GovCIO MEDIA & RESEARCH

AUGUST 2026

DeepDives

Government Prepares for a POST-QUANTUM FUTURE

INSIDE:

SPONSORED BY

AXIAD FEDERAL

GovCIO MEDIA & RESEARCH

From the editor's desk

Sarah Sybert, Managing Editor

Rethinking Government's Risk Tolerance

Two new quantum executive orders are pushing federal agencies to accelerate development of quantum technologies while preparing government systems for the cybersecurity risks they will create.

One launches a national initiative to accelerate the development of a fault-tolerant quantum computer for scientific research by 2028 and directs federal agencies to develop five-year plans for advancing quantum sensing and networking technologies.

The other focuses on accelerating the federal transition to post-quantum cryptography (PQC) by requiring agencies to upgrade high-value assets and high-impact systems to quantum-resistant encryption by the end of 2030. The directive also lays the groundwork for applying those requirements to federal contractors and subcontractors through future acquisition regulations.

While quantum computing promises breakthroughs in scientific discovery, AI and national security, it also threatens the cryptographic algorithms that protect today's networks and sensitive data. Although quantum computers capable of breaking current encryption may still be years away, adversaries are already harvesting encrypted data with the expectation that it can be decrypted once quantum capabilities mature. That reality makes preparation an immediate priority.

Preparing for quantum requires more than replacing encryption algorithms. Agencies must inventory cryptographic assets, identify legacy systems that will require significant modernization and build the governance structures needed to support long-term cryptographic agility. Success will depend on enterprise-wide planning, coordinated leadership and close collaboration between government and industry.

Table of Contents

Executive Order Speeds Up Post-Quantum Cryptography Timelines

A new White House executive order and OMB guidance call for faster post-quantum cryptography migration for federal agencies.

BY SILVIA OAKLAND

The White House's latest quantum cybersecurity directive accelerated the timeline for agencies to prepare for post-quantum cryptography, and experts said the first step is understanding where vulnerable cryptography exists.

The order, signed in June, directed agencies to transition high-value assets and high-impact systems to PQC by Dec. 31, 2030. It also directed agencies to submit prioritized migration plans under new implementation guidance from the Office of Management and Budget.

Cybersecurity experts said agencies should begin by inventorying cryptographic assets, identifying sensitive data and prioritizing systems that will require the most time and effort to modernize.

"We're never going to be able to say 'we're 100% cyber secure.' It's an ongoing expense that needs to be allocated for, and there's a risk assessment that goes along with that," Celia Merzbacher, director of the Quantum Economic Development Consortium (QED-C), told GovCIO Media & Research. "Maybe some of your data doesn't need to be prioritized, but that's for every organization and every CIO to undertake that assessment and make a plan."

While larger organizations may have in-house capabilities for their PQC migration journey, others will likely work with service providers to keep systems secure, compliant and up to date.

(ctd.)

Photo credit: Official White House Photo | Joyce N. Boghosian

"IT managers, CISOs or whoever is in charge of that migration need to know the questions to ask. They also need to know how to inform management and boards that they are on track to not have a problem, like a data breach or loss of encryption, because they have a plan in place and they're executing on it," said Merzbacher.

Where Agencies Should Focus Efforts

For agencies already preparing for the transition, experts said the biggest challenge won't be replacing algorithms; it will be understanding where vulnerable cryptography already exists across sprawling federal environments.

Bill Wright, head of government affairs at Everpure and former member of the intelligence community, said he expects to see varying levels of quantum-readiness depending on how agencies previously treated data hygiene efforts.

"Those that have good visibility and accounting are going to be able to move quickly. Others that haven't had the same kind of discipline over the years are going to struggle," said Wright.

Agencies may also face additional challenges beyond data visibility and cleanup. Legacy systems often rely on older cryptographic implementations that are difficult to replace or upgrade. Without modernizing those systems, agencies may struggle to deploy PQC algorithms or implement cryptographic agility across their environments.

"It's a problem throughout the government — this reliance on legacy systems, and we've been talking for the better part of a decade on how to leapfrog out of it," Wright said.

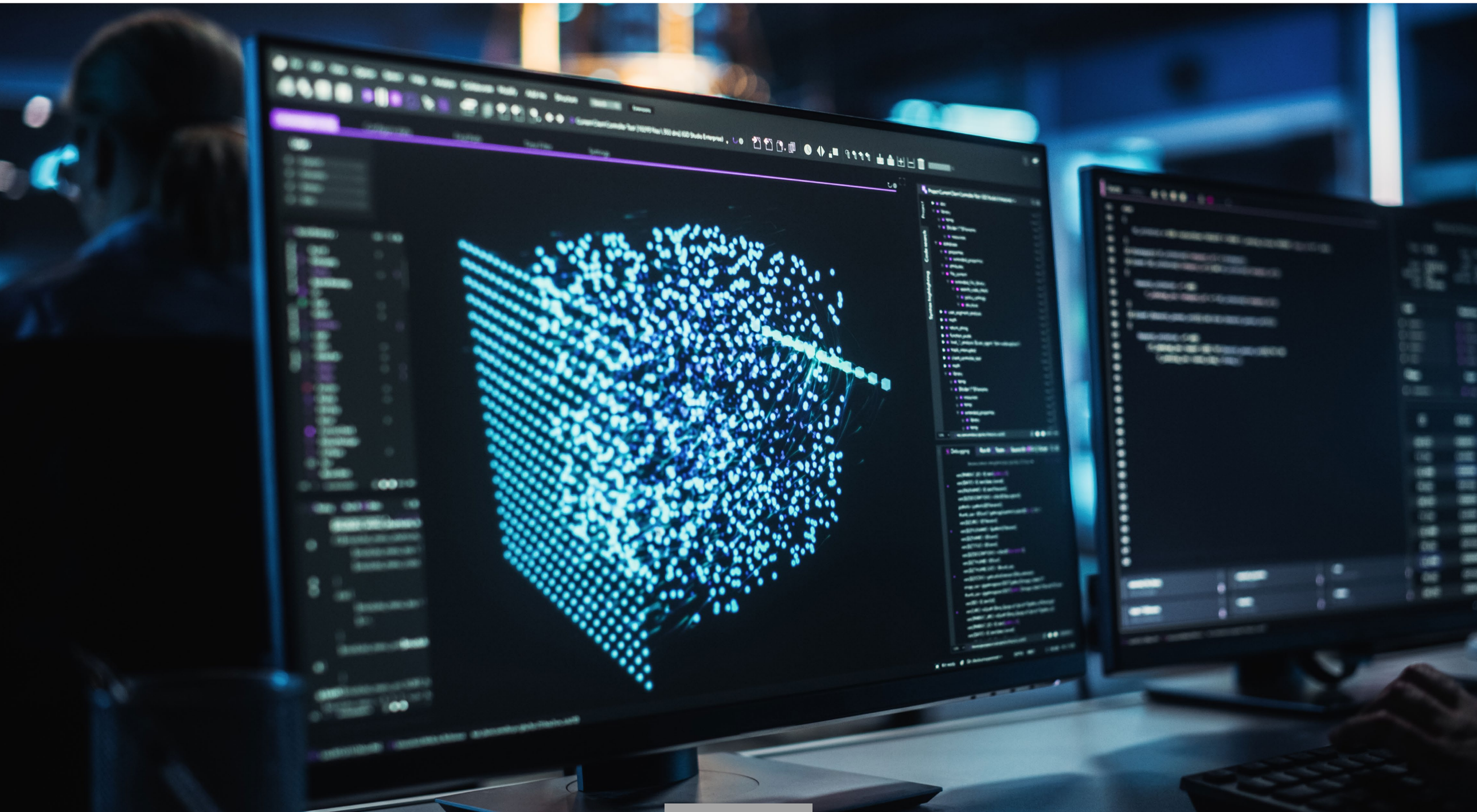
Prathibha Rama, computer engineer at Johns Hopkins University Applied Physics Laboratory, said legacy systems should be among the first priorities in an agency's PQC migration because they often require more time and engineering effort to modernize.

“Legacy systems tend to be more difficult to update. They take longer to update. A lot of times because there’s older hardware, you might have embedded systems involved in that. Those are systems you want to focus on early on because there’s going to be more engineering, creativity and feats that are involved in updating those systems,” Rama said in April.

Wright said IT leaders should design systems to remain cryptographically agile because NIST’s approved algorithms will likely continue to evolve as new standards emerge.

“The algorithms that agencies are being asked to migrate to aren’t guaranteed to be the last. NIST is going to continue to do the hard work of refining those. Agencies need to be designing systems so that you can swap out one algorithm for another without a wholesale disruption.

Photo Credit: Gorodenkoff/Shutterstock



“Legacy systems tend to be more difficult to update. They take longer to update. A lot of times because there’s older hardware, you might have embedded systems involved in that. Those are systems you want to focus on early on because there’s going to be more engineering, creativity and feats that are involved in updating those systems.”

— Prathibha Rama, Computer Engineer, Johns Hopkins University Applied Physics Laboratory

GovCIO MEDIA & RESEARCH

DeepDives

Transitioning to Post-Quantum Cryptography

President Donald Trump signed an executive order in June directing federal agencies to accelerate their transition to post-quantum cryptography (PQC) to protect government systems from future quantum threats. The order sets migration deadlines, assigns agency responsibilities and calls for new technical guidance and procurement requirements to strengthen the nation's cybersecurity posture. Here's the timeline.

WITHIN 30 DAYS

OMB WITH CISA AND ONCD

Issue government-wide guidance requiring agencies to review high-value assets (HVAs) and high-impact systems, establish migration requirements, and submit agency migration plans.

WITHIN 90 DAYS

ALL FEDERAL AGENCIES

Designate a PQC migration lead and provide information to OMB and the National Cyber Director.

WITHIN 180 DAYS

NSA

Submit the first annual report to the President on PQC migration progress for National Security Systems (NSS). Reports continue annually until migration is complete.

WITHIN 180 DAYS

NIST

Launch a pilot PQC migration project on selected NIST information systems.

WITHIN 180 DAYS

FAR COUNCIL

Publish a proposed FAR rule requiring covered contractors to comply with NIST's post-quantum cryptography standards by Dec. 31, 2030.

WITHIN 180 DAYS

NIST

Revise Cryptographic Module Validation Program (CMVP) processes to accelerate validation of cryptographic modules.

WITHIN 270 DAYS

CISA WITH NIST

Publish public guidance defining the minimum elements of a Cryptographic Bill of Materials (CBOM) to enable automated identification of cryptographic assets.

WITHIN 270 DAYS

FAR COUNCIL

Publish a proposed FAR rule requiring covered contractors to comply with NIST's post-quantum cryptography standards by Dec. 31, 2030.

DECEMBER 31, 2027

ALL FEDERAL AGENCIES

Complete migration of all High Value Assets (HVAs) and High Impact Systems (excluding National Security Systems) to PQC for key establishment.

DECEMBER 31, 2030

NIST

Complete the agency's PQC migration pilot project.

DECEMBER 31, 2030

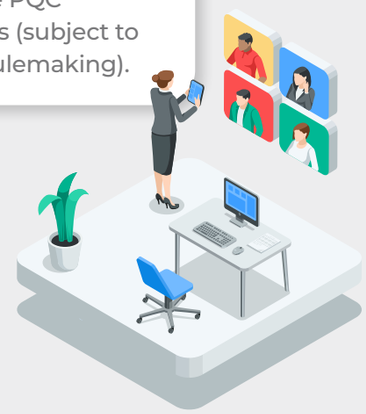
ALL FEDERAL AGENCIES

Complete migration of HVAs and High Impact Systems to PQC for digital signatures.

DECEMBER 31, 2031

CONTRACTORS

Comply with NIST FIPS requirements, including applicable PQC algorithms (subject to the FAR rulemaking).



Source: The White House

PARTNER INTERVIEW

GovCIO MEDIA & RESEARCH

AXIAD FEDERAL

Building a Successful PQC Migration Strategy

Learn why visibility, crypto agility and enterprise-wide planning are critical as agencies prepare to migrate to post-quantum cryptography.

Bassam Al-Khalidi
Co-Founder and Chief Innovation Officer, Axiad

What are the common challenges agencies face transitioning to PQC?

Al-Khalidi When organizations sit down to plan their PQC migration, they consistently stall at the initial discovery phase. The primary obstacle is not a lack of intent but a severe lack of baseline visibility. Most agencies operate with a massive cryptographic deficit, completely unaware of the sheer volume of self-signed certificates, legacy keys, shadow IT workloads and third-party integrations running across their networks.

Inventorying is more than a simple asset count. The complexity lies in capturing cryptographic context — identifying the source issuing authority, the destination application, the system owner and the operational dependencies. Without understanding this full context, an agency cannot accurately calculate its true exposure or prioritize its remediation efforts.

What should agencies prioritize today as they begin planning their post-quantum migration?

Al-Khalidi While official federal timelines often point toward 2030, industry consensus and rapid quantum leaps indicate that the operational deadline is accelerating toward

“A unified plug-and-play approach ensures that agencies maximize their current architecture investments while building a scalable foundation for continuous monitoring and rapid key rotation.”

—Bassam Al-Khalidi, Co-Founder and Chief Innovation Officer, Axiad

2028 or 2029. For teams initiating their journey today, the upcoming 12 months must be dedicated entirely to two actions: establishing foundational visibility and solving for “the long tail” of legacy applications.

Legacy software in missions like health, finance and defense logistics cannot natively process new post-quantum algorithms. Identifying these incompatible systems early allows agencies to plan upgrades, architect replacements or implement compensating controls before deadlines expire. Instead of deploying a fragmented array of niche security tools that exacerbate existing data silos, agencies must prioritize centralized orchestration.

A unified plug-and-play approach ensures that agencies maximize their current architecture investments while building a scalable foundation for continuous monitoring and rapid key rotation.

What do you see as the biggest priority for organizations over the next year as they prepare for PQC? What’s the most common misconception about that process?

Al-Khalidi A common misconception surrounding PQC is that it is strictly a public key infrastructure (PKI) or certificate authority (CA) issue. Historically,

when PQC mandates arrive, leadership hands the task exclusively to their isolated PKI engineering teams. This approach creates localized solutions that fail at an enterprise scale.

While the PKI team focuses on backend server architectures, the identity and access management (IAM) team handles human credentials, and completely separate groups oversee automated AI agents or machine-to-machine communications. When these teams operate within budgetary and operational silos, they inadvertently generate fresh blind spots.

Just as zero trust shifted from a network-team problem to a holistic, agency-wide modernization directive, PQC demands an enterprise-wide lead — an empowered stakeholder to synchronize funding, policy and implementation across all directorates. Only then can an agency achieve true "crypto agility," ensuring that when future algorithms are deprecated, the organization can seamlessly pivot and restore secure operations in hours rather than months.

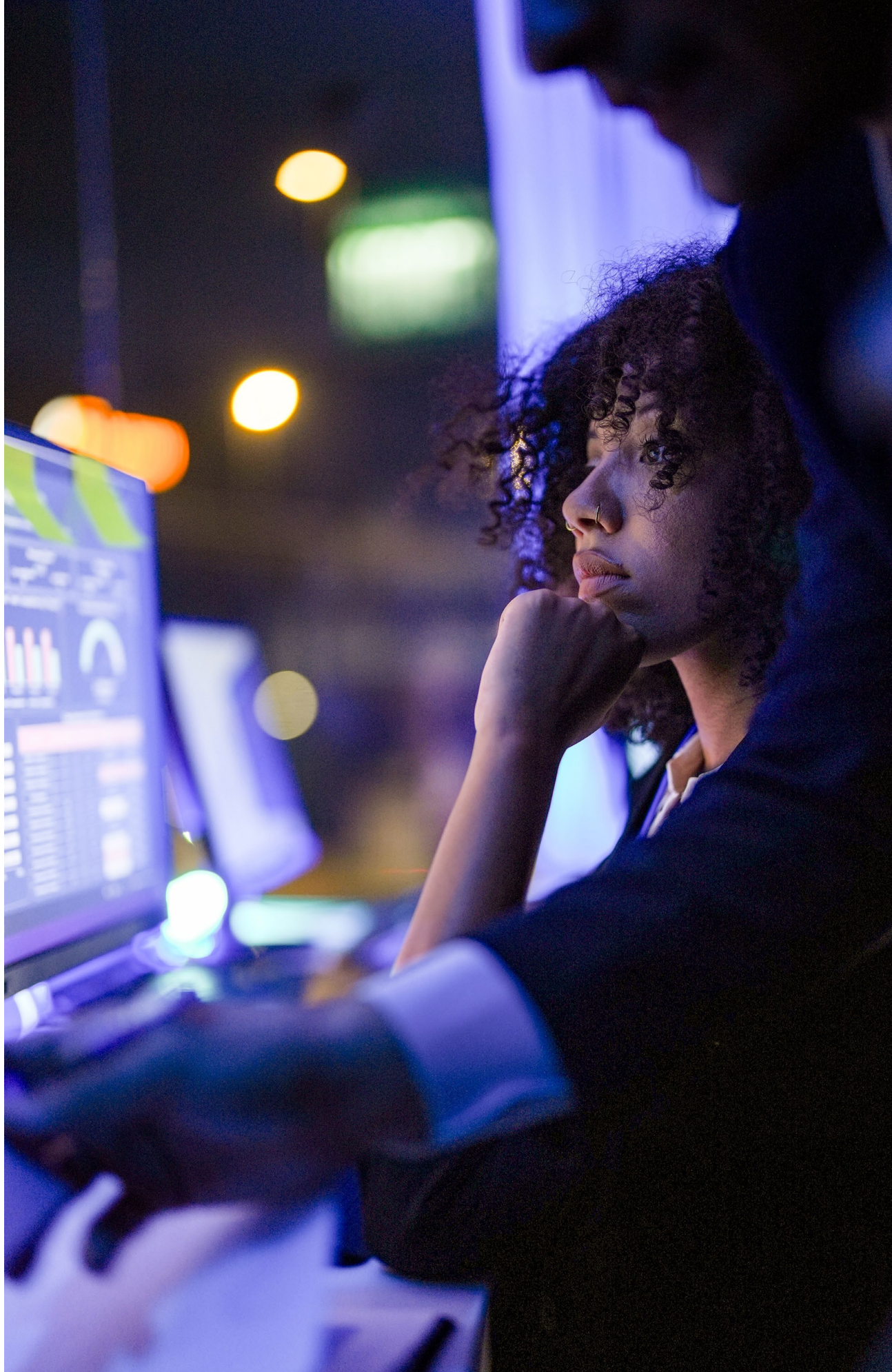


Photo Credit: ultramansk/Shutterstock

AXIAD

Is Your Cryptographic Infrastructure Quantum-Ready?

Take our assessment to find out.

PQC Domain Assessment
quantum.axiad.io

axiad.ai

War Department Details Post-Quantum Cryptography Roadmap

The Pentagon is accelerating PQC adoption across military networks, weapons systems and the defense industrial base under a new strategy.

BY ROSS GIANFORTUNE

The War Department's first enterprise-wide strategy to transition military systems to post-quantum cryptography (PQC) sets firm deadlines to secure high-impact national security systems by 2030 and the broader force by 2031 as quantum computing threatens today's encryption.

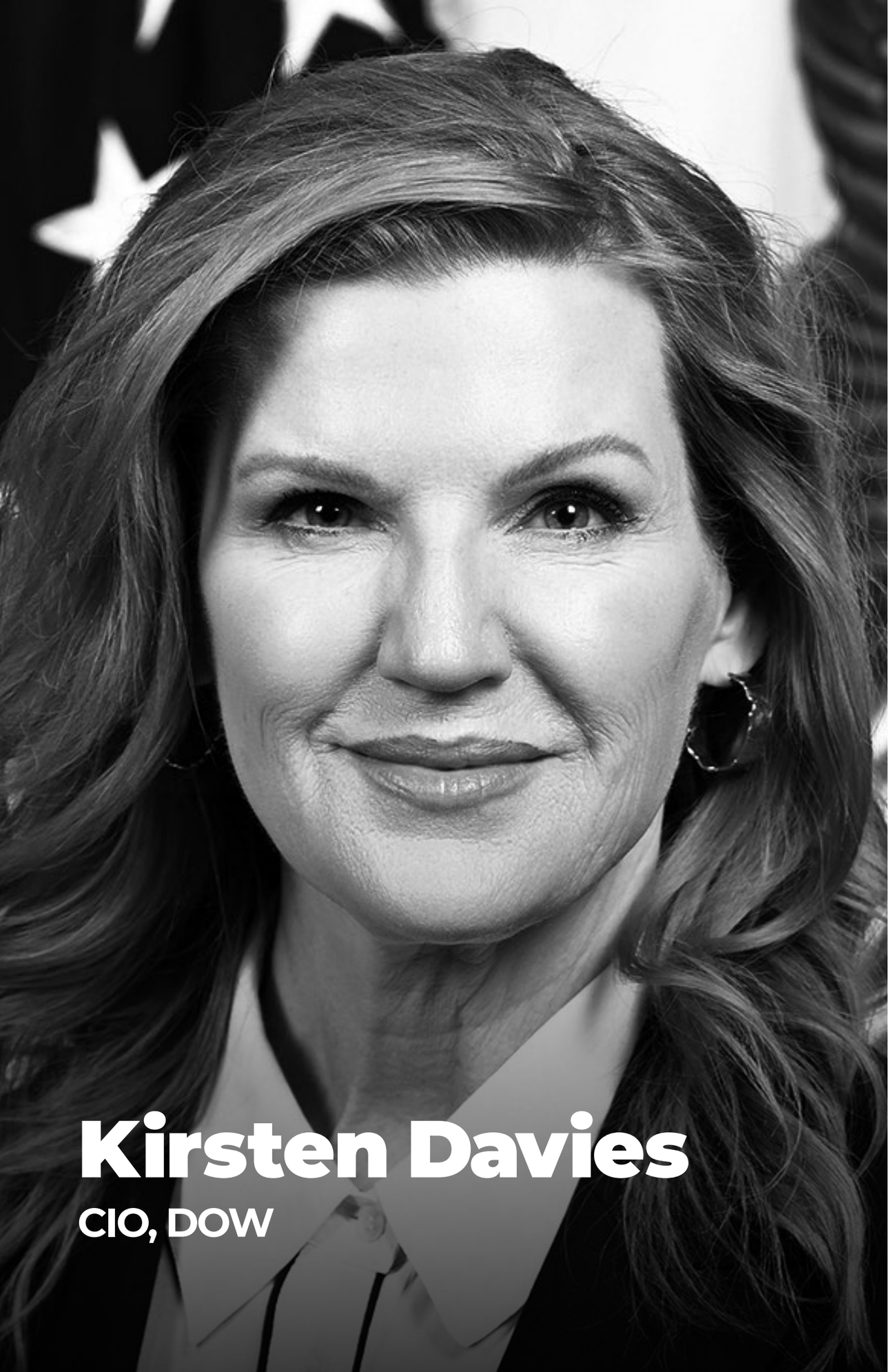
The strategy outlined how the department will deploy quantum-resistant cryptography across military networks, command-and-control systems and weapons platforms. It followed one day after President Donald Trump's June executive orders on quantum innovation and national security.

"Empowering the warfighter is the relentless objective that drives every program," Pentagon CIO Kirsten Davies said in the strategy's accompanying fact sheet. "To deliver on Secretary [Pete] Hegseth's vision of the most lethal and dominant military force in the world, our networks must be impenetrable."

While practical quantum computers remain years away, officials warn adversaries could already be collecting encrypted military communications with plans to decrypt them once the technology matures — a threat commonly known as "harvest now, decrypt later." The strategy aims to replace today's vulnerable public-key encryption with quantum-resistant algorithms before that happens.

(ctd.)

Photo Credit: Invision Events



Experts say national security systems must begin the transition now because migrating cryptographic infrastructure across the Defense Department will take years.

"If there are other nations that get ahead of us as far as post-quantum cryptography is concerned, they have a head start in terms of security," Prathibha Rama, computer engineer at Johns Hopkins University Applied Physics Laboratory, said during GovCIO Media & Research's Cybersecurity Summit in April. "They won't have to worry about it in five to 10 years down the line when quantum computers are around. We'll be behind."

DOW's Enterprise Migration Strategy

The plan establishes five priorities for the department's transition:

- Centralized governance to standardize implementation across military services.
- Department-wide inventories of existing cryptographic systems. Accelerated testing and development of quantum-resistant technologies.
- Expanded partnerships with industry and standards organizations.
- Deployment of PQC capabilities across land, sea, air, space and cyber operations.
- The strategy calls quantum computing an "existential threat" to military operations.

"Cryptography is a foundational mission enabler across nearly all DOW systems," the strategy states. "From the authorization and deployment of nuclear weapons to the execution of coordinated maneuvers with mission partners, insecure communications pose an existential threat to DOW missions."

Implementation Will Be Complex

Defense Information Systems Agency leaders told GovCIO Media & Research that transitioning to PQC will require years of testing, engineering and modernization.

At TechNet Cyber 2026, DISA DODNet Chief Engineer Mike Butler said early prototyping has already shown the department will need to adjust requirements as migration efforts progress.

“You may learn [prototyping is] going to change what the end state is and ultimately may need to be,” Butler said. “It may introduce new requirements that we didn’t think about from a defensive cyber operations perspective or from a quantum encrypting perspective.”

DISA PAE Cyber Brian Hermann said the transition begins with modernizing the department’s public key infrastructure (PKI), which underpins digital identities across War Department networks.

“The one thing that I think is on our mind, especially is the drive to accelerate PQC adoption. Step one of that is the basis for identity, which are [PKI],” Hermann said.

Hermann said many organizations across the department have yet to

Photo Credit: Gorodenkoff/Shutterstock

realize they'll play a role in the migration.

"There's probably a bunch of people that haven't heard that they have a role to play in PQC," Hermann said. "We'll begin to test across the department, but it's a pretty challenging space."

The strategy also calls for developing a new generation of High Assurance End Cryptographic Units and embedded tactical encryption modules to secure battlefield communications, satellite networks and other operational technology.

"Every piece of [operational technology-connected] hardware, every software application that we buy, we need to make sure that it's compliant with those standards for PQC," Hermann said. "That's a big challenge, not unlike zero trust adoption across the department."

Driving Industry Adoption

Beyond modernizing DOW's systems, the strategy aims to reshape how the department acquires cybersecurity technologies.

Davies said centralized governance will help the department streamline procurement, reduce duplicative spending and accelerate adoption.

"We are answering the president's call by establishing centralized governance — ensuring we leverage our buying power, eliminate waste, and secure the best possible value for every taxpayer dollar while moving at speed of innovation," Davies said in the fact sheet.

The strategy directs the department to review acquisition policies, streamline testing and deployment processes, and use its purchasing power to encourage broader adoption of quantum-resistant technologies across the commercial cybersecurity market.

Defense contractors will also be expected to prepare for future Federal Acquisition Regulation requirements related to post-quantum cryptography. The strategy directs military components to inventory cryptographic capabilities across both national security systems and Defense Industrial Base

"We are answering the president's call by establishing centralized governance — ensuring we leverage our buying power, eliminate waste, and secure the best possible value for every taxpayer dollar while moving at speed of innovation."

—Kirsten Davies, CIO, DOW

networks while identifying vulnerabilities and opportunities to automate the transition where appropriate.

As implementation begins, combatant commands are starting cryptographic inventories while DISA continues working with vendors to refine technical requirements.

"We understand what their requirements are, we understand what that's going to look like," DISA Acting DODNet Deputy Program Manager Kelli Garczynski told GovCIO Media & Research, adding that quantum-resilient protections must provide the "same or better" performance than current capabilities.

Hermann said the department is already accelerating its timeline.

"You'll see us trying to move a little faster than we had thought of a few years ago and that's pretty challenging," Hermann said. "I've been extremely proud of our team."

With the strategy now in place, Davies said the department has a roadmap to protect military communications before quantum computing becomes capable of breaking today's encryption.

"With deliberate and careful planning, guided by this strategy, I am confident the DOW will meet this challenge and provide confidence to our warfighters that the systems they trust with their lives will be secure and available when it counts," she wrote.

Photo Credit: Parilov/Shutterstock