates, telemetry, group keying, swarm communications, relay, gateway trust, loss, latency, jamming, and disconnected behavior.

- **SOFTWARE — Boot, firmware, applications, and models.**

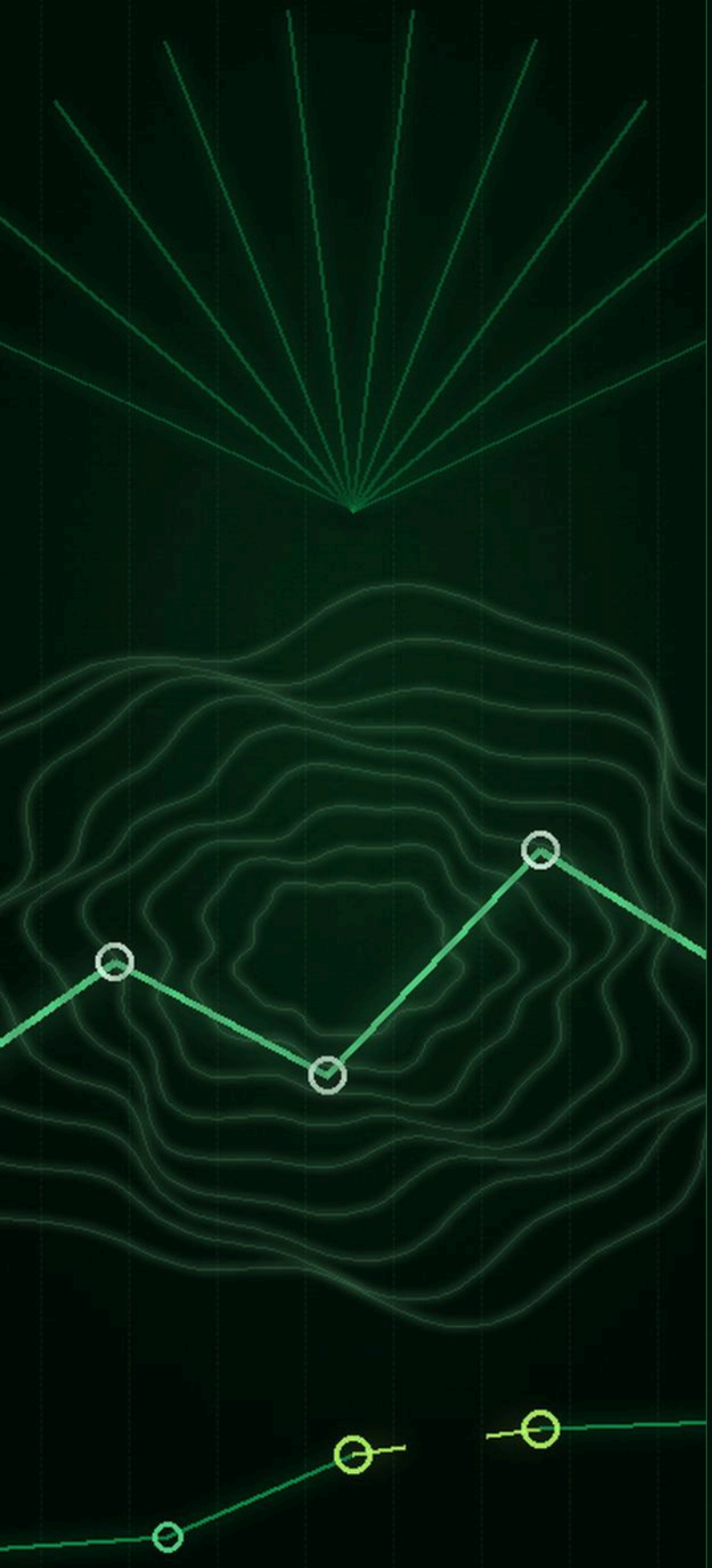
  Signed boot chains, remote update, model provenance, configuration, rollback prevention, third-party components, mission data, and emergency recovery images.

- **SENSING — Navigation and data provenance.**

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



Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

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.**

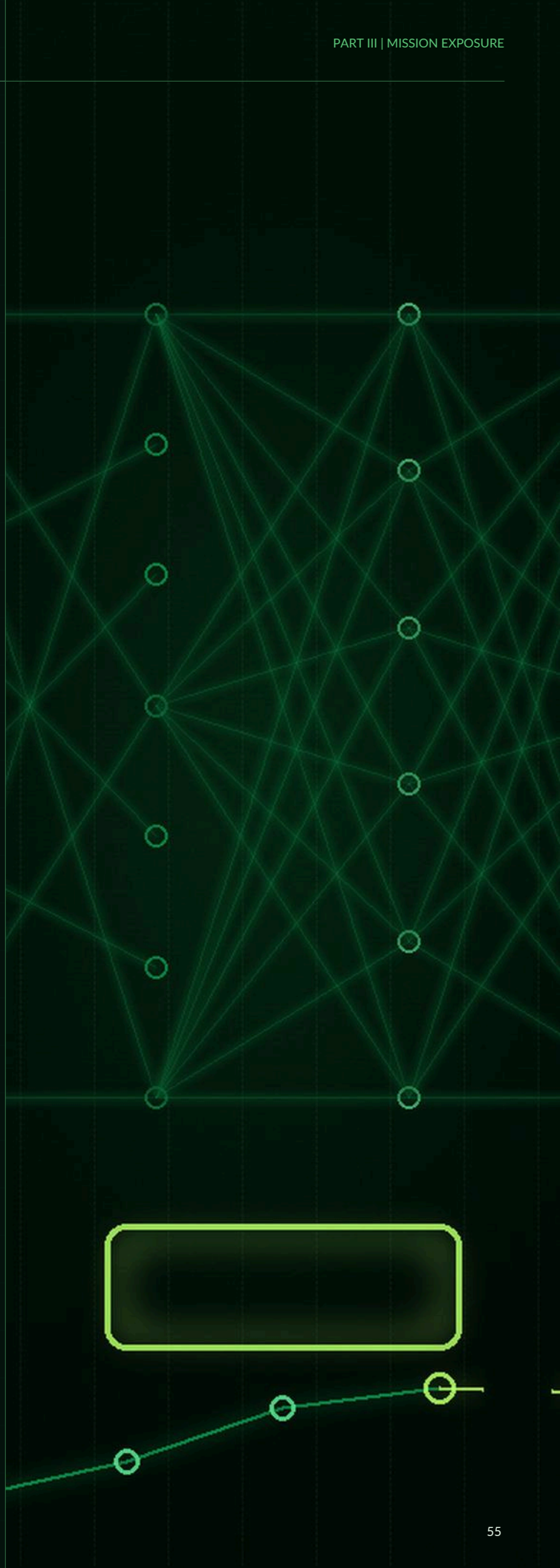
  Signing, hashing, registry, version, approvals, evaluation results, fine-tuning lineage, rollback, intellectual property, and long-lived sensitive content.

- **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.



Original technical artwork: Qtonic Quantum.

MISSION ASSURANCE

Sustain the fielded state.

CONFIGURATION

Record installed versions and trust anchors.

PROVISION

Control certificates, keys and identity.

UPDATE

Prove the authorized update path.

RECOVER

Test rollback, revocation and restoration.

Match suppliers, training and replacement plans to the fielded configuration.

ILLUSTRATIVE TRUST PATH

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.

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.**

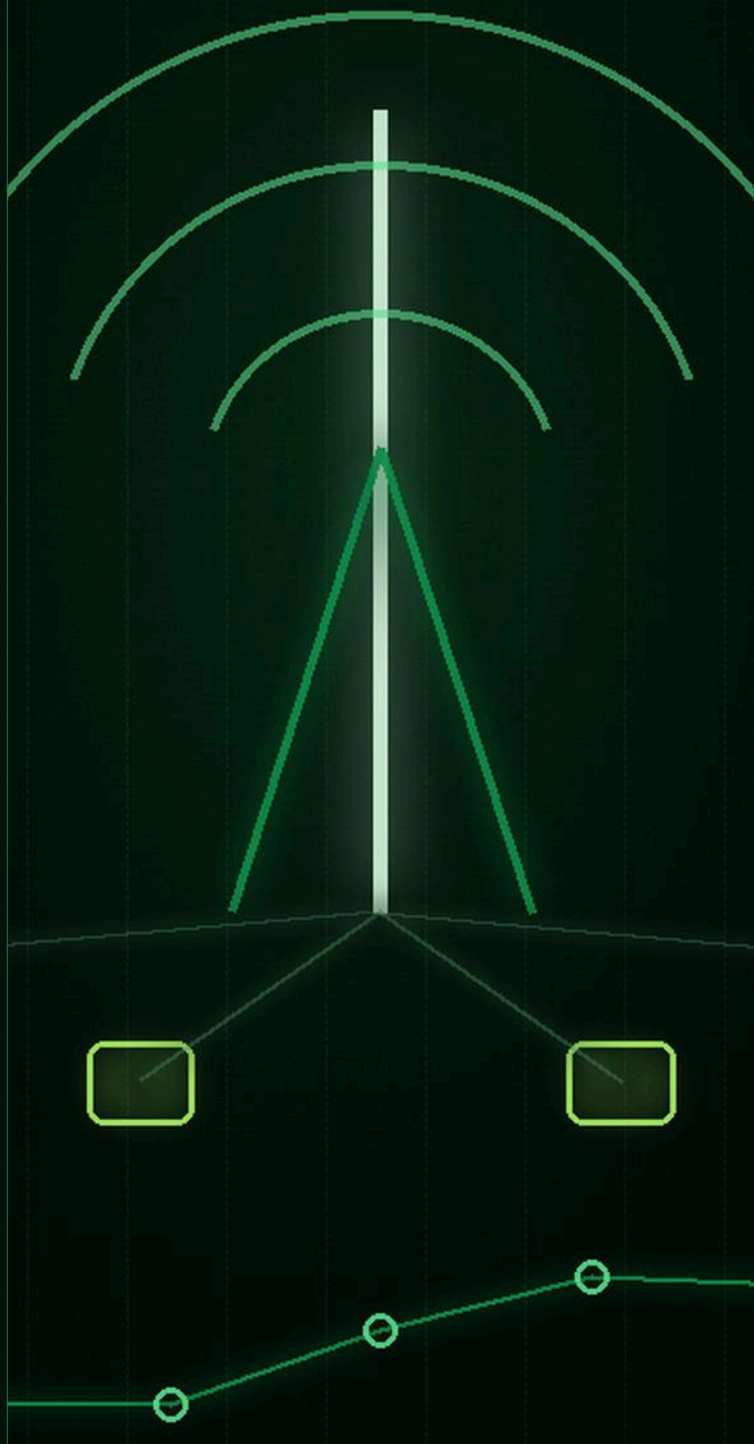
  Virtualized and containerized core functions, service mesh, APIs, certificates, secrets, orchestration, management planes, images, and artifact signing.

- **Edge applications.**

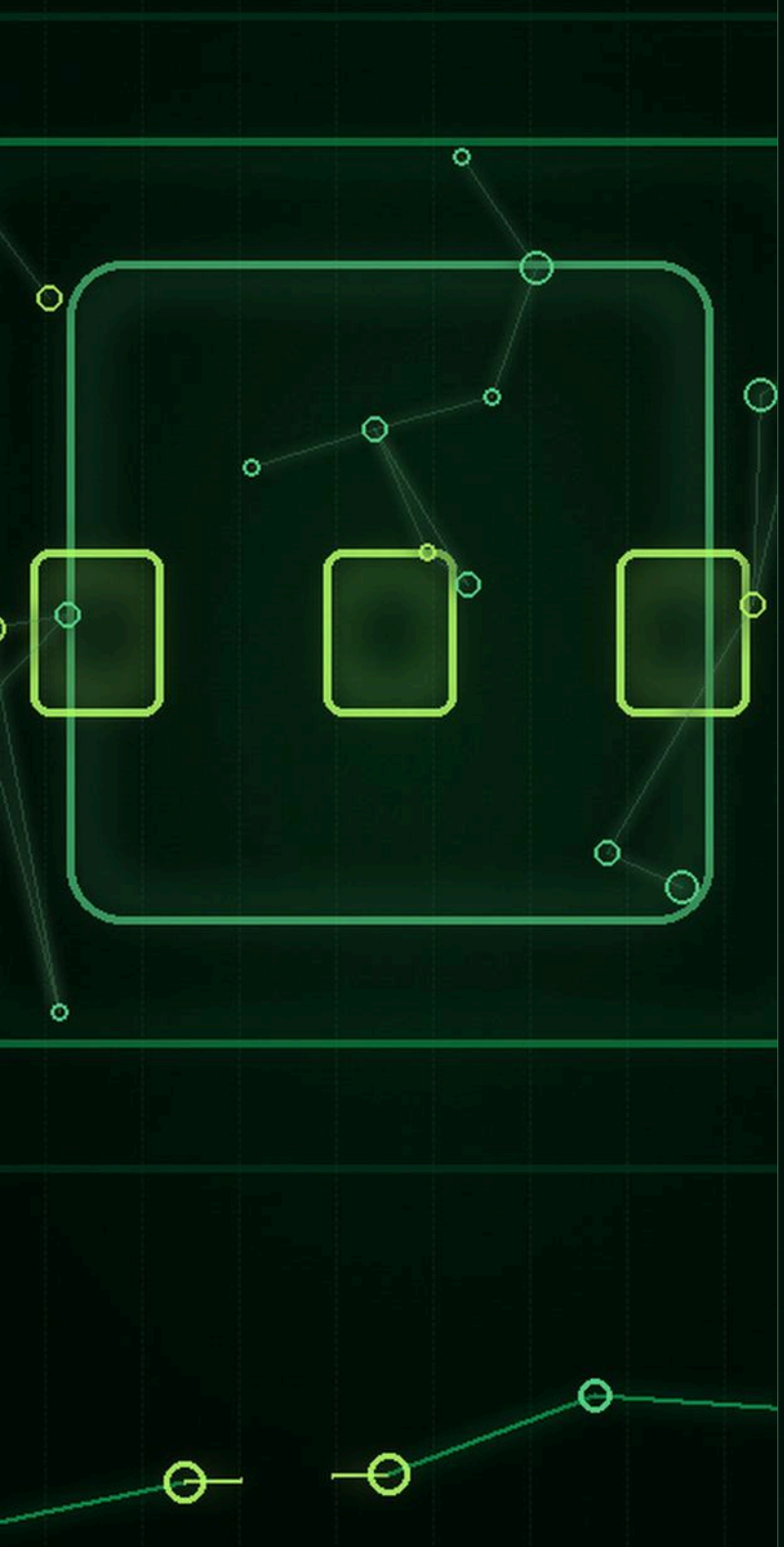
  Mission workloads, sensors, AI services, databases, message buses, gateways, and local KMS/HSM dependencies may use separate cryptographic stacks.

- **Transport and backhaul.**

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



Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

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.**

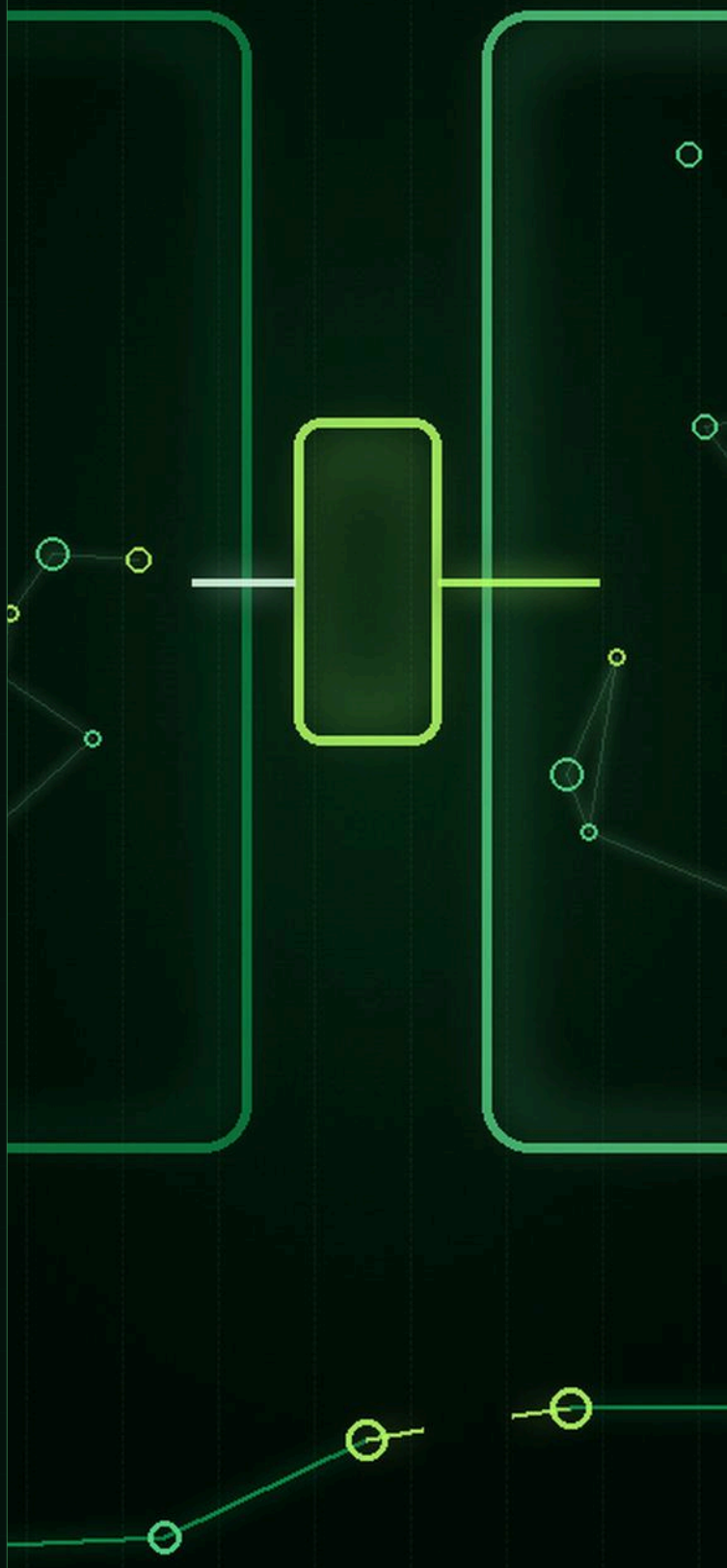
  Cross-domain release may rely on origin, integrity, approval, sanitization, and provenance signatures. Verify that the complete signing and validation chain can transition.

- **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.



Original technical artwork: Qtonic Quantum.

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.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.

Sources: D01, D02, C01

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.

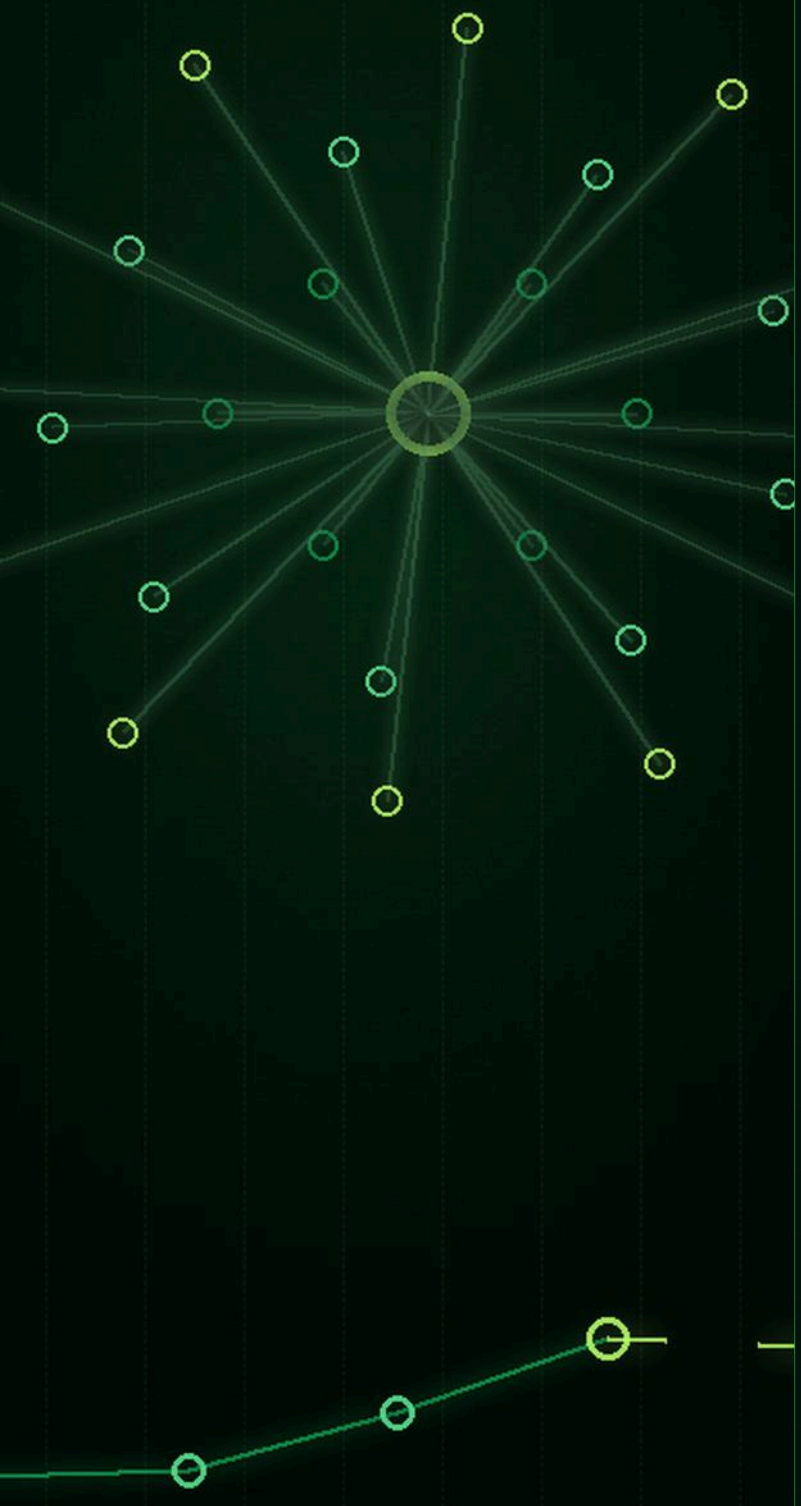
IN THIS PART

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

Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

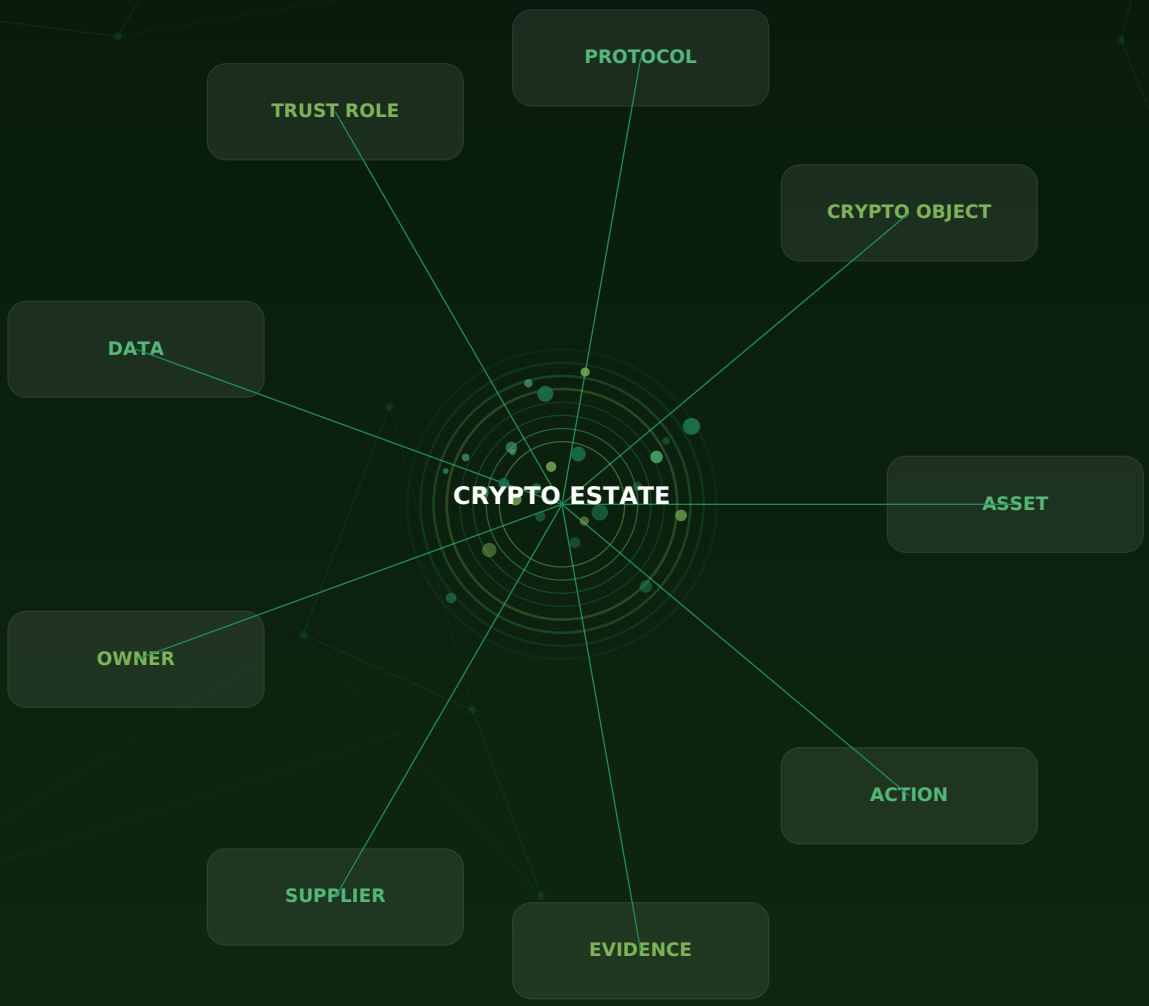
WHAT MUST BE INVENTORIED

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.



Sources: D01, D02, S07, S08

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

Sources: S07, S08, D01, Q01

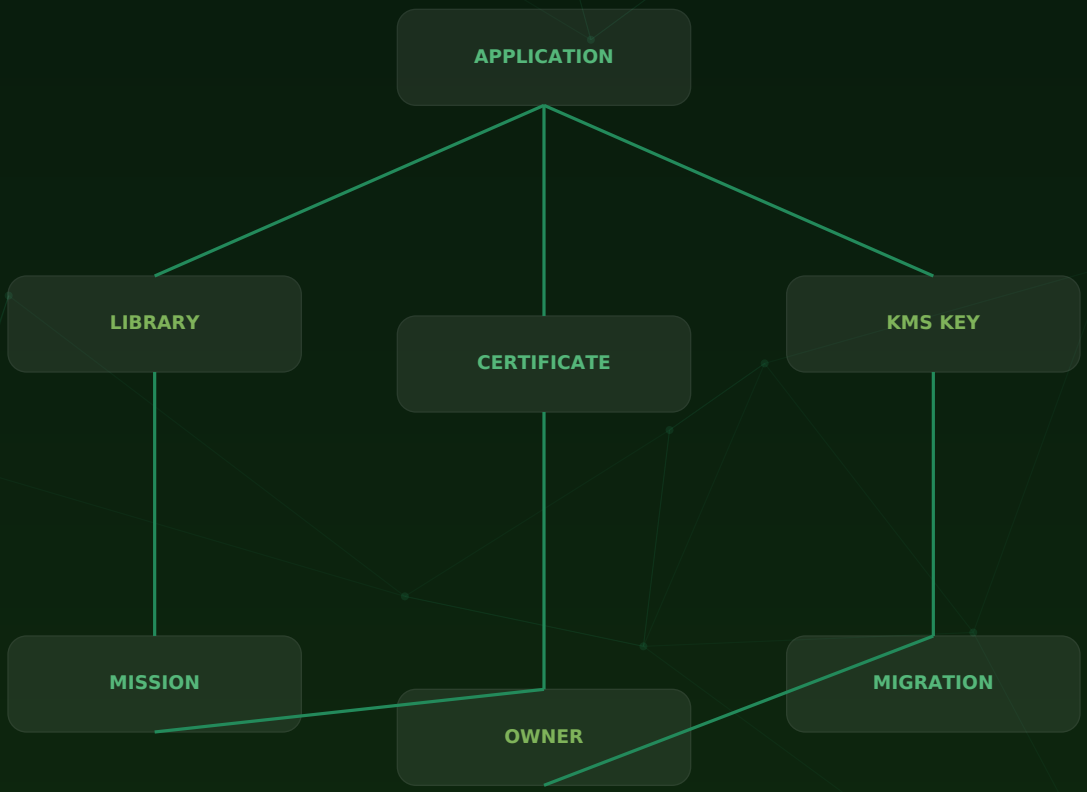
CRYPTOGRAPHIC BILL OF MATERIALS

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.

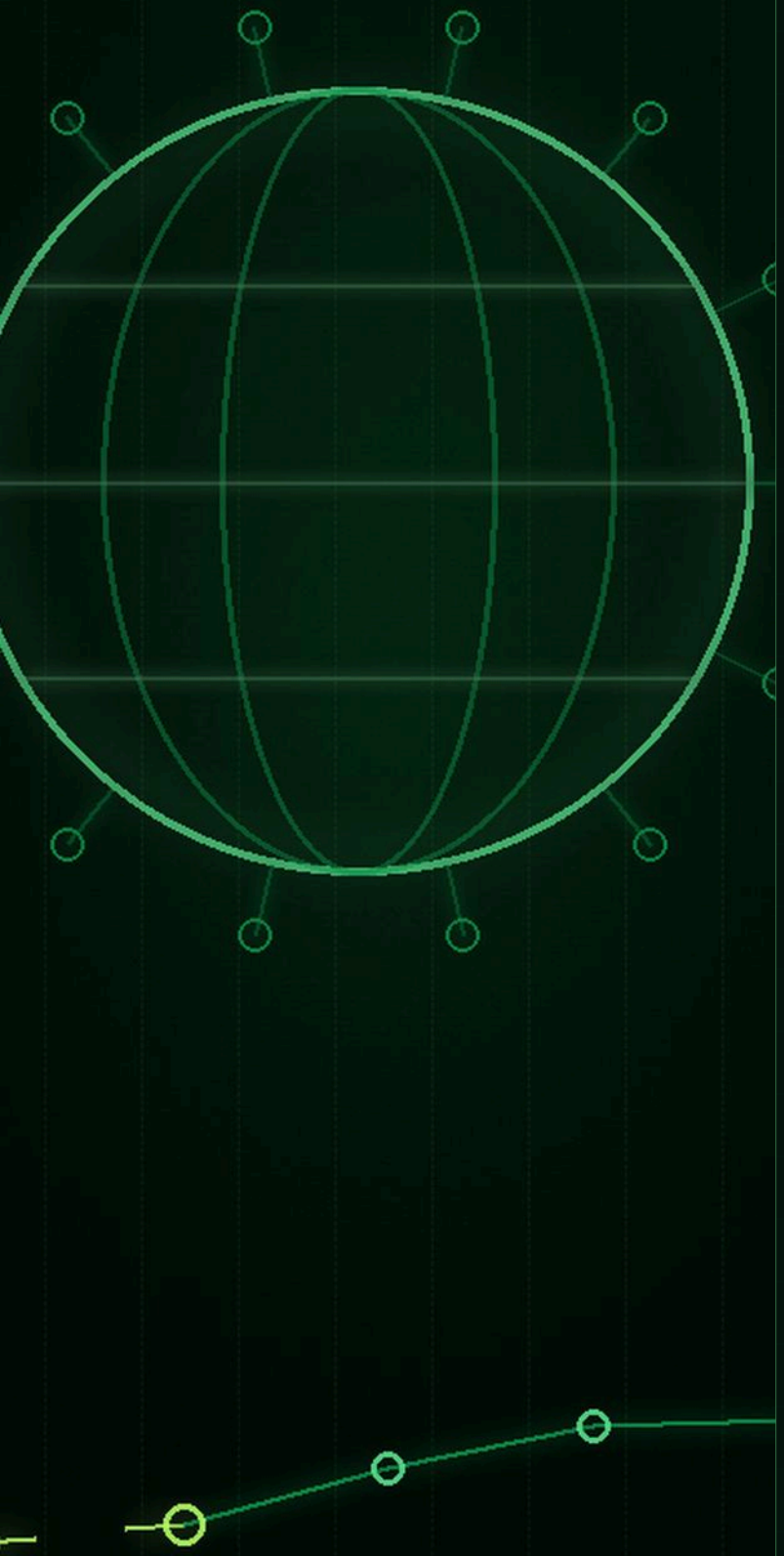
DECISION RULE

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.

Sources: S07, S08, Q01



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.

Original technical artwork: Qtonic Quantum.

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.**

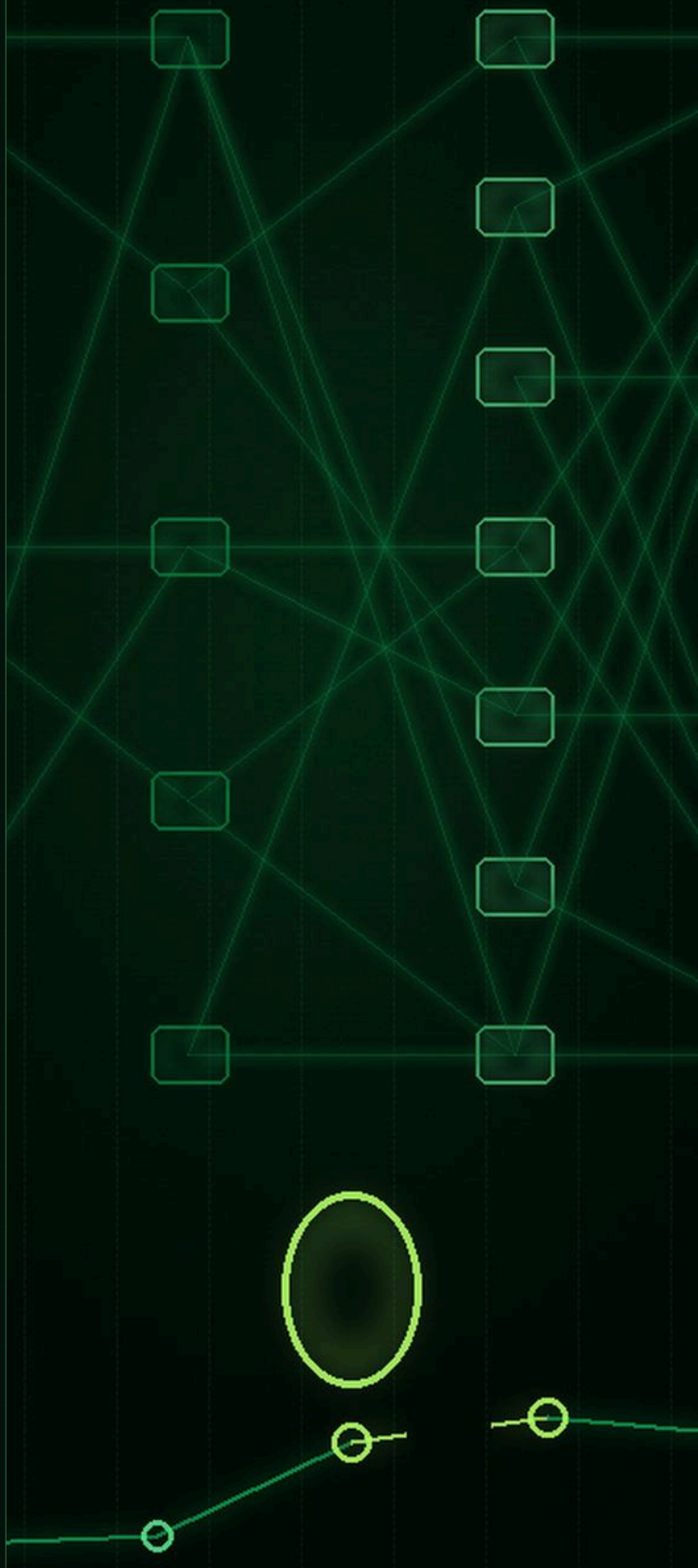
  Algorithm names, key sizes, cipher suites, protocol versions, certificate pins, OIDs, provider-specific assumptions, serialized formats, message limits, and fallback behavior.

- **Dependencies.**

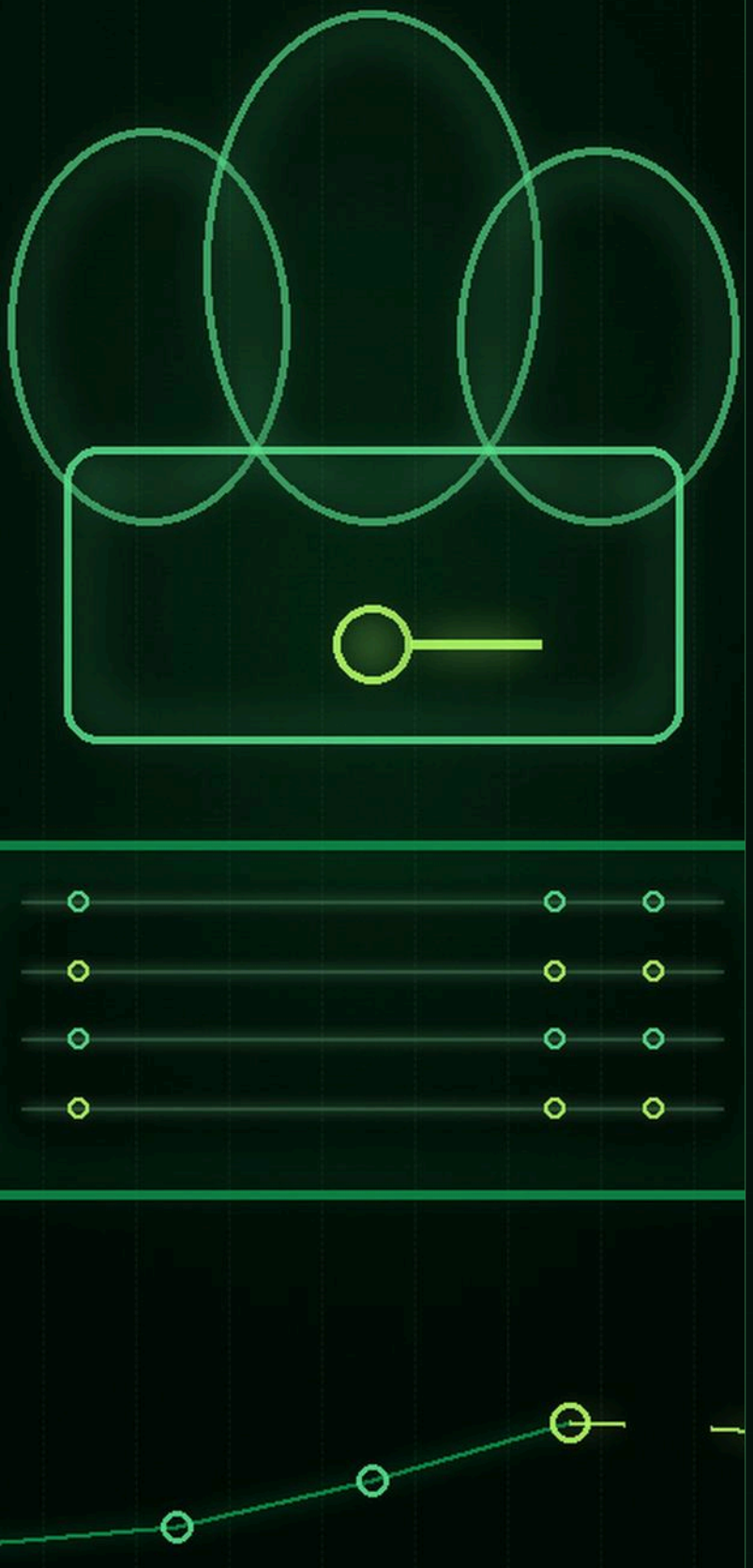
  Direct and transitive libraries, language runtimes, OS providers, containers, firmware SDKs, hardware APIs, open-source packages, and supplier components.

- **Build and signing.**

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



Original technical artwork: Qtonic Quantum.



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.

Original technical artwork: Qtonic Quantum.

FROM CRYPTO OBJECT TO MISSION RISK

Classify confidentiality and trust priorities

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

Illustrative mission framework: review impact, urgency, exposure and friction alongside evidence confidence. This is not the QScout HNDL scoring engine; approve the engagement method before examining results.

01

DATA / TRUST LIFETIME

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

02

COLLECTION EXPOSURE

For confidentiality, assess ciphertext collection now. For integrity and trust, assess future forgery and the signed artifacts or identities it could affect.

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.

Sources: D01, C01, W01, Q01

SCORE THE DECISION, NOT THE DRAMA

A defensible quantum-risk scoring model

Illustrative mission-priority dimensions, separate from the QScout HNDL engine. A score is not a measured probability of a quantum break on a particular date.

IMPACT | URGENCY | EXPOSURE | 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.

Sources: D01, S07, Q01

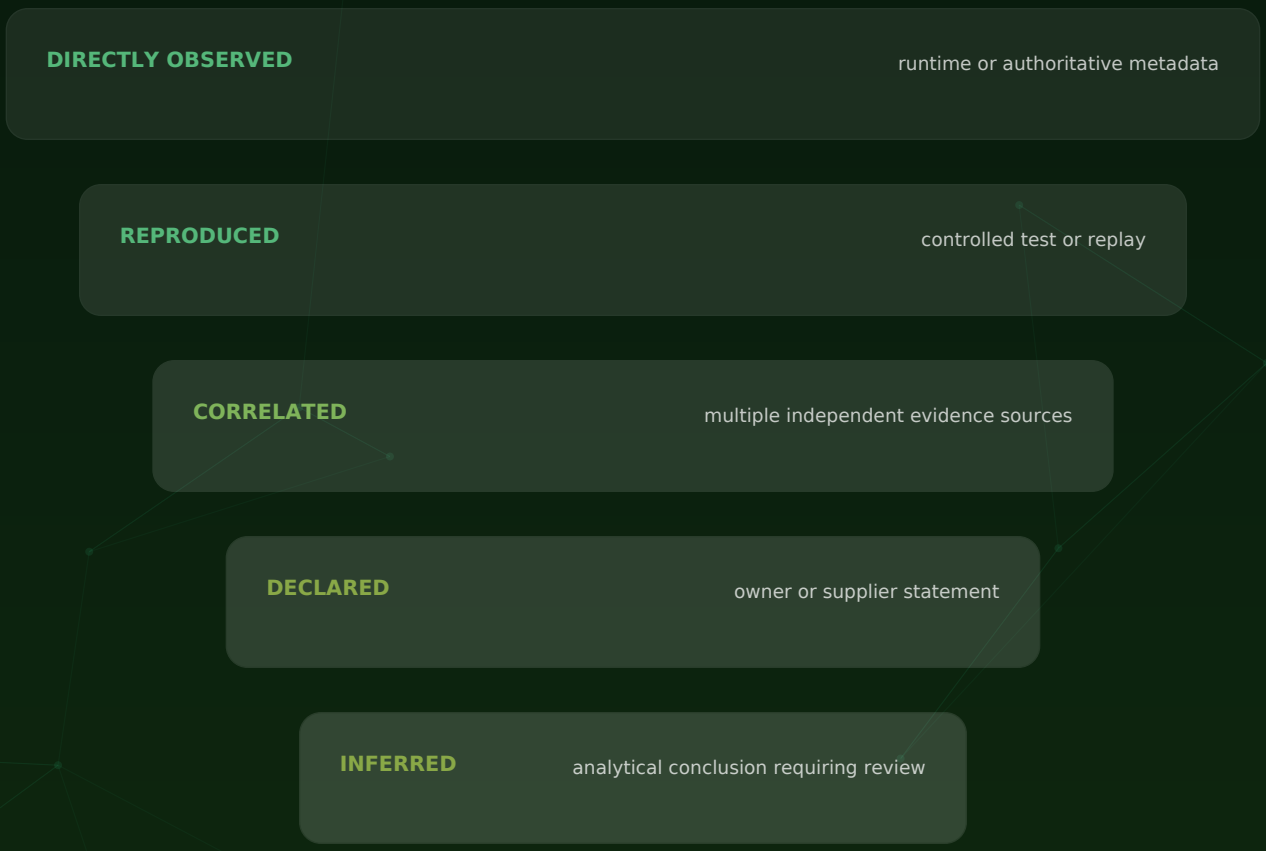
TRUST THE FINDING

Evidence confidence and provenance

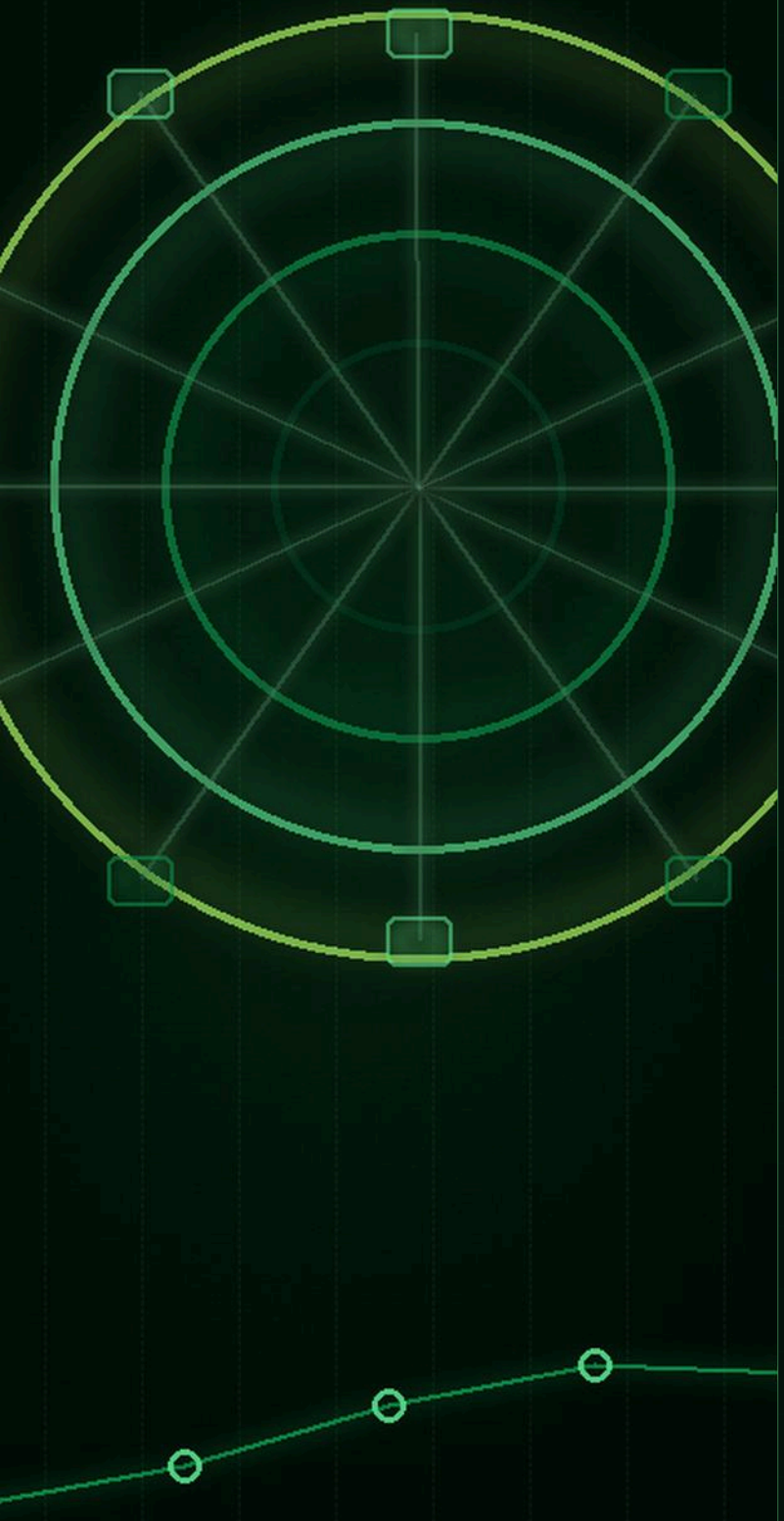
Decision-makers need to distinguish what was directly observed, what was inferred, what an owner declared, and what was reproduced under controlled validation.

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.



Sources: S08, Q01, Q04



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.**

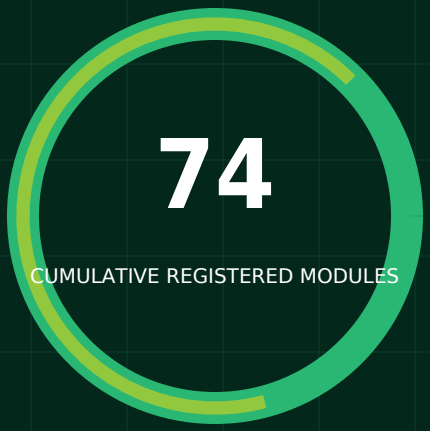
  Absence of internal or embedded cryptography, exploitability, production impact, classified mission context, supplier internals, secure implementation, or completed remediation without additional evidence and validation.

Original technical artwork: Qtonic Quantum.

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.



- **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.

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

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.

Sources: Q01, Q02, Q05 | Vendor-authored product definition

ALWAYS-ON CRYPTOGRAPHIC-RISK INTELLIGENCE

QScout Gold Pulse: 24/7/365 continuity

Company-reported operating cadence. QScout Gold 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.

Sources: Q01, Q02, Q09 | Vendor-authored product operating state

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

Original technical artwork: Qtonic Quantum.

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 THEATRICS

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

Sources: D01, Q04, Q06

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 pass documented acceptance gates for coverage, fidelity, traceability, secret exclusion, freshness, replay, graph integrity and reproducible rebuild. Record the accepting authority and limitations before applying results to 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.

Sources: Q04, D01, S07

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

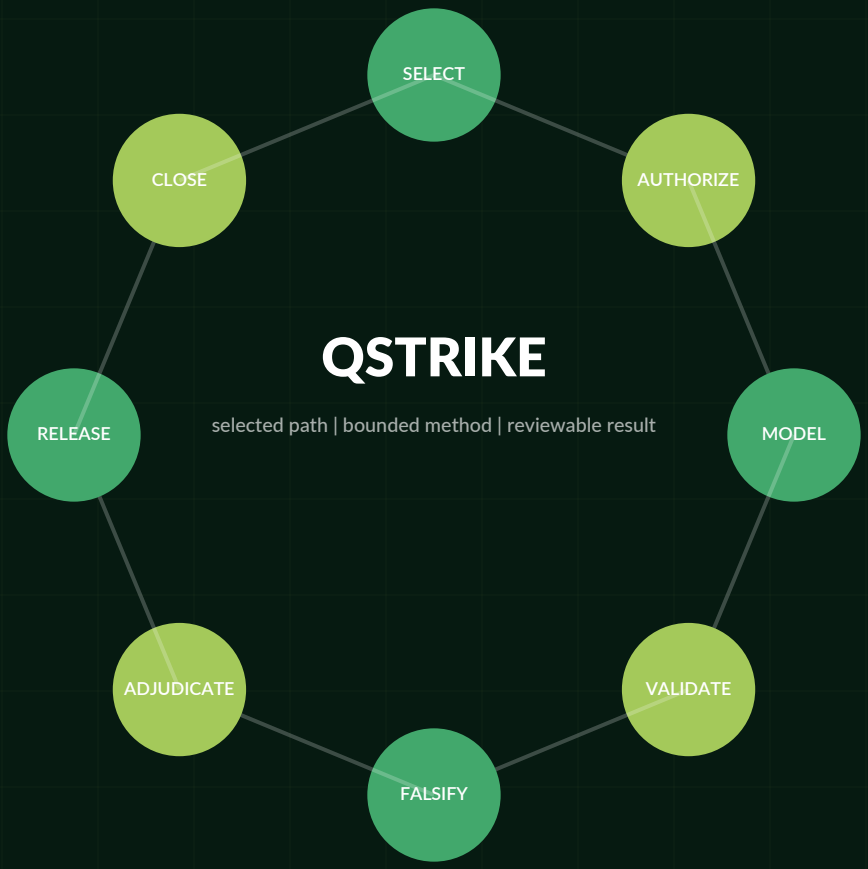
The owner sees the affected mission thread, security effect, duration, detectability, recovery path, dependencies, and operational workaround.

Sources: Q04, D01

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.

Sources: Q04, Q01, D01

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.

Sources: D01, N01, S04, Q04

ANNOUNCED AUGUST 19, 2026

QHunt

QHunt for the warfighter. Scoped mission and operational-technology cryptographic exposure assessment, with a decision and evidence handoff.

The default mission boundary is non-destructive. Targets, methods, exclusions and stop conditions are agreed before work. Restricted and air-gapped engagements operate inside the customer boundary.

MISSION-THREAD INTELLIGENCE

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

MISSION-OWNER QUESTIONS

Identify which cryptographic dependencies, supplier constraints and trust relationships prevent an accountable readiness decision.

SCOPED PROFESSIONAL SERVICE

Access follows the approved engagement. The current public boundary prohibits out-of-scope activity, credential guessing, protected-data access and stop-condition crossings.

EVIDENCE TO ACTION

Return findings tied to scope, evidence, limitations, owner decisions and remediation handoff. Any additional validation is defined in the statement of work.

QHunt is a professional service, not downloadable software. A CBOM is an engagement output. The earlier public sample is withdrawn and is not relied on as proof here.

MISSION ASSURANCE

From scope to decision.

AUTHORIZE

Define the mission and evidence boundary.

ASSESS

Record observations and limitations.

REVIEW

Tie findings to accountable owners.

DECIDE

Accept a remediation and verification path.

QHunt is a scoped professional service. Methods and outputs follow the engagement.

ILLUSTRATIVE TRUST PATH

Sources: Q06, Q10, Q11 | Current service and engagement boundary

FEDERAL AND MILITARY USE CASES

Where QHunt can create decision value

The strongest QHunt 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.

Original technical artwork: Qtonic Quantum.

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

Sources: D03, N03, Q06

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

Sources: D01, C01, Q06

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

Sources: Q04, S07, D01

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.

Sources: Q04, Q06, D01

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

Original technical artwork: Qtonic Quantum.

CHOOSE THE PROTECTED PATH

Transition architecture patterns

Choose a mechanism for each dependency. Record what it protects, what remains exposed, and the evidence that will allow retirement.

DIRECT REPLACEMENT

Move key establishment or signatures to the approved PQC mechanism when platform, profile and mission testing support it.

APPROVED HYBRID

Use only a reviewed composition. Test negotiation, interoperability, failure and downgrade; hybrid key exchange alone does not migrate signatures.

CRYPTOGRAPHIC SERVICE

Govern algorithms, keys, certificates, policy and updates through controlled interfaces where architecture and assurance permit.

TRANSITION OVERLAY

Identify the exact protected span and remaining endpoint trust. Require authority, measurable limits, an owner and a retirement gate.

RE-PROTECT / RE-SIGN

Protect future exposure and preserve provenance. This cannot erase copies already harvested or repair an untrusted historical record.

REPLACE / CONSTRAIN / RETIRE

Use replacement, isolation, restricted operation or retirement where upgrade is infeasible. Record residual risk and approval.

DOW ARCHITECTURE BOUNDARY

The strategy says PQC proxies should be avoided in place of actual upgrades. An overlay can be evaluated only within an approved transition plan; it does not automatically establish end-to-end migration.

SAFE/29 WITH QSHIELD v1.0 | COMPANY-REPORTED STATE

Qtonic Quantum reports SAFE/29 with QShield v1.0 as built and operating. This edition records that company statement. It does not treat an engineering specification alone as proof of a particular release or deployment.

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.

Sources: D01, N01, C01, S07

WHY QTONIC QUANTUM

One evidence system across the decision lifecycle

Choose Qtonic Quantum for quantum-risk priorities, scoped assessment, controlled validation and vendor-neutral migration decisions.

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 validation and QHunt mission assessment follow explicit scope. Methods, models, stop conditions and reviewable evidence are defined for the engagement.

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.

Sources: Q01, Q02, Q03, Q04, Q07 | Vendor-authored product positioning

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.

0-100

MOBILIZE + BASELINE

- Accountable authority and mission scope
- Automated and operator-reviewed inventory
- HNDL and trust-path priorities
- Immediate procurement controls
- First validation hypothesis

101-365

DESIGN + WAVE 1

- Approved target architectures
- Supplier commitments and evidence
- Representative path implemented
- Interoperability and mission test
- Signed acceptance package

366-700

SCALE PORTFOLIOS

- Approved patterns industrialized
- DIB and coalition transition waves
- Data re-protection and re-signing
- Portfolio metrics and exception aging
- Field evidence from representative missions

701-1,000

RETIRE + SUSTAIN

- Vulnerable fallback removed or accepted
- Exceptions closed, owned, or time-bounded
- Operations and sustainment transfer
- Recurring evidence and reassessment
- Mission performance and recovery proven

Migration complete means the approved profile protects the full path and lifecycle, with vulnerable fallback removed and mission performance verified. Report any remaining approved exceptions separately as migration with exceptions, with owner and expiry.

Sources: D01, D02, N01, S06, Q01, Q04, Q07

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.

Sources: D01, W02, Q01, Q02

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.

Sources: D01

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	Authentication exposure; verify negotiated key exchange and data lifetime.
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

SCOPE > PROVENANCE > VERSION / HASH > SIGN / ATTEST > CHANGE / CLOSURE

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

Sources: Q01, Q02, Q03 | Illustrative sanitized output

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.

Sources: Q07, D01, S06, S07, C03

SECURITY AND DELIVERY POSTURE

Evidence for the buyer decision

Separate the service boundary, deployment architecture, procurement route, cryptographic profile and acceptance evidence.

DEPLOYMENT IS SCOPED

Agree the hosting provider, region, tenant, data flow and control owner. A Marketplace purchasing route does not establish the runtime location.

RESTRICTED MISSION ENVIRONMENTS

Current engagement policy describes operator-to-operator assessment inside the customer boundary for air-gapped, restricted and on-premise systems.

CONTROLLED DILIGENCE

Request clearance-sponsorship information, current certification status, ownership records and the authorization pathway for the proposed engagement.

PROFILE-SPECIFIC ACCEPTANCE

Current QHunt CBOM policy specifies ML-DSA-65; CNSA 2.0 selects ML-DSA-87. Where applicable, require ML-DSA-87 in the contract and verify the delivered artifact, signer and release before acceptance.

DATA AND ACCESS

Specify evidence sources, permitted methods, residency, retention, deletion, release, access controls and incident handling before collection begins.

BUYING AND ACCEPTANCE

Use a direct contract or applicable Marketplace offer. Incorporate the supplier-neutral acceptance clauses on p.103 and agree the evidence for any required mission authorization.

STAFF ACCEPTANCE CHECK

A signature parameter is one requirement. Verify the authenticated key, exact signed bytes, implementation version and applicable module/profile evidence; record the accepting authority and unresolved exceptions.

Sources: Q03, Q10, N02, S02; procurement tool p.103 | Reviewed September 9, 2026

COMMAND JUDGMENT. OPERATOR ACCOUNTABILITY.

Leadership accountable to the mission

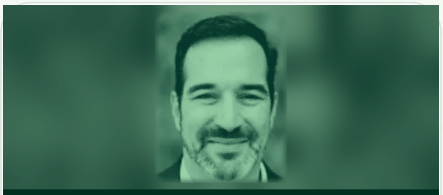
Mission standards, enterprise and cyber execution, allied readiness, doctrine, and national policy - with specialist capacity scoped only when an engagement requires it.

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

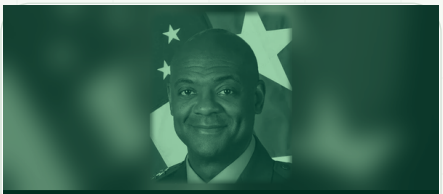
Cyber operations, enterprise security, and accountable decisions.

GOVERNS

Roger L. Cloutier Jr.

Founding Chair, Allied Defense Council

Coalition-readiness standards for allied cryptographic transition.



OPERATES / ADVISES

Milford H. Beagle Jr.

Senior Leader, Allied Defense Council

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.

Company team portraits used with permission. Council titles describe Qtonic Quantum private-sector responsibilities. Prior public roles confer no current official role or procurement authority.

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Sources: Q08 | Current profiles: qtonicquantum.com/leadership

SEPTEMBER 2026 ACTION BRIEF

Turn mission exposure into a buying path

Bring one consequential mission thread and one unanswered readiness question. Agree the evidence needed to make the next decision.

01

SCOPE ONE MISSION THREAD

Name the protected data, trust decision, systems and accountable owner. Agree the environment, safety boundary and evidence handling.

02

DEFINE THE PURCHASE

A scoped QScout assessment or mission engagement can connect evidence to selected validation and a QSolve migration decision. Timing and deliverables are agreed in the statement of work.

03

ACCEPT A DECISION PACKAGE

Require inventory, unknowns, priority rationale, owner, dependencies, next action and acceptance criteria. Buy a reviewable result tied to the mission.

FEDERAL PROCUREMENT PROFILE

UEI: FRYFAD3GW5W5
CAGE: 14E99
NAICS: 541512 / 541519
Company-provided; confirm status at purchase.

FEDERAL AND DEFENSE GOVERNMENT AFFAIRS

Reginald M. Harris
Managing Director of Government Affairs
Joined announcement: September 1, 2026.
Former Chief of Staff, U.S. Army Cyber Command. [Q08, Q12]

START THE CONVERSATION

J. Nathaniel Ader | Co-Founder and Chief Innovation Officer
jna@qtonicquantum.com | 305-268-2626
qtonicquantum.com/contact | +1 (866) 4-QTONIC

Sources: Q01, Q06, Q07, Q08, Q12 | Reviewed September 9, 2026

PRIMARY AND OFFICIAL SOURCES

Evidence register

Click any entry. New September claims are linked to primary publications; source status and scope are stated on the relevant pages.

D01	DoW PQC Strategy	S01	NIST FIPS 203 - ML-KEM	C04	G7 PQC call to action (Sept 3)	Q02	QScout methodology and product boundary
D02	DoW migration-preparation memo	S02	NIST FIPS 204 - ML-DSA	C05	NSA: active Siemens S7 threats (Aug 19)	Q03	Qtonic Quantum Trust Center
D03	Department of Defense Zero Trust Strategy	S03	NIST FIPS 205 - SLH-DSA	W01	Executive Order 14412 - Federal Register	Q04	Qtonic Quantum QStrike
D04	Zero Trust Capability Execution Roadmap v1.1	S04	NIST SP 800-227 - KEM recommendations	W02	OMB M-26-15 (June 24, 2026)	Q05	QScout market and evidence boundary
D05	U.S. Army Unified Network Plan 2.0	S05	NIST IR 8547 initial public draft	W03	NSM-10 - Quantum leadership and risk	Q06	QHunt current service boundary
D06	Army FY2026 tactical-network budget material	S06	NIST CSWP 39upd1 - Crypto agility	W04	OMB M-23-02 - Migrating to PQC	Q07	Qtonic Quantum QSolve
D07	Cybersecurity guidance for LEO SATCOM	S07	NIST NCCoE Migration to PQC project	W05	NSPM-12 - NSS cybersecurity governance	Q08	Qtonic Quantum leadership
D08	CMMC Phase II suspension (July 13)	S08	NIST SP 1800-38B preliminary draft	W06	National Security S&T Strategy (Aug 2026)	Q09	QScout Gold Pulse 24/7/365 launch
N01	NSA Post-Quantum Cybersecurity Resources	S09	NIST SP 800-208 - Stateful hash signatures	G01	GAO-26-107759 - Updating the National Strategy	Q10	Current engagement policy (Aug 19)
N02	CNSA 2.0 FAQ v2.1 (Dec 2024)	S10	NIST PQC project / standards status	G02	GAO-25-107703 - Quantum Threat Mitigation Strategy	Q11	QHunt launch publication record
N03	CNSSP 15 (March 4, 2025) directory	S11	NIST CMVP transition / FAQ	G03	GAO-25-108590 - Cyber Threat Mitigation Testimony	Q12	Harris government-affairs appointment
N04	NSA Zero Trust Implementation Guideline Primer	C01	CISA/NSA/NIST Quantum-Readiness guide	A01	TechNet Augusta 2026 official conference site	R01	IonQ full-stack ECC estimate (Sept 4)
N05	NSA Embracing a Zero Trust Security Model	C02	CISA Post-Quantum Considerations for OT	A02	TechNet Augusta official FAQ, venue, theme	R02	QuEra AI laser-control pilot (Aug 27)
N06	NIAP Policy Letter 33 (Aug 31)	C03	CISA PQC product categories	Q01	Qtonic Quantum QScout		

Source key: D defense | N NSA/CNSS | S NIST | C CISA/G7 | W executive policy | G GAO | A conference | Q company | R research

Research and status review through September 9, 2026. Company sources establish company statements only. Historical sources remain for the unchanged fundamentals; current requirements must be checked against the applicable authority.

QTONIC QUANTUM

POST QUANTUM READY

SECURE THE MISSION. CONTROL THE TRANSITION.

Find with QScout. Sustain with QScout Gold Pulse. Validate with QStrike. Assess with QHunt. Fix with QSolve.

Bring one mission thread. Leave with a decision path.

Applicable Marketplace offer or direct | Company-offered references under NDA

SEPTEMBER 9, 2026 | RESEARCH AND ACCEPTANCE EDITION

QHunt serves scoped mission and OT engagements. QScout Gold Pulse tracks the agreed external surface and configured evidence sources. Delivery, service levels, access and acceptance are defined by the engagement.

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

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

ORIGINAL RESEARCH | QQ-PQC-LOCAL-2026-09

Budget the bytes. Preserve the tail.

Inherited Qtonic publication experiment. Recomputed from retained observations for this edition; no new measurements collected.

6
PARAMETER SETS

6,000
VALID CYCLES

18,000
OPERATION TIMINGS

Parameter set	Public key (B)	Ciphertext / signature (B)	Combined (B)
ML-KEM-512	800	768	1568
ML-KEM-768	1184	1088	2272
ML-KEM-1024	**1568**	**1568**	**3136**
ML-DSA-44	1312	2420	3732
ML-DSA-65	1952	3309	5261
ML-DSA-87	**2592**	**4627**	**7219**

All observed lengths matched FIPS 203 Table 3 or FIPS 204 Table 2. Combined values are arithmetic sizing aids, not measured packets, certificate chains or handshakes.

METHOD | SEPTEMBER 7, 2026

pqcrypto 0.3.4; one CPU-pinned shared Linux container. Five blocks of 200 cycles per parameter set after 20 excluded warm-ups. Timings include Python/CFFI overhead. AI-assisted publication measurements; no product, field-system or FIPS-validation claim.

TURN A MEASUREMENT INTO AN ACCEPTANCE TEST

ML-DSA-87 signing: 648.1 microseconds median; 1,802.6 microseconds nearest-rank p95. Set a target-system tail-latency requirement and test it under the intended workload. Where CNSA 2.0 applies, use the required 1024/87 profile.

Fresh dedicated 1024/87 measurements: p.105. Earlier observations remain unchanged.

ORIGINAL RESEARCH | QQ-TLS-LOCAL-2026-09

One handshake. Three facts to verify.

Key exchange, authentication and bulk encryption answer different questions. The retained hello messages make the byte accounting inspectable.

Server identity	Key exchange	TLS record bytes	Completed
ECDSA P-256	X25519	1,029-1,031	20 / 20
ECDSA P-256	X25519MLKEM768	3,351-3,353	20 / 20
RSA-2048	X25519	1,613	20 / 20
RSA-2048	X25519MLKEM768	3,935	20 / 20

All four configurations reported TLS_AES_256_GCM_SHA384. Hybrid key exchange retained classical authentication. Record the cipher suite, negotiated group and certificate/signature behavior separately.

THE HELLO-MESSAGE BYTE LEDGER

2,272	+ 36	+ 14	= 2,322
SELECTED FIELDS	EXTRA SHARE	GROUP IDS	OBSERVED GROWTH

The extra 50 bytes came from this OpenSSL configuration. Budget the complete configured exchange, not only the selected key-share fields.

METHOD | SEPTEMBER 8, 2026

80 fresh TLS 1.3 handshakes: 20 per configuration. Python 3.12.13 / OpenSSL 3.5.7; in-memory SSL, no network sockets. Server certificate and report.invalid hostname verified; synthetic data exchanged. One lab leaf certificate; no resumption; tickets disabled.

MILITARY ACCEPTANCE BOUNDARY

This ML-KEM-768 hybrid study is not a CNSA 2.0 profile demonstration. It measures no network latency, throughput, production chains or field interoperability. Require profile-specific target-system tests.

Fresh 1024 exchange / ML-DSA-87 authentication: p.106. Bandwidth model: p.107.

Sources: Flagship build 13 pp.41,44-45; embedded TLS archive; RFC 10024 | Reviewed September 9, 2026

BUYER WORK PRODUCT | DRAFT CONTRACT LANGUAGE

Make the evidence part of acceptance.

Six supplier-neutral requirements. Adapt to the engagement and applicable procurement rules; obligations begin when incorporated into an executed agreement.

01 STRUCTURE AND SCOPE

Require machine-readable CycloneDX 1.7 JSON or a later version agreed in writing. Include scope, observation dates, population, collection methods and schema version. Exclude credentials and private keys.

02 ORIGIN AND INTEGRITY

Require SHA-256, a detached signature, public verification key, signer identity, authenticated key source, parameters and the exact signed byte representation.

03 REPRODUCIBLE VERIFICATION

Require the pinned schema, tool versions, executable instructions and actual verification receipt, including failed checks. The buyer must reproduce schema, digest and signature checks.

04 COVERAGE AND GAPS

Reconcile to the agreed population and denominator. Identify inaccessible assets, unsupported paths, inferred values, stale observations and missing relationships. Schema and signature validity do not prove coverage.

05 DECISIONS AND PORTABILITY

Map material dependencies to a service, owner, protection objective, blocker and prioritized action. Supply field definitions and relationships sufficient for reuse outside the supplier platform.

06 ACCEPTANCE AND RENEWAL

Combine technical checks with buyer review of coverage, gaps and decisions. Assign exceptions, refresh triggers, cadence and key-change handling. Require corrected, versioned records.

MILITARY PROFILE ADDENDUM

The frozen sheet defaults to ML-DSA-65 or another scheme agreed in writing. Where CNSA 2.0 applies, specify ML-DSA-87 as required and verify release-specific deliverables before acceptance. The default is not evidence of CNSA 2.0 compliance.

Sources: Frozen CBOM acceptance sheet (embedded); N02; Q10 | Reviewed September 9, 2026

RESEARCH PROVENANCE | EXACT EMBEDDED ORIGINALS

Carry the originals. Verify the record.

Three files, unchanged from the flagship. Each was extracted, byte-compared, hashed and checked before integration into this edition.

01 PRIMITIVE STUDY | 18,000 RETAINED TIMINGS

Qtonic_Quantum_Original_Research_Q4_2026.zip

SHA-256

ebb8cb716dc568dfb70cca04f5f89ebcb2cf74b9b3a75451b7ffeeec62eef6f4

02 TLS STUDY | 80 RETAINED HANDSHAKES

Qtonic_Quantum_TLS_Proof_Study_Q4_2026.zip

SHA-256

d5728e297dab86ad884baf1815876545dad976f41f3274d14c9282a989df8a20

03 CBOM ACCEPTANCE | SIX SUPPLIER-NEUTRAL CLAUSES

Qtonic_Quantum_CBOM_Acceptance_Requirements.pdf

SHA-256

e62f5978dd72a4b3d48882fbe4f4440761ac913146e8d3f3ac9862ffbe41f13c

REPRODUCE THE PUBLISHED NUMBERS

Save all three files from a desktop PDF reader's Attachments panel; some browser viewers hide attachments. Check the hashes, extract each ZIP separately and read its README. From the relevant extracted folder, run:

Primitive folder: python3 -I recompute.py

TLS folder: python3 -I recompute_tls.py

Both recomputations passed for this edition. This verifies retained observations, not a new experiment or a Qtonic product. Frozen README page references point to the original flagship. Company study provenance: Q4 2026 flagship, build 13, pp.41-45.

Fresh mission-profile bundle: p.108. These three earlier originals remain unchanged.

FRESH RESEARCH | QQ-MISSION-PRIMITIVES-2026-09-09

Measure the required parameters.

Fresh collection centered on ML-KEM-1024 and ML-DSA-87. No observation rows were imported from the earlier experiment on page 101.

2,000
VALID CYCLES

6,000
FRESH TIMINGS

1,000
SAMPLES / OPERATION

Parameter set	Operation	Median (µs)	p95 (µs)
ML-KEM-1024	Key generation	136.6	206.4
ML-KEM-1024	Encapsulation	149.2	205.2
ML-KEM-1024	Decapsulation	176.2	247.3
ML-DSA-87	Key generation	390.5	534.4
ML-DSA-87	Signing	1,026.9	2,890.8
ML-DSA-87	Verification	412.0	539.0

METHOD | SEPTEMBER 9, 2026, 17:31 UTC

Five blocks × 200 cycles per parameter set; algorithm order randomized within each block. Twenty excluded warmups each. Python 3.12.14 / pqcrypto 0.3.4 / CFFI 2.1.1; CPU 0 pinned on a shared Intel Xeon Platinum 8370C host. Python/CFFI overhead included; garbage collection disabled; no trimming. p95 uses nearest rank. All encapsulation/decapsulation and signature checks passed.

OBSERVED LENGTHS

ML-KEM-1024 public key / ciphertext: 1,568 / 1,568 B. ML-DSA-87 public key / signature: 2,592 / 4,627 B; 1,024-byte signed message. These lengths are not packet sizes.

MAKE THE TAIL AN ACCEPTANCE REQUIREMENT

The observed ML-DSA-87 signing p95 was 2.891 ms. Set the signing workload, device, concurrency and tail-latency gate for the intended system; repeat there. This shared-container sample is not a field-device forecast, comparative product benchmark or validated-module claim.

Sources: New embedded mission bundle; FIPS 203 Table 3; FIPS 204 Table 2 | Reviewed September 9, 2026

FRESH RESEARCH | QQ-MISSION-TLS-2026-09-09

Measure authentication, too.

Six configurations separate exchange overhead from identity overhead. The ML-DSA-87 rows close the earlier study's classical-authentication gap.

Server identity	Key exchange	TLS record bytes	Verified runs
ECDSA P-384	P-384	2,133–2,135	20 / 20
ECDSA P-384	Hybrid 1024	5,007–5,009	20 / 20
RSA-3072	P-384	3,591	20 / 20
RSA-3072	Hybrid 1024	6,465	20 / 20
ML-DSA-87	P-384	20,699	20 / 20
ML-DSA-87	Hybrid 1024	23,573	20 / 20

Hybrid 1024 = SecP384r1MLKEM1024 (0x11ED). All used TLS_AES_256_GCM_SHA384. ECDSA and RSA authentication remain classical; the ML-DSA-87 rows test post-quantum server authentication.

OBSERVED HELLO GROWTH: 2,874 B

3,136 B of additional key-share fields − 254 B padding − 8 B EC-format extension = 2,874 B net growth. Hybrid ClientHello / ServerHello: 1,818 / 1,755 B. Actual configured messages determine the budget.

ML-DSA-87 CHAIN + AUTHENTICATION

Transmitted leaf 7,566 B + intermediate 7,539 B = 15,105 B DER. The trusted 7,531 B root was not sent. CertificateVerify signature: 4,627 B. Whole-handshake flights: 1,823 client / 21,670 server / 80 client bytes.

METHOD | SEPTEMBER 9, 2026, 17:33 UTC

120 in-memory TLS 1.3 handshakes; OpenSSL 3.5.8 / Python 3.12.14. Root–intermediate–leaf test chains; server identity and hostname verified. Six negative certificate controls rejected; application data passed both directions. No sockets, resumption, tickets, mutual TLS or HelloRetryRequest.

Twenty runs check byte repeatability: four fixed-length configurations; ECDSA varies by 2 B. No TLS timing claim.

DRAFT RISK AND ACCEPTANCE BOUNDARY

The binding is draft-05 (expires January 7, 2027); it can change. Track the final specification and recheck interoperability before deployment. IANA already assigns mldsa87 = 0x0906. These implementation measurements do not establish CNSA 2.0 deployment approval, module validation or field interoperability.

Sources: New mission TLS archive; RFC 10024; RFC 9846; TLS ML-DSA draft-05; NSA FAQ v2.1 | Reviewed September 9, 2026

DERIVED MODEL | MEASURED BASIS, EXPLICIT ASSUMPTIONS

Budget the complete handshake.

The observed configuration anchors the model. Change chain length, certificate sizes, MTU and rate in the included worksheet; validate the result on the target system.

MEASURED INPUT | ONE TRANSMITTED INTERMEDIATE

23,573 TLS record bytes

ML-DSA-87 + hybrid 1024; observed client / server / client flights: 1,823 / 21,670 / 80 B.

DERIVED MODEL | SELECTED MTUs AND RATES, NOT NETWORK MEASUREMENTS

Illustrative IP MTU	TCP data (B)	Segments C / S / C	TLS + IP/TCP (B)
IPv4 / 1500	1,460	2 / 15 / 1 = 18	24,293
IPv6 / 1280	1,220	2 / 18 / 1 = 21	24,833
IPv4 / 576	536	4 / 41 / 1 = 46	25,413

Segments = sum of ceil(flight bytes / TCP payload). Fixed headers: IPv4 20 + TCP 20 B; IPv6 40 + TCP 20 B. Pack each flight separately. Actual TCP may use more segments.

Illustrative data rate	TLS serialization floor	IPv4/1500 + TCP floor
9.6 kbit/s	≥ 19.644 s before RTT / loss / ARQ	≥ 20.244 s before RTT / loss / ARQ
64 kbit/s	≥ 2.946 s before RTT / loss / ARQ	≥ 3.036 s before RTT / loss / ARQ
256 kbit/s	≥ 0.736 s before RTT / loss / ARQ	≥ 0.759 s before RTT / loss / ARQ

Floors are rounded down to 0.001 s. They exclude processing, TCP setup / ACKs, options, tunnels, FEC and duty-cycle delays. These are sizing bounds, not measured latency.

CHAIN SENSITIVITY | MODELED, NOT A NEW HANDSHAKE

One more 7,539 B DER intermediate adds 7,566 TLS B: 7,544 B entry + 22 B new record. IPv4/1500 segments rise 18 to 24. Assumes 16,384 B content fragments, no padding, compression or entry extensions; other records stay fixed. Use your chain sizes in the included worksheet (p.108).

MISSION PLANNING DECISION

These are TCP data segments, not IP fragments or evidence that PQC cannot fit a radio. Test the intended chain, MTU, path rate, loss and duty cycle. Illustrative settings do not represent a named radio or SATCOM service.

Sources: Mission bundle / budget + sensitivity; RFC 9846 §§4.5.1, 5.2; RFC 9293 §3.7; RFC 8200 §5 | Reviewed September 9, 2026

RESEARCH PROVENANCE | FOURTH EMBEDDED EVIDENCE FILE

Reproduce the mission evidence.

The new archive travels with the report. Its file hashes bind the published numbers to the measurements and assumptions that produced them.

04 FRESH MISSION-PROFILE EVIDENCE BUNDLE

Qtonic_Quantum_Mission_Profile_Evidence_2026-09-09.zip

2,823,929 bytes | SHA-256

be793fac61687d7ee585cdea9eadebbb7bd4c5ca5d3973e6684a75ad41094046

Includes both study ZIPs, the baseline model, chain sensitivity and an editable bandwidth worksheet.

NESTED ARCHIVE HASHES

Primitive study | 6,000 fresh timings

9f1edbdbeaf7b889a4a40471573e513c0bd2cd45721b2ed1ff174629b0c741a7

TLS profile study | 120 fresh handshakes, all raw transcripts

595f503f7ab163903610ef27d37b307717ac57e9a85b5200948d0a49bafdf549

RECOMPUTE THIS EDITION

Save the mission-profile ZIP from the PDF Attachments panel (some browser readers hide it). Check its SHA-256 and extract. Open the Excel file in worksheet/ to change inputs. Read README.md and inspect the scripts, then run:

```
python3 -I verify_bundle.py
```

Python standard library only; offline. Checks both studies, 120 raw TLS flights, 18 baseline budget rows and 38 chain-sensitivity vectors. Workbook formulas were separately checked against all 38 vectors. Longer chains are modeled; no new handshake was collected for this clarification.

PROVENANCE IS AN ACCEPTANCE DELIVERABLE

Measurements were collected on September 9, 2026 with AI-assisted publication harnesses. The two nested study ZIPs and three original files on p.104 remain unchanged. This bundle adds a derived sensitivity model and worksheet. RFC 9846 supersedes RFC 8446; its certificate and record sections support the added sizing ledger.