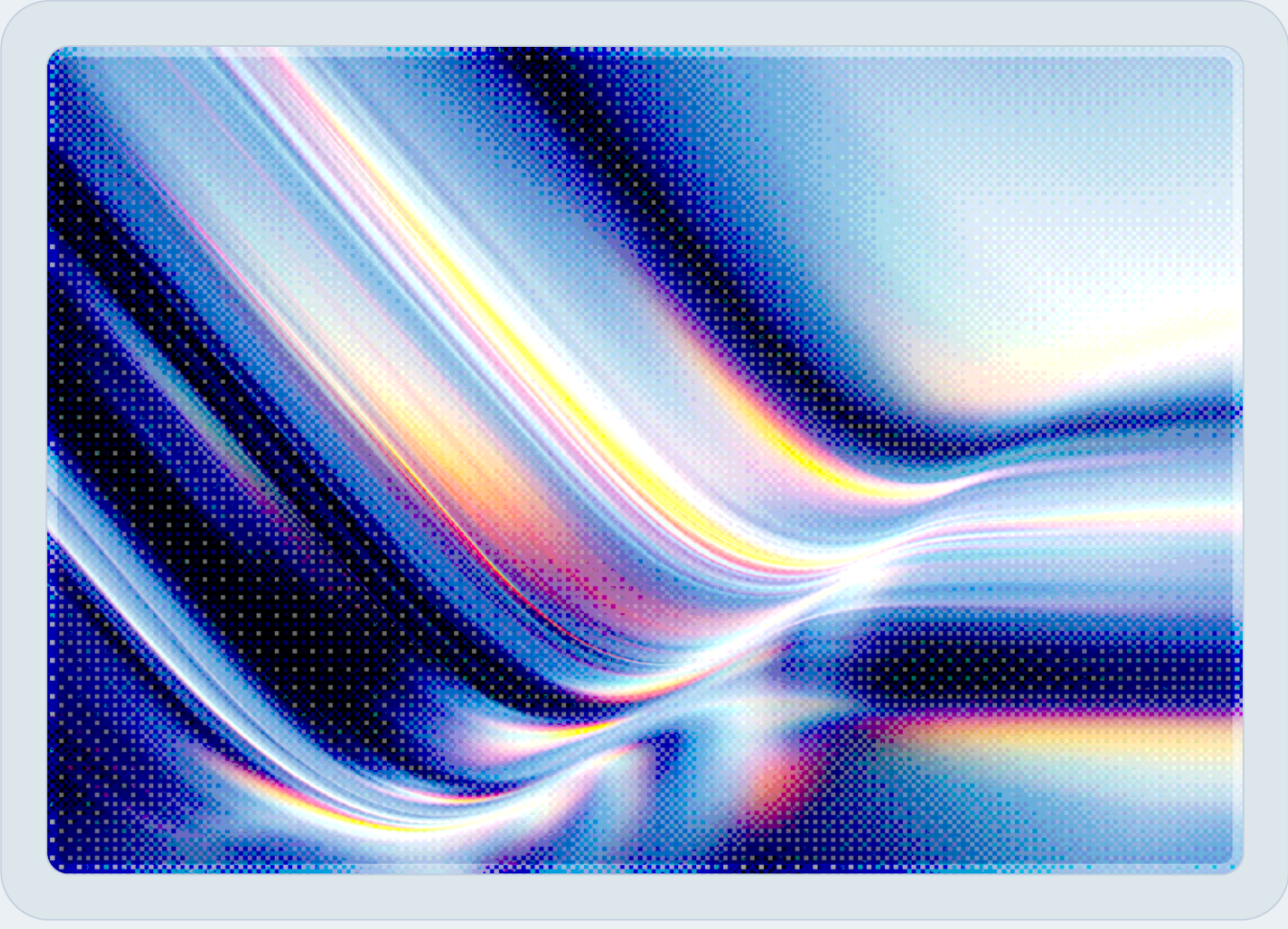
CSAI Foundation | Cloud Security Alliance

The Quantum Executive Orders of June 2026

A CSA Analysis and Cybersecurity Roadmap for CISOs, Software and AI Companies, and the Infrastructure Ecosystem

2026-06-22

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Table of Contents

Executive Summary

On June 22, 2026, the President signed two executive orders that together reposition quantum information science at the center of United States technology and national-security policy. The first, *Ushering in the Next Frontier of Quantum Innovation* (Executive Order 14411), is an offensive industrial-strategy order: it directs a whole-of-government push to build a national quantum computing capability, strengthen domestic supply chains, expand the quantum workforce, and protect American research from foreign acquisition. The second, *Securing the Nation Against Advanced Cryptographic Attacks* (Executive Order 14409), is its defensive counterpart: it commits the federal government to migrate its information systems to post-quantum cryptography on a fixed schedule and, for the first time, extends concrete cryptographic obligations to federal contractors through the acquisition system. Read together, the two orders express a single strategic judgment — that the same technology the nation intends to lead in building will, in adversary hands, break the cryptography that protects nearly all digital communication and stored data.

For the security community this is less a surprise than a ratification. The cryptographic transition these orders accelerate has been underway since the National Institute of Standards and Technology (NIST) finalized its first three post-quantum standards — FIPS 203, 204, and 205 — in August 2024, and it rests on a policy foundation laid by the 2022 Quantum Computing Cybersecurity Preparedness Act, National Security Memorandum 10, and the National Security Agency's Commercial National Security Algorithm Suite 2.0. The Cloud Security Alliance's Quantum-Safe Security Working Group has been publishing migration guidance, governance mappings, and practitioner resources throughout this period. What the June 2026 orders change is not the science or the standards, both of which are settled, but the schedule and the reach: the orders convert a recommended migration into a dated obligation with deadlines beginning at the end of the decade, and they pull the private sector into scope through critical-infrastructure coordination and the Federal Acquisition Regulation.

The central message of this paper is that the binding constraint on quantum readiness is no longer the availability of algorithms; it is organizational execution. The decisive capabilities are a complete and continuously maintained cryptographic inventory, genuine crypto-agility in products and architectures, and a governance model that treats cryptographic dependency as a managed enterprise risk rather than an implementation detail. The "harvest now, decrypt later" threat means that data with a long confidentiality lifetime is already exposed today, regardless of when a cryptographically relevant quantum computer actually arrives, so the migration cannot wait for certainty about "Q-Day." This paper analyzes both orders, situates them within the existing regulatory framework, explains why their effects reach well beyond federal agencies, and provides specific recommendations for chief information security officers, software companies, artificial-intelligence companies, network-infrastructure providers, cloud-service providers, and

critical-infrastructure operators. It closes by mapping the work ahead to the Cloud Security Alliance resources — from the AI Controls Matrix to the Quantum-Safe Security body of work — that organizations can use to execute it.

Two Orders, One Inflection Point

It is tempting to treat the June 2026 orders as a single quantum announcement, but their division of labor matters. The *Innovation* order is concerned with building capability and protecting the means of producing it; the *Cryptographic Security* order is concerned with surviving the consequences of that capability falling into adversary hands. The first order treats quantum computing as an opportunity to be seized, the second treats it as a threat to be managed, and the security ecosystem sits squarely at the intersection. An organization that reads only the headline about a powerful new government quantum computer, and misses the companion order that sets cryptographic migration deadlines, will have absorbed exactly the wrong half of the policy.

The orders also signal a shift in posture from encouragement to obligation. Prior federal action on post-quantum cryptography was real but largely hortatory for anyone outside national-security systems: agencies were told to inventory their cryptography and prepare to migrate "as soon as practicable," and contractors were affected only indirectly and eventually. The *Cryptographic Security* order replaces much of that conditional language with calendar dates and assigns named accountability inside each agency. For the private sector the relevant change is that the order directs the Federal Acquisition Regulatory Council to amend procurement rules so that covered contractors must comply with NIST's post-quantum standards by a date certain, and it directs sector risk-management agencies to work through the Cybersecurity and Infrastructure Security Agency (CISA) to help critical-infrastructure owners and operators build their own migration plans. The federal government is using the two levers it most reliably controls — what it buys and what it regulates — to move the surrounding ecosystem.

What the Executive Orders Actually Say

Ushering in the Next Frontier of Quantum Innovation (Executive Order 14411)

The *Innovation* order establishes a policy of maintaining a strategic technical advantage in quantum information science and building a trusted quantum ecosystem spanning research, manufacturing, commercialization, and application. Its most concrete initiative is a federal effort to develop and field a large-scale quantum computer for scientific discovery, delivering at least one such machine to a Department of Energy facility and, where possible, making it available to the broader scientific community.

Around this centerpiece the order arranges a familiar set of industrial-policy instruments: an updated national quantum strategy due within 180 days, advance-market-commitment and prize-challenge mechanisms to stimulate domestic supply, expanded foundry access and user facilities, a reconstituted advisory committee, and a workforce program that tasks the Office of Personnel Management, the Department of Labor, and the National Science Foundation with recruiting, training, and even defining the occupational categories of a quantum workforce.

For security professionals the order's most important provision is comparatively quiet. It directs the Director of National Intelligence and the Secretary of War, in coordination with the relevant subcommittee and other departments, to identify within one year the national-security implications of the increasing scale and performance of commercial quantum computers — explicitly including the implications for migration to post-quantum cryptography — and to report annually thereafter. In other words, the order that is ostensibly about building quantum capability contains a standing requirement to assess how close that capability is bringing the world to a cryptographically relevant quantum computer, and to feed that assessment back into the migration timeline. This is the mechanism by which the optimistic, capability-building order and the defensive, cryptography-protecting order remain coupled over time.

Securing the Nation Against Advanced Cryptographic Attacks (Executive Order 14409)

The *Cryptographic Security* order opens with a plain statement of the threat: large-scale quantum computers, particularly in adversary hands, will pose a significant threat to widely used cryptographic systems, and adversaries are assumed to be collecting encrypted United States information now in order to decrypt it later once such computers exist. From that premise the order commits the federal government to transition its information systems to NIST-approved Federal Information Processing Standards for post-quantum cryptography, and it puts dates on that transition.

The order's operative deadlines fall into two categories: fixed calendar dates for the migration itself, and shorter clocks for the guidance and rulemaking that enable it. The migration dates apply to the government's most sensitive systems — its High Value Assets and high-impact systems — and distinguish between the two cryptographic functions that must be replaced. The enabling actions reach further, into module validation, acquisition rules, vulnerability disclosure, and a new cryptographic bill of materials that will make cryptographic dependencies discoverable in the way a software bill of materials makes software dependencies discoverable. The following table consolidates the order's principal provisions.

Provision	Responsible entity	Timeline
Designate an agency PQC Migration Lead responsible for cryptographic inventory and a prioritized migration plan	Each agency head	Within 30 days
Issue detailed migration guidance to agencies	OMB, with CISA and the National Cyber Director	Within 90 days
Accelerate cryptographic module validation processes	NIST	Within 180 days
Report on National Security Systems migration	NSA	Within 180 days, then annually
Amend the FAR to require covered contractors to comply with NIST post-quantum FIPS	FAR Council	Proposed rule within 180 days; contractor compliance by Dec 31, 2030
Amend the FAR to require contractor vulnerability-disclosure policies covering cryptographic weaknesses and non-FIPS algorithms	FAR Council	Proposed rule within 270 days
Issue guidance for a Cryptographic Bill of Materials (CBOM)	DHS/CISA with NIST	Within 270 days
Initiate and complete a NIST internal PQC migration pilot	NIST	Initiate within 180 days; complete by Dec 31, 2027
Transition High Value Assets and high-impact systems to PQC for key establishment	All covered agencies	By Dec 31, 2030
Transition High Value Assets and high-impact systems to PQC for digital signatures	All covered agencies	By Dec 31, 2031

Provision	Responsible entity	Timeline
Assist critical-infrastructure owners and operators with PQC migration planning	Sector Risk Management Agencies via CISA	Ongoing
Encourage foreign governments and industry to adopt NIST-standardized PQC	Department of State and partners	Ongoing

Two features of this structure deserve emphasis. First, the order separates the deadline for key establishment from the deadline for digital signatures, giving the latter an extra year. This reflects a real operational asymmetry that practitioners have already encountered: vendor support for the key-encapsulation standard, ML-KEM, has matured considerably faster than support for the signature standards, producing what the community has begun to call the "signature gap." Sequencing the mandates acknowledges that the ecosystem can deliver confidentiality protection sooner than it can deliver authentication and integrity protection at scale. Second, the order does not impose its own migration deadline directly on private enterprises; instead it works through the acquisition system and critical-infrastructure coordination. The practical effect, however, is broad, because the population of organizations that sell to the federal government or operate critical infrastructure encompasses much of the technology economy.

The Threat: Q-Day, Harvest Now, and the Asymmetry of Time

The phrase "harvest now, decrypt later" captures why this transition cannot be deferred until a quantum computer capable of breaking public-key cryptography demonstrably exists. Most security investments defend against threats that must be present to cause harm; this one defends against a future capability acting on data captured today. An adversary that records encrypted traffic or exfiltrates encrypted archives now can simply store the ciphertext and wait. When a cryptographically relevant quantum computer eventually runs Shor's algorithm against the RSA and elliptic-curve systems that protect that data, the confidentiality of everything harvested in the interim collapses retroactively. The relevant question for a defender is therefore not "when will Q-Day arrive?" but "how long must this data remain confidential, and does that lifetime extend past the plausible arrival of the threat?"

Expert estimates for the arrival of a cryptographically relevant quantum computer cluster in the 2030s, with meaningful uncertainty in both directions. That range is comfortably inside the confidentiality horizon of a great deal of sensitive information: trade secrets, source code, cryptographic keys and credentials, health

and genomic records, financial and legal records, classified and controlled information, and the long-lived signing keys that anchor software supply chains. For any data whose value persists ten or fifteen years, the harvest-now threat is not a future risk but a present one, and the federal migration deadlines of 2030 and 2031 are best read as the latest defensible dates rather than as early ones. The data most exposed is precisely the data an organization most wants to protect, which is why a migration program should begin by identifying high-confidentiality, long-lived data flows rather than by trying to replace all cryptography uniformly.

A second asymmetry compounds the first. Cryptographic migration is slow because cryptography is embedded everywhere and is usually invisible until it breaks — buried in protocol libraries, hardware security modules, firmware, certificates, embedded devices, and third-party products whose internals the operator cannot see. Historical transitions away from broken primitives such as SHA-1 took many years even when the replacement was well understood and the change was comparatively local. The post-quantum transition is larger in every dimension: it touches both key establishment and digital signatures, it changes key and signature sizes enough to affect protocol behavior and performance, and it must propagate through supply chains that no single organization controls. The lesson the security community has drawn, and that the executive orders implicitly accept by setting deadlines years in advance, is that an organization that waits for certainty will not have time to act on it.

A CSA Perspective: Reading the Orders Against the Existing Framework

The June 2026 orders did not arrive on an empty field. They sharpen and accelerate a framework that has been assembling for several years, and understanding that framework is essential to acting on the orders correctly rather than treating them as a standalone mandate. The Quantum Computing Cybersecurity Preparedness Act of 2022 established the statutory expectation that federal agencies inventory their cryptography and migrate on a prioritized basis once standards existed. National Security Memorandum 10, issued the same year, set the national goal of achieving quantum resistance to the maximum extent feasible by 2035 and has been preserved across administrations. The Office of Management and Budget's memorandum M-23-02 operationalized the inventory requirement, directing agencies to catalog quantum-vulnerable systems and report on them. On the national-security side, the NSA's CNSA 2.0 has for several years specified the concrete algorithms and the aggressive timelines that apply to national-security systems and their vendors, with software and firmware signing and networking equipment expected to be exclusively quantum-resistant by 2030.

The technical foundation matured in parallel. NIST finalized FIPS 203 (ML-KEM) for key encapsulation, FIPS 204 (ML-DSA) for primary digital signatures, and FIPS 205 (SLH-DSA) as a mathematically diverse hash-based signature backup in August 2024, and in March 2025 it selected the code-based HQC algorithm to provide further diversity in key establishment. NIST's draft Internal Report 8547 sketches the deprecation path the standards bodies expect to follow, proposing that the classical algorithms most at risk be deprecated around 2030 and disallowed by 2035. The June 2026 *Cryptographic Security* order should be read as the executive-branch instrument that converts these standards and goals into dated agency obligations and, crucially, into acquisition requirements that reach contractors. It does not invent the destination; it commits the government to a schedule for arriving there and brings the private sector into the convoy.

The Cloud Security Alliance has been making this case for the better part of a decade. CSA established its Quantum-Safe Security Working Group in 2015 — the group was already presenting its work at the ETSI/IQC quantum-safe cryptography workshop that October — and published its foundational primer *What is Quantum-Safe Security?* in 2016, well before post-quantum standards existed. In March 2022, years ahead of the federal deadlines, CSA gave the threat a memorable shape by launching its "Year to Quantum" (Y2Q) initiative and a public countdown clock, setting **April 14, 2030** as the date by which organizations should assume a quantum computer could break present-day cryptography and urging, in the words of CSA CEO Jim Reavis, that "the time is now to prepare for a quantum-safe future." The convergence is striking: the *Cryptographic Security* order's headline deadline for migrating the government's most sensitive systems to post-quantum key establishment — December 31, 2030 — lands within months of the Y2Q date CSA fixed in 2022. The executive orders have, in effect, ratified on a national scale the timeline the quantum-safe community identified years earlier, and organizations that took Y2Q seriously when it was announced are now the ones best positioned to meet the federal schedule.

This lineage carries a practical implication that the Cloud Security Alliance has emphasized throughout its quantum-safe work: the governance problem and the engineering problem are inseparable. An organization cannot migrate cryptography it cannot see, and it cannot prioritize a migration it has not mapped against the confidentiality lifetime of its data. The federal order's first substantive act — requiring each agency to name a migration lead responsible for cryptographic inventory within thirty days — is a governance act before it is a technical one, and private organizations would do well to mirror it. The work that determines whether a migration succeeds or stalls is the unglamorous work of inventory, ownership, and prioritization, and that work can and should begin immediately, independent of any external deadline.

Why This Reaches the Private Sector

A common misreading of both orders is that, because they are addressed to federal departments and agencies, they impose no obligations on private companies. That reading is mistaken in several concrete ways, and the gap between "no direct mandate" and "no effect" is where unprepared organizations will be caught.

The most direct channel is acquisition. The *Cryptographic Security* order directs the FAR Council to amend the Federal Acquisition Regulation so that covered contractors must comply with NIST's post-quantum FIPS, including all applicable standards incorporating quantum-resistant algorithms, by the end of 2030, and to add a separate requirement that contractors maintain vulnerability-disclosure policies covering cryptographic weaknesses — explicitly including the absence of encryption and the use of non-FIPS-approved algorithms. Any organization that sells software, cloud services, hardware, or professional services to the federal government should expect these requirements to appear in contract clauses and to flow down to subcontractors and suppliers, in the same way that other security requirements have propagated through federal supply chains. Because the federal government is such a large customer, an obligation that is formally limited to contractors becomes, in practice, a market expectation.

The second channel is critical infrastructure. The order directs sector risk-management agencies, working through CISA, to help critical-infrastructure owners and operators develop post-quantum migration plans. Although framed as assistance rather than mandate, this is how sector expectations are established and how, over time, they harden into baseline practice and sometimes into binding rules. Operators in energy, finance, healthcare, communications, and other sectors should anticipate that quantum readiness will become a subject of sector engagement, examination, and eventually regulation, and that long asset-replacement cycles make early planning essential. The third channel is the cryptographic bill of materials. By directing CISA and NIST to define a CBOM, the order seeds a transparency mechanism that, once it exists, customers and regulators will ask vendors to produce — much as the software bill of materials moved from federal initiative to broad market expectation. A vendor that cannot describe the cryptography embedded in its products will increasingly be at a disadvantage.

A fourth channel is less obvious but consequential: the cryptographic-module validation bottleneck. The order directs NIST to accelerate module validation precisely because that process is a chokepoint. Validation of cryptographic modules already takes well over a year on average, and the federal program is moving older module certifications to historical status, which means the supply of validated, post-quantum-capable modules will lag demand for some time. Organizations that depend on validated modules — which includes most regulated industries and any vendor selling into government — should treat the validation queue as a real constraint on their own timelines and plan procurement accordingly rather than assuming compliant modules will be available on demand.

Recommendations by Ecosystem Role

The remainder of this paper translates the orders into action for the principal constituencies of the security ecosystem. The recommendations share a common spine — inventory, agility, prioritization, and governance — but their emphasis differs by role, and the differences matter.

Chief Information Security Officers and Enterprise Security Leaders

For enterprise security leaders the single most valuable response to the June 2026 orders is to begin a cryptographic inventory now and to treat it as a permanent capability rather than a one-time project. The orders make the federal version of this mandatory and time-bound, but the underlying logic is universal: an organization that does not know where it uses RSA, elliptic-curve cryptography, and the protocols that depend on them cannot estimate its exposure, cannot prioritize, and cannot demonstrate progress to a board or a regulator. The inventory should reach beyond the obvious endpoints into protocol libraries, certificates and the public-key infrastructure that issues them, hardware security modules, code-signing and document-signing keys, embedded and operational-technology devices, and the third-party and software-as-a-service products whose cryptography the organization inherits without controlling. The forthcoming cryptographic bill of materials will eventually make the third-party portion of this picture easier to assemble; in the meantime, vendor questionnaires and contractual disclosure requirements are the available instruments.

With an inventory in hand, prioritization should follow the harvest-now logic rather than treating all systems equally. The first systems to migrate are those that protect data with the longest confidentiality lifetime and the greatest sensitivity, and those most exposed to interception or exfiltration — externally facing communications, long-lived archives, key material, and the credentials and signing keys that, if compromised, would unlock far more than themselves. Crypto-agility is the architectural property that makes all of this sustainable: systems should be designed so that cryptographic algorithms can be replaced without re-architecting the application, because the post-quantum transition will not be the last cryptographic transition, and because the standards themselves continue to evolve with the addition of backup algorithms such as HQC. Hybrid schemes, which combine a classical and a post-quantum algorithm so that the result is secure if either holds, are the pragmatic bridge during the transition and should be the default for new deployments protecting sensitive data.

Finally, CISOs should fold quantum readiness into the governance and reporting structures the board already understands. Cryptographic dependency is an enterprise risk with a known direction and an approximate timeline, which makes it well suited to the kind of key-risk-indicator reporting boards increasingly expect: percentage of systems inventoried, percentage migrated to quantum-resistant or hybrid cryptography, exposure of long-lived sensitive data, and dependency on vendors whose timelines the organization cannot control. The Cloud Security Alliance's AI Controls Matrix and Cloud Controls Matrix,

together with the Consensus Assessments Initiative Questionnaire, provide the control language and the vendor-assessment mechanism to make this reporting consistent and comparable across an organization and its supply chain. The decisive point is not to wait for a mandate that applies directly to the enterprise; the data exposure is present now, and the organizations that begin early will face a manageable program rather than a crisis.

Software Companies and Independent Software Vendors

Software vendors occupy a pivotal position because the cryptography they embed becomes their customers' inherited risk, and because the acquisition provisions of the *Cryptographic Security* order will increasingly make quantum readiness a condition of selling into government and, by extension, a competitive differentiator more broadly. The foundational task is to make products crypto-agile, so that the algorithms used for key establishment and for digital signatures can be updated through configuration or modular replacement rather than through a rearchitecture that takes years to ship and longer for customers to adopt. Hard-coded algorithm choices, assumptions about key and signature sizes, and protocol implementations that cannot negotiate new algorithms are the technical debt that the transition will expose, and they are cheaper to address deliberately now than under deadline pressure later.

Vendors should plan for the asymmetry between key establishment and signatures that the federal deadlines themselves acknowledge. Support for ML-KEM has matured faster than support for ML-DSA and SLH-DSA, and the larger key and signature sizes of the post-quantum algorithms have real consequences for storage, bandwidth, latency, and protocols with tight size constraints. Building and testing against the signature standards early, rather than treating them as a later phase, is the way to avoid being on the wrong side of the signature gap when customers begin demanding compliance. Equally important is transparency about cryptographic composition: vendors should prepare to produce a cryptographic bill of materials alongside their software bill of materials, both because the order seeds the expectation and because customers conducting their own inventories will increasingly require it. A vendor that can hand a customer a clear account of the cryptography in its product, and a credible roadmap to quantum resistance, converts a compliance burden into a trust advantage.

The order's vulnerability-disclosure provision is a further signal. By directing that contractor disclosure policies cover cryptographic weaknesses and the use of non-FIPS-approved algorithms, the government is treating weak or absent cryptography as a reportable defect rather than a design preference. Software companies should align their own vulnerability-handling processes accordingly, and should audit their products for the quiet failure modes the provision targets: unencrypted channels, deprecated algorithms, and home-grown cryptography. These are precisely the issues that machine-speed code analysis now surfaces at scale, and a vendor that finds and fixes them proactively will be better positioned than one that waits for a customer or a researcher to find them first.

Artificial-Intelligence Companies and Model Providers

Artificial-intelligence companies sit at a particularly sharp corner of the quantum transition, for reasons that are easy to overlook amid the more familiar AI-safety conversation. The assets that define an AI company — proprietary model weights, training datasets, fine-tuning data, and the credentials and keys that govern access to expensive inference infrastructure — are exactly the kind of long-lived, high-value secrets that the harvest-now-decrypt-later threat targets. Model weights that represent years of investment and that will remain commercially and strategically valuable for a long time are worth harvesting today even if they cannot be decrypted for a decade. The Cloud Security Alliance has examined this convergence directly in its work on the quantum risk to AI infrastructure, and the implication for model providers is that protecting training pipelines, weight storage, and model-serving channels with quantum-resistant or hybrid cryptography is not a distant concern but a present one.

The intersection runs in the other direction as well. AI systems are increasingly agentic — composed of autonomous agents that authenticate to systems, establish secure channels, sign actions, and exchange messages with other agents — and every one of those cryptographic operations is a candidate for the post-quantum transition. As organizations build the agentic control plane, they should ensure that the identity, signing, and channel-security mechanisms underpinning it are crypto-agile from the outset, so that agent identities and the receipts that attest to their actions remain trustworthy across a cryptographic transition. The Cloud Security Alliance's work on securing the agentic control plane — including the Autonomous Action Runtime Management specification for runtime action enforcement and the Agentic Trust Framework for Zero Trust agent governance — provides the structure for this, and quantum readiness should be treated as a property those structures must preserve rather than as a separate program. An agentic architecture that bakes in non-agile cryptography today will inherit the same migration debt that has made the broader transition so painful, only in a layer that is newer and faster-changing.

Finally, AI companies that increasingly act as platform and infrastructure providers to other enterprises carry a shared-responsibility obligation that mirrors the one cloud providers already bear. Customers building on a model provider's platform inherit that provider's cryptographic choices, and they will increasingly ask — through questionnaires, contracts, and eventually cryptographic bills of materials — what those choices are. Providers that can answer clearly, and that offer quantum-resistant options for the channels and storage that protect customer data and model interactions, will earn the trust that the agentic era demands.

Network-Infrastructure Providers

Network-infrastructure providers carry some of the heaviest and earliest burdens of the transition, because the protocols that secure the network — TLS, IPsec and IKEv2, SSH, and the public-key infrastructure beneath them — are where public-key cryptography is most pervasive and most performance-sensitive. The CNSA 2.0 timelines already expect networking equipment to be exclusively quantum-resistant by 2030, and the federal deadlines in the *Cryptographic Security* order reinforce that direction. The larger key and

signature sizes of post-quantum algorithms interact directly with protocol design: handshake sizes grow, fragmentation behavior changes, and latency-sensitive paths feel the difference, so providers must test post-quantum and hybrid configurations under realistic load rather than assuming a drop-in replacement.

Certificate and key lifecycle management is the discipline most stressed by this transition. Providers should ensure that their public-key infrastructure can issue, rotate, and revoke certificates using post-quantum and hybrid algorithms, and that automation exists to do so at the scale and speed the network requires, because manual certificate processes that are merely painful today become unworkable when a fleet must be re-keyed under deadline. Hardware refresh cycles deserve particular attention: networking equipment with multi-year service lives that is purchased today should be evaluated for its ability to support quantum-resistant algorithms throughout that life, since equipment bought without that capability becomes a stranded migration liability. Providers evaluating quantum key distribution as an alternative should do so with clear eyes; it addresses a narrow part of the problem, carries significant deployment constraints, and is not a substitute for migrating the algorithms that secure the overwhelming majority of network traffic, a position consistent with the guidance of the national-security agencies.

Cloud-Service Providers

Cloud providers sit at a leverage point in the ecosystem, because the cryptographic choices they make are inherited by every customer who builds on their platforms, and because they can accelerate the entire transition by making quantum-resistant options available, default, and easy to adopt. The shared-responsibility model that governs cloud security applies directly to cryptography: providers are responsible for the quantum readiness of the platform's own cryptographic services — key-management systems, hardware security modules, load balancers and transit encryption, certificate services, and the control-plane channels that secure the platform itself — while customers remain responsible for the cryptography of what they build on top. Providers should make this division explicit, document which services already offer post-quantum or hybrid options and on what timeline the rest will, and resist leaving customers to infer the platform's cryptographic posture.

The most useful thing a cloud provider can do is to make quantum-resistant cryptography the path of least resistance. Offering post-quantum and hybrid key establishment in managed TLS termination, supporting post-quantum algorithms in key-management and signing services, and surfacing cryptographic posture in the tooling customers already use to assess their environments will move customer migrations faster than any amount of exhortation. Because cloud providers are themselves significant federal contractors and critical-infrastructure operators, they are squarely within the reach of the order's acquisition and sector provisions, and the cryptographic bill of materials they will be expected to produce can double as a customer-facing transparency artifact. Providers that lead here will find that quantum readiness becomes, like compliance certifications before it, a reason customers choose one platform over another.

Critical-Infrastructure Operators

Critical-infrastructure operators face the migration under the hardest constraints in the ecosystem, and the *Cryptographic Security* order's direction that sector risk-management agencies assist them through CISA is an acknowledgment of that difficulty rather than a solution to it. Operational-technology environments are populated by devices with service lives measured in decades, by equipment that cannot be patched without revalidation or safety recertification, and by systems for which downtime carries physical and human consequences. In such environments the clean migration available to an IT estate is often impossible, and a degraded-mode doctrine becomes necessary: where cryptography cannot be upgraded in place, operators must compensate with segmentation, monitoring, strict access control, and the isolation of vulnerable systems from exposure, while planning replacement on the only timeline the equipment allows.

For these operators the harvest-now threat and the long asset lifecycle combine into an unusually unforgiving problem, because equipment specified and purchased today may still be in service when a cryptographically relevant quantum computer exists, and the data it protects may need confidentiality for the entire interval. The practical response is to make quantum resistance a procurement criterion now — to require, in new purchases of long-lived equipment, the crypto-agility that will allow algorithms to be updated over the asset's life — and to engage early with the sector coordination the order establishes rather than waiting for it to harden into requirement. Operators should also recognize that their sector regulators are already naming quantum as an emerging risk, and that early, documented planning is both a security measure and a defense against the regulatory and examination pressure that is coming.

Cross-Cutting Imperatives

Beneath the role-specific recommendations lie three imperatives that apply to every constituency and that determine whether the others succeed. The first is crypto-agility, the architectural discipline of treating cryptographic algorithms as replaceable components rather than fixed assumptions. Every organization in the ecosystem will migrate more than once — the standards bodies are still adding algorithms, and the history of cryptography guarantees future transitions — so the value of agility compounds well beyond the immediate post-quantum move. The second is cryptographic inventory, soon to be formalized as the cryptographic bill of materials, which is the precondition for every other action: prioritization, vendor assessment, board reporting, and migration itself all depend on knowing where cryptography lives. The third is governance, the assignment of clear ownership and the integration of cryptographic risk into the enterprise risk and reporting structures that leadership already uses. The federal order's first act was a governance act, naming accountable leads; private organizations that imitate it will find the technical work follows more readily.

A fourth imperative, easy to underestimate, is workforce. The *Innovation* order devotes an entire section to building a quantum workforce because the talent to execute this transition is scarce, and the same scarcity affects the defensive side. Organizations should invest now in building cryptographic literacy within their security teams and in cultivating the small number of specialists who understand both the mathematics and the engineering of the migration, because the demand for that expertise will only intensify as deadlines approach and as every organization competes for the same limited pool.

CSA Resources and Alignment

The Cloud Security Alliance has been preparing the community for this transition since 2015, and organizations acting on the June 2026 orders do not need to start from a blank page. The Quantum-Safe Security Working Group — which also maintains the Y2Q countdown clock that fixed April 14, 2030 as the community's working deadline — has produced a body of practitioner-oriented guidance, including *A Practitioner's Guide to Post-Quantum Cryptography*, which walks organizations that lack deep in-house cryptographic expertise through identifying vulnerable components, assessing the store-now-decrypt-later threat, and planning mitigation for data in transit and at rest. The working group's *Quantum-Safe Security Governance with the Cloud Controls Matrix* connects the migration to the control framework that many organizations already use for cloud governance, and *Confidence in Post-Quantum Algorithms* helps practitioners reason about the maturity and trustworthiness of the new standards. For the AI constituency in particular, the CSA Labs research on *Harvest Now, Decrypt Later: Quantum Risk to AI Infrastructure* addresses the convergence of quantum risk and AI assets directly, and the broader Labs work on enterprise post-quantum migration provides strategic framing for the timeline decision.

These quantum-specific resources sit within a larger CSA framework that the recommendations above repeatedly invoke. The AI Controls Matrix, which supersedes and extends the Cloud Controls Matrix, supplies the control language for treating cryptographic dependency as a governed risk, and the Consensus Assessments Initiative Questionnaire and the STAR program provide the mechanisms for assessing and attesting to that posture across a supply chain — the same mechanisms through which the coming cryptographic-bill-of-materials expectation will most naturally be satisfied. For organizations building the agentic systems that the AI section describes, the Autonomous Action Runtime Management specification and the Agentic Trust Framework define the runtime enforcement and Zero Trust governance of the agentic control plane, and crypto-agility should be treated as a property those structures preserve. Taken together, this portfolio lets an organization move from the abstract obligation the executive orders create to a concrete, framework-aligned program of inventory, assessment, migration, and reporting.

Conclusion: From Federal Mandate to Ecosystem Readiness

The two executive orders of June 2026 are best understood as a single message delivered in two registers. The *Innovation* order says the United States intends to build the most powerful quantum computers in the world; the *Cryptographic Security* order says the United States assumes its adversaries are trying to do the same, and that the nation must protect its information against that possibility before it becomes a reality. For the security ecosystem the operative consequence is that the post-quantum transition has moved from a recommended practice to a scheduled obligation, and that the schedule reaches the private sector through acquisition rules, critical-infrastructure coordination, and the transparency mechanisms the orders set in motion.

The encouraging reality is that the hardest prerequisites are already met. The algorithms exist and are standardized, the governance framework is in place, and the migration path is well understood. What remains is execution, and execution rewards those who begin early: an organization that starts its cryptographic inventory now, designs for crypto-agility, prioritizes its most exposed and longest-lived data, and folds cryptographic risk into the governance its leaders already practice will experience the coming years as a managed program rather than a scramble against a deadline. The harvest-now-decrypt-later threat means the clock has, in an important sense, already started, and the data an organization most wants to protect is the data most at risk today. The Cloud Security Alliance's role, as it has been throughout this transition, is to give the community the frameworks, the assessments, and the practitioner guidance to act with confidence. The executive orders have set the destination and the schedule; the work now is to move.

References

[1] The White House. "Executive Order 14411: Ushering in the Next Frontier of Quantum Innovation." Presidential Actions, June 22, 2026.

[2] The White House. "Executive Order 14409: Securing the Nation Against Advanced Cryptographic Attacks." Presidential Actions, June 22, 2026.

[3] National Institute of Standards and Technology. "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard." August 13, 2024.

[4] National Institute of Standards and Technology. "FIPS 204: Module-Lattice-Based Digital Signature Standard." August 13, 2024.

[5] National Institute of Standards and Technology. "FIPS 205: Stateless Hash-Based Digital Signature Standard." August 13, 2024.

[6] National Institute of Standards and Technology. "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption." March 11, 2025.

[7] National Institute of Standards and Technology. "NIST IR 8547 (Draft): Transition to Post-Quantum Cryptography Standards." November 2024.

[8] U.S. Congress. "Quantum Computing Cybersecurity Preparedness Act (P.L. 117-260)." December 21, 2022.

[9] The White House. "National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." May 4, 2022.

[10] Office of Management and Budget. "M-23-02: Migrating to Post-Quantum Cryptography." November 18, 2022.

[11] National Security Agency. "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems (CNSA 2.0)." September 7, 2022.

[12] Cybersecurity and Infrastructure Security Agency, NSA, and NIST. "Quantum-Readiness: Migration to Post-Quantum Cryptography." 2023.

[13] The Quantum Insider. "Trump Administration Executive Order Places Quantum at Center of Federal Technology Strategy." June 22, 2026.

[14] Nextgov/FCW. "Trump signs 2 orders to prepare the US for a quantum future." June 2026.

[15] NBC News. "Trump signs orders calling for powerful quantum computer." June 2026.

[16] Cloud Security Alliance. "A Practitioner's Guide to Post-Quantum Cryptography." Quantum-Safe Security Working Group.

[17] Cloud Security Alliance. "Quantum-Safe Security Governance with the Cloud Controls Matrix." Quantum-Safe Security Working Group.

[18] Cloud Security Alliance. "Confidence in Post-Quantum Algorithms." Quantum-Safe Security Working Group.

[19] Cloud Security Alliance Labs. "Harvest Now, Decrypt Later: Quantum Risk to AI Infrastructure." 2026.

[20] Cloud Security Alliance Labs. "Strategic Post-Quantum Cryptography Migration: The Enterprise Imperative." 2026.

[21] Cloud Security Alliance. "Quantum-Safe Security Working Group." Accessed June 2026.

[22] Cloud Security Alliance. "Cloud Security Alliance Sets Countdown Clock to Quantum." Press Release, March 9, 2022.

[23] Cloud Security Alliance, Quantum-Safe Security Working Group. "What is Quantum-Safe Security?." 2016.