Crypto-agility

How federal agencies can get ahead–and stay ahead–of post-quantum decryption

Accenture Federal Services

Executive summary

Quantum computing technology is maturing at a rapid and accelerating pace.

Driven by billions of dollars in private- and public-sector R&D globally, quantum computers could achieve sufficient maturity to break current encryption keys by the end of this decade—if not sooner.

The threat to federal agencies from quantum-enabled hacking is difficult to overstate. Data and systems at risk span national security secrets, defense systems, financial regulatory systems, elections, utilities and other public infrastructure, and the personal identifiable information (PII) and protected health information (PHI) of millions of government employees, contractors, and citizens.

Although most experts agree that it will be a few years before quantum computing can compromise modern cybersecurity, there is no doubt that it will eventually defeat current encryption models. Our nation's adversaries know this, too, and are working to steal encrypted data today with the intent of decrypting it later—the "Hack Now, Crack Later" strategy. Any government data stolen now can be presumed to be compromised.

Fully securing government systems and data will take years. It must be done thoughtfully—in partnership with known and trusted vendors—and in compliance with applicable regulations and standards. For all federal agencies—intelligence, defense, law enforcement, and civilian—**the time to begin the journey toward quantum-safe cryptography is now.**

Since January 2022, the White House has issued a series of National Security Memoranda requiring federal agencies to prepare for the coming threat of quantum hacking. As part of this preparation, **agencies must adopt a nimble approach to cryptographic security known as crypto-agility.**

More than just a replacement for existing encryption technologies, crypto-agility enables federal agencies to replace compromised keys and certificates **without impacting the functions of mission-critical infrastructure**. Crypto-agile agencies will be well positioned to upgrade their systems to the quantum-resistant cryptographic standard, which the National Institute of Standards and Technology (NIST) expects to release by 2024. Significant progress toward this new standard came in July 2022, when NIST selected four algorithms for standardization.

Immediate-term requirements for all agencies:

Inventorying and reporting on instances of encryption that are not quantum resistant

Prioritizing high-value assets and systems

Defining and automating a process to track the migration to quantum-resistant cryptography

The good news is that models, tools, and trusted partner organizations exist to help agencies meet these requirements **without committing significant personnel or budgetary resources**.

By adopting a crypto-agile strategy, platform, and operating model, federal agencies can safeguard their information systems and communications against the post-quantum threats that are imminent today—and successor threats yet to be defined.

Standing at the brink: Modern cryptography and quantum computers

Before 1994, the RSA cryptosystem was widely considered to be completely impenetrable and had proven to be so for nearly four decades. A single discovery—Shor's algorithm—changed everything, demonstrating that quantum computers could conceivably crack RSA and other asymmetric public-key encryption systems.

Since then, cryptosecurity experts have held the threat at bay by increasing the minimum length for uncrackable keys, allowing RSA to remain the most widely used public-key encryption system in the world.

Quantum-safe alternatives and their limits

RSA is vulnerable to brute force attacks because it uses asymmetric keys, one of which is public. Subsequent cryptosystems—specifically the Advanced Encryption Standard (AES)—rely on symmetric private keys. Theoretically, AES could also be cracked via brute force using an accelerator known as Grover's algorithm. To do so, however, a threat actor would need an exponentially more sophisticated quantum computer than that required to crack RSA encryption.

AES-256—the most current AES standard with the longest keys, which are currently used to safeguard top secret government data—is considered quantum safe for now. Unfortunately, because it would require large-scale key distribution, **AES is not a suitable replacement for public key cryptography in all federal agency scenarios**.

The question of when

Because of the prevalence of RSA encryption, the public and private sectors stand at the brink of a precipice, as quantum computing technology matures at a rapid and accelerating pace. Driven by billions of dollars in private- and public-sector R&D globally, **by the end of this decade—if not earlier—quantum computers could achieve sufficient maturity to break current RSA encryption keys.**

The day that happens, every platform, application, device, file, and email encrypted via RSA or other vulnerable cryptosystems will be at risk.

How vulnerable are we?

Advances in quantum computing will render multiple cryptosystems—all previously deemed impenetrable—vulnerable to brute force attacks.[1]

Key Standard	Qubits	Time to Break
RSA-1024	2050	**3.58 hours**
RSA-2048	4098	**28.63 hours**
NIST P-256	2300	**10.5 hours**
NIST P-521	4098	**55 hours**
AES-128	2953	2.6×10^{12} years
AES-256	2953	2.29×10^{32} years

Employing Shor's algorithm

Employing Grover's algorithm

[1] The Impact of Quantum Computing on Present Cryptography (arxiv.org)

The threat of “hack now, crack later”

While cryptographically relevant quantum computers do not exist today, the threat is more than imminent. **It is already here.**

Adversaries are working to steal sensitive data today, with the intent of decrypting it when quantum computers mature.

A significant advance in any facet of quantum science—particularly qubit architecture, noise prevention, or error-correcting algorithms—could deliver the disrupting technology that elevates quantum hacking from the realm of theory and experiment to a real and present danger. The threat could be exacerbated exponentially if quantum computers were applied to machine learning (ML) or artificial intelligence (AI) algorithms,[2] which may further accelerate a threat actor’s ability to compute immense quantities of data and break modern encryption technologies.

The potential scale of disruption from quantum-enabled hacking is difficult to overstate. As with Russia’s 2020 SolarWinds breach, which left high-value assets (HVAs) exposed for at least nine months and possibly years,[3] a quantum-enabled attack could go undetected, exposing federal agencies to multiple global threat actors simultaneously—and irreversibly.

Data and systems at risk span national security secrets, defense systems, financial regulatory systems, elections, utilities and other public infrastructure, and the personal identifiable information (PII) and protected health information (PHI) of millions of government employees, contractors, and citizens.

Regardless of when it happens, there is no doubt that quantum computing will eventually defeat current encryption models.

Our nation’s adversaries know this, too, and are working to steal encrypted data today with the intent of decrypting it later—the “Hack Now, Crack Later” strategy. Thus, **any government data stolen now can be presumed to be compromised.**

[2] Quantum Computing and AI: A Transformational Match (bbvaopenmind.com)
[3] A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack (npr.org)

Daunting but doable: The scale of Y2Q preparation

Across the intelligence, defense, and civilian sectors, government agencies face the enormous challenge of securing their systems, data, and communications against this looming threat.

The scale bears some semblance to the massive efforts undertaken to address the Year 2000 (Y2K) bug.[4] However, because the "years to quantum"—or Y2Q—cannot be definitively predicted, most agencies have postponed preparations. Without doubt, agency leaders understand their responsibility for securing their information systems, but many of their **business and mission stakeholders do not fully understand the urgency**.

As veterans of the government response to prior cybersecurity breaches know, fully securing government systems and data will take years. It must be done thoughtfully—in partnership with known and trusted vendors—and in compliance with Federal Risk and Authorization Management Program (FedRAMP) and other regulations.

But it can—and must—be done.

For all federal agencies—intelligence, defense, law enforcement, and civilian—the time to begin the journey toward quantum-safe cryptography is now.

[4] Y2K Bug (britannica.com)

Common misconceptions about post-quantum cryptography (PQC)

Agency leaders must understand quantum science to prepare for PQC.

false

Preparing for PQC starts with an inventory and assessment of cryptography currently in use. Agencies can—and must—launch this effort regardless of their level of knowledge about quantum science.

Achieving quantum-resilient cryptography requires quantum computers.

false

NIST is currently reviewing candidate standards for PQC and plans to announce them in 2024. While these standards cannot be definitively proven quantum safe until fault-tolerant quantum computers are on line, they can be measured against theoretical capabilities.

There's nothing we can do today to protect data against quantum-enabled decryption.

false

Symmetric encryption algorithms exist today that, combined with long encryption keys, are deemed to be quantum safe.

Inventorying and auditing my agency's current cryptographic posture will take months of effort.

false

Tools exist that can systematically assess current algorithms and devices in weeks.

It is the responsibility of the cloud service provider to secure my GovCloud environment against the quantum threats.

false

While service level agreements (SLAs) for security are in place, the responsibility for architecting secure cloud solutions, including cryptography, resides with the agency.

Y2Q is 20 years out.

unknowable

Expert estimates vary widely. Quantum computers capable of breaking current encryption standards could arrive by 2030—or perhaps sooner.

Quantum computing and the U.S. government

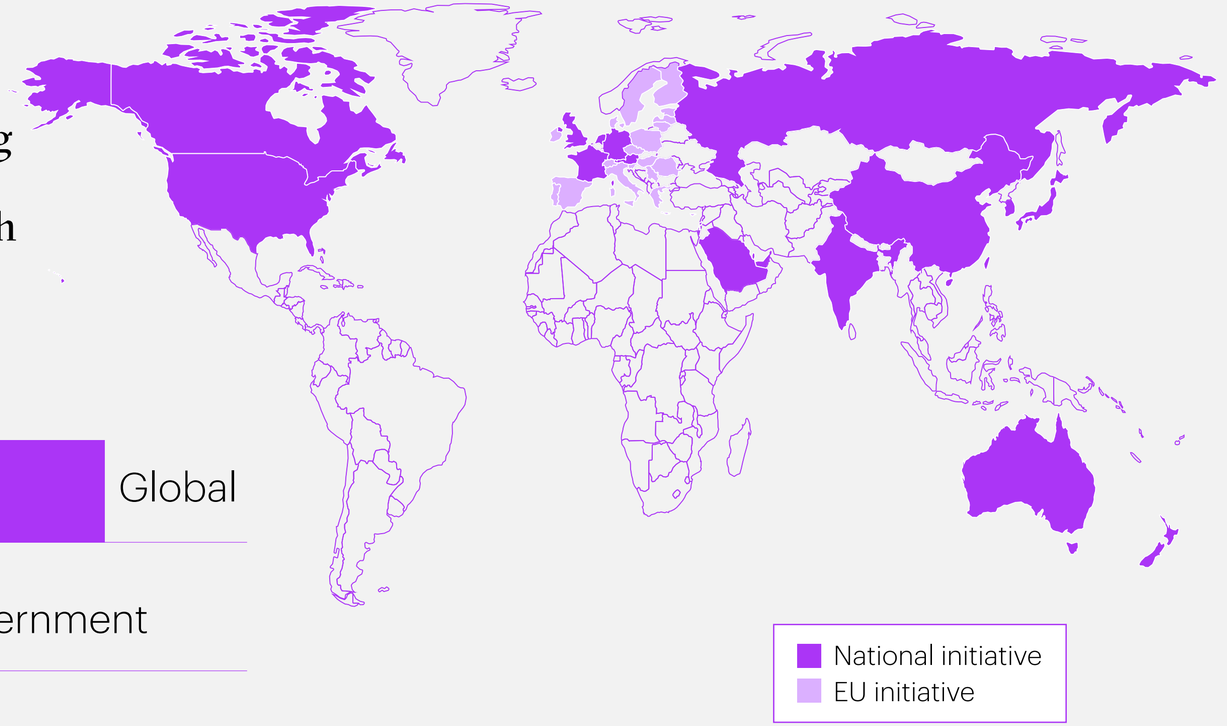
By harnessing quantum mechanical phenomena such as superposition and entanglement rather than binary functions to perform computational operations, quantum computers are exponentially faster and more powerful than even the largest classical computers.

Global investment in quantum science grows year over year, as governments, venture capitalists, and multinational technology companies including Alphabet, IBM, and Microsoft seek to establish technical superiority and market dominance in quantum computing. Still, the quantum computers that exist today are multi-million dollar installations that demand super-cooled environments and precision microwave technology[6] to function at all, let alone perform complex feats of prime factoring.

While U.S. government activity in quantum computing dates to 1994, recent legislation has dramatically expanded funding and focus. In 2018, the National Quantum Initiative Act launched a whole-of-government approach to accelerate quantum research and development in service of U.S. economic and national security.[7]

In 2021, federal funding for quantum computing R&D reached $1B. Recent and pending legislation—including the CHIPS for America Act—will continue the pace of accelerating investment.[8]

Countries investing in quantum computing research



2021 investment in quantum science[5]

$24B Global

$1B U.S. Government

To prepare for a post-quantum world, in 2016 the National Institute of Standards and Technology (NIST) began work to define and standardize one or more quantum-resistant public-key algorithms. In July 2022, NIST selected four algorithms for standardization, including CRYSTALS-Kyber for general encryption of publicly exchanged data and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for verification of digital signatures. Four additional algorithms are currently under consideration for inclusion in the final standards, which are slated for release in 2024.[9]

Thereafter, national laboratories will likely lead exploratory projects to optimize implementation of the new standard(s). These efforts include developing application programming interfaces (APIs) to help agencies update the cryptography across their systems, applications, and connected devices.

While the mechanisms, programs, and funding for this work remains to be determined, ultimately the entire U.S. government infrastructure—hardware, networking, and computing—must and will achieve quantum-safe capabilities to offset threats.

[5] Overview on quantum initiatives worldwide – update mid 2021 (qureca.com), Middle East countries accelerate quantum computing research (computerweekly.com)
[6] A new super-cooled microwave source boosts the scale-up of quantum computers (sciencedaily.com)
[7] National Quantum Initiative (quantum.gov)
[8] Washington's new crush on quantum computing (politico.com), Congress' CHIPS Act Passage Generates Applause (nextgov.com)
[9] PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates (nist.gov)

White House mandates agency action

Since January 2022, the White House has issued a series of National Security Memoranda (NSM) requiring federal agencies to begin preparing for the forthcoming post-quantum cryptography standards.

NSM-8[11] and NSM-10[12] set clear expectations for federal agencies to take action. Deadlines vary for agencies that operate national security systems (NSS) and those that do not, but **the first step required of all agencies is to inventory and report on instances of encryption that are not quantum resistant.**

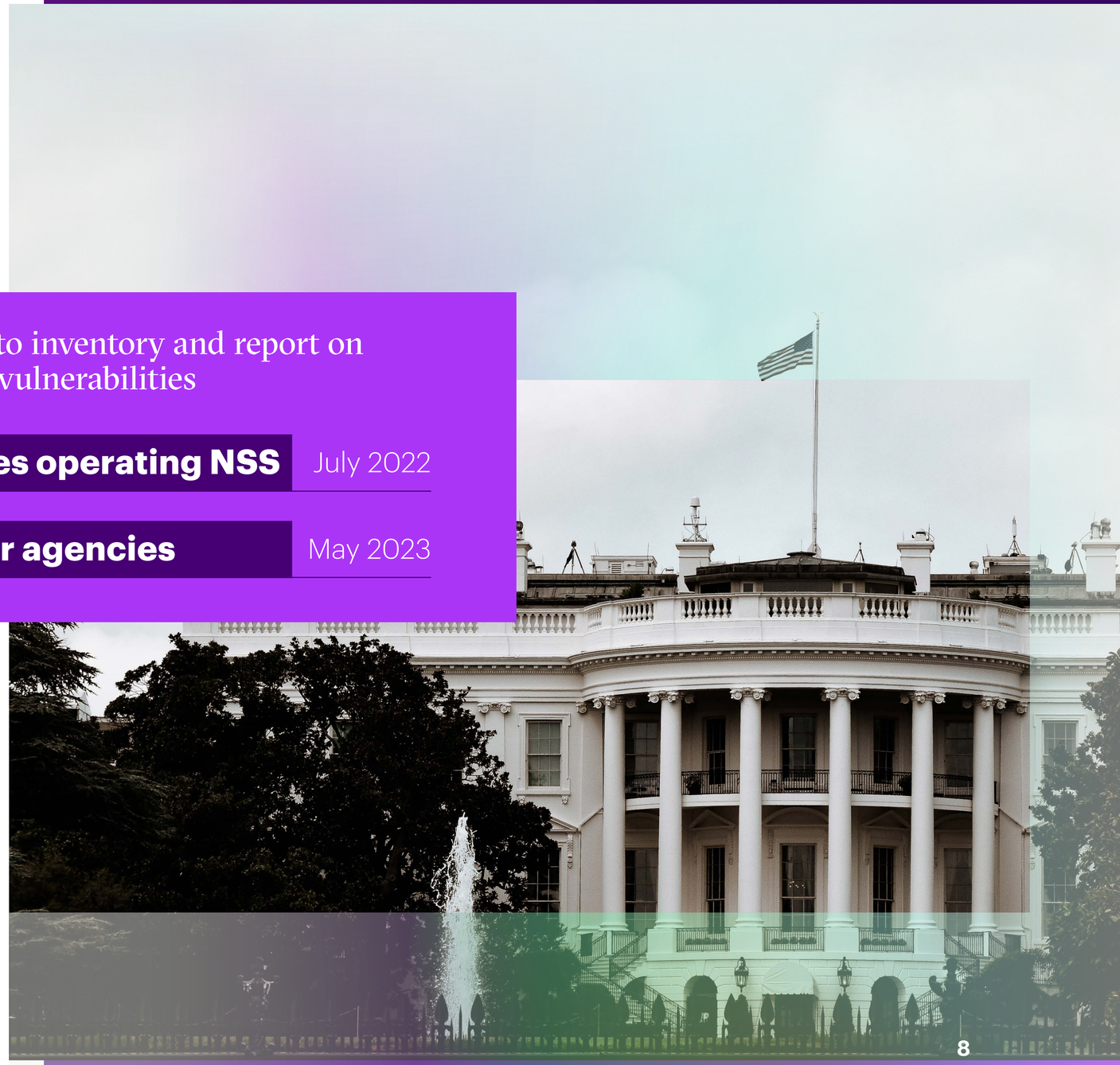
In the resulting reports, agencies must also prioritize their high-value assets and systems, and they must define—and ideally automate—a process for tracking their migration to quantum-resistant cryptography.

These requirements to inventory systems, prioritize assets, and track progress serve a longer-term intention of the White House directives: the realization of a **new and nimble approach to cybersecurity known as crypto-agility**.

[11] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (whitehouse.gov)
[12] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (whitehouse.gov)

Deadline to inventory and report on quantum vulnerabilities

Agencies operating NSS	July 2022
All other agencies	May 2023



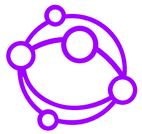
Crypto-agility: The key to compliance and enduring security

More than just a replacement for existing encryption technologies, crypto-agility enables an organization to quickly switch between algorithms, cryptographic primitives, and other encryption mechanisms.

Agencies that adopt a crypto-agile approach will be able to replace compromised keys and certificates without impacting the functions of mission-critical infrastructure.

Advantages of crypto-agility

Crypto-agility simultaneously solves for current and future threats. Key advantages include:



Agencies can support legacy and post-quantum cryptographic algorithms while in transition, enabling them to immediately safeguard high-value assets.

During the interim state, risk assessments can determine which assets can be protected with conventional cryptography while others require quantum-resistant methods or other mitigating controls.

Agencies can maintain continuous compliance and adopt the highest appropriate level of security as encryption and decryption technologies advance.

Agencies can gain access to advanced threat detection and response capabilities as those technologies are built into government cryptosystems, enabling agencies to detect previously unknown cryptography on their networks.

Agile vs. hasty: Avoiding the risks of unproven cryptosystems

Crypto-agility is not the hasty adoption of post-quantum encryption technologies. Flaws in unproven cryptosystems could expose data presumed to be protected and/or degrade system performance beyond acceptable levels.

Worse, if a threat actor creates a quantum-safe cypher that somehow makes its way into an agency's infrastructure, the entire system could be held ransom or permanently deleted by employing cryptographic erasure.[13]

[13] Cyprographic Erase (csrc.nist.gov)

Key elements and tooling for crypto-agility

At the heart of crypto-agile strategy is a defensive but practical mindset powered by ground truth. Crypto-agile strategy factors in the full scope of the agency's enterprise IT and operational technology and the current cryptography ecosystem that protects its digital assets. The strategy encompasses the agency's assessment and authorization (A&A) policies and procedures, which may require review and updating to ensure that future systems comply with the 2022 White House mandates.

Crypto-agility combines a strategy, a platform, and an operating model.

To operationalize the strategy, agencies will need an enterprise platform that uses a lightweight and scalable post-quantum framework API to integrate all endpoints throughout the network infrastructure—computers, mobile devices, terminals, etc.—as well as data stores, cloud storage and computing services, and supervisory control and data acquisition (SCADA) systems.

The purpose of a crypto-agile platform is to orchestrate security protocols and algorithms, provisioning quantum-safe encryption for data at rest and in flight as well as code signing for software updates. The API builds agility into the enterprise by enabling use of classical, hybrid, and fully quantum-resistant algorithms.

To implement and maintain crypto-agility, agencies may need to modify their cyber operating models and provide training for systems administration personnel. Modifications include integrating crypto-agile APIs and configuring them within devices and systems, as well as updating agency policies and security processes that govern authority to operate.

A crypto-agile system is one that is aware of all cryptography within the enterprise.

The platform and operating model support routine collection of cryptographic intelligence to quickly identify rogue cryptography, compromised algorithms, and other associated threats. The agency's cyber operating model must accommodate new feedback loops to ensure that this intelligence reaches security and organizational leaders responsible for the cryptography ecosystem.

Key features of a crypto-agile platform

Integration with crypto key management systems

Integration with identity and access management systems

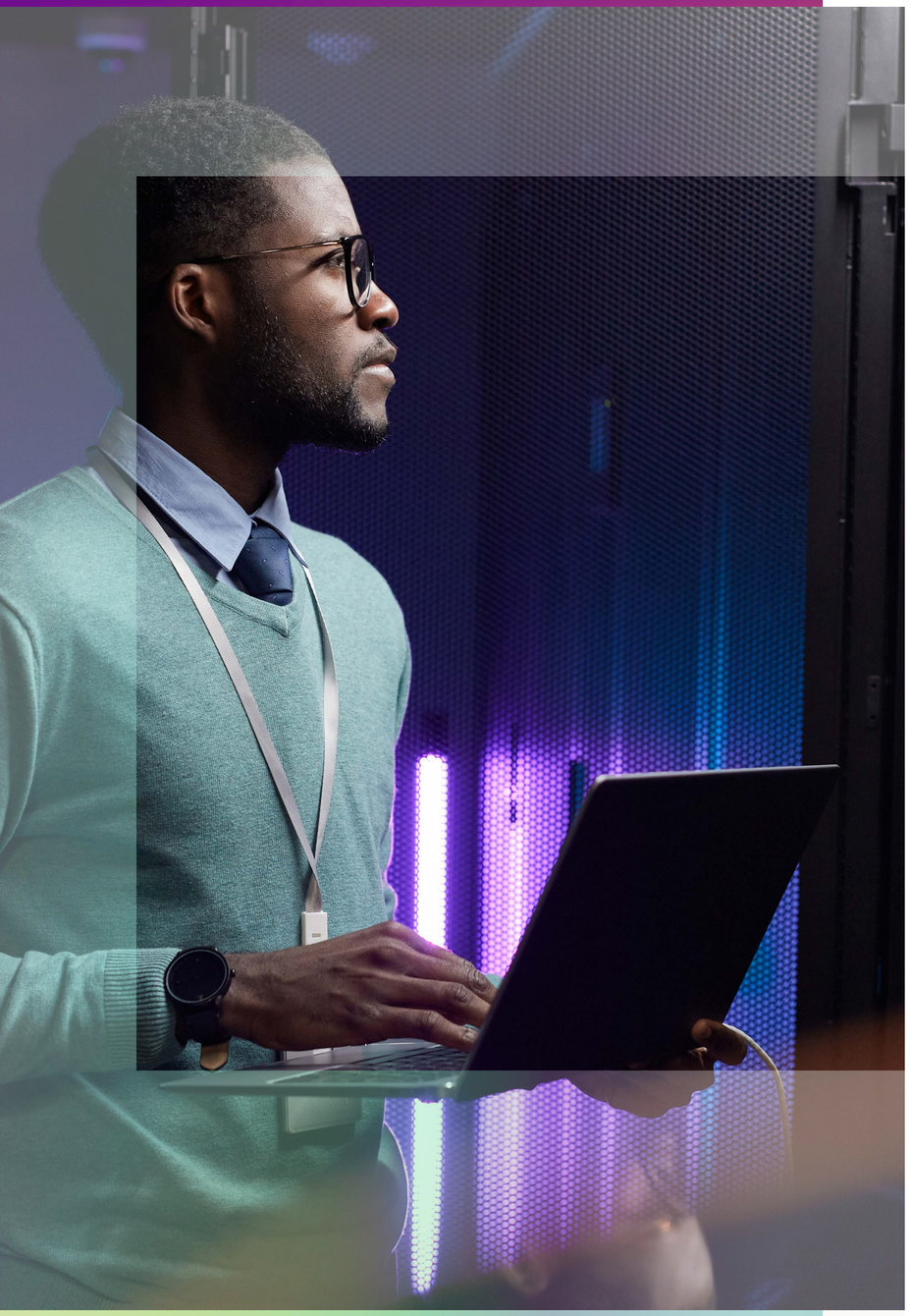
Secure virtual private network (VPN) that leverages quantum-secure algorithms

Monitoring of secure communication to inventory protocols and encryption algorithms

Dashboard for real-time monitoring and traceability of past events and discovery of unknown cryptography

Cryptography policy management

Machine learning automation to optimize performance



Crypto-agility, Zero Trust, and Cloud Smart

Driven by previous Executive Memoranda and Executive Orders, federal agencies have already begun investing in efforts to advance toward Zero Trust architecture—with the goal of making it a reality by 2024.[14] Among its other components, a mature Zero Trust architecture encrypts data in flight and at rest and uses cryptography as a means of authentication.

Similarly, the 2019 Federal Cloud Computing Strategy (aka Cloud Smart)[15] emphasizes the need for modernized security, data-level protections, and continuous monitoring, among other security features.

Following the release of Executive Order 14028[16] in May 2021, the Cybersecurity and Infrastructure Security Agency (CISA), Office of Management and Budget (OMB), and NIST appended requirements for federal agencies that focus specifically on adoption of a Zero Trust approach to cybersecurity.[17] NSM-8 extended these requirements to agencies that operate national security systems.

Crypto-agility allows agencies to simultaneously prepare for post-quantum threats and address Zero Trust and Cloud Smart requirements.

Together, these mandates and guidelines provide a path for agencies to effectively incorporate crypto-agility into their Zero Trust architecture and the Zero Trust model overall. Agency leaders can simultaneously address regulatory requirements associated with Zero Trust and Cloud Smart initiatives and the specific threats posed by quantum computing—maximizing the allocation of resources to comply with all three mandates.

The journey will be a long one, requiring tooling that can be integrated into agencies' existing crypto ecosystems and provide visibility into their post-quantum readiness.

[14] M-22-09 Federal Zero Trust Strategy (whitehouse.gov)
[15] Federal Cloud Computing Strategy (cio.gov)
[16] Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)
[17] Zero Trust Maturity Model (cisa.gov), Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators (crsc.nist.gov)

First steps: Launching the journey toward crypto-agility

The good news for agency leaders is that models and tools exist to meet the immediate-term requirements. By applying these models and tools, **agencies can begin the work of inventorying and auditing their current cryptographic posture without committing significant personnel or budgetary resources**.

The level of effort required to fully inventory and understand an agency's vulnerability to a QC-enabled threat actor is a function of the size and complexity of its enterprise network, including:

- Custom systems with embedded algorithms
- Legacy systems, including government-off-the-shelf (GOTS), which may contain legacy cryptography
- Disconnected or island networks
- The maturity of the agency's current cybersecurity and information assurance program

Given the depth, breadth, and sensitivity of information that must be compiled during the inventory process, **it is imperative that agencies fully vet any partner organizations they engage for support**.

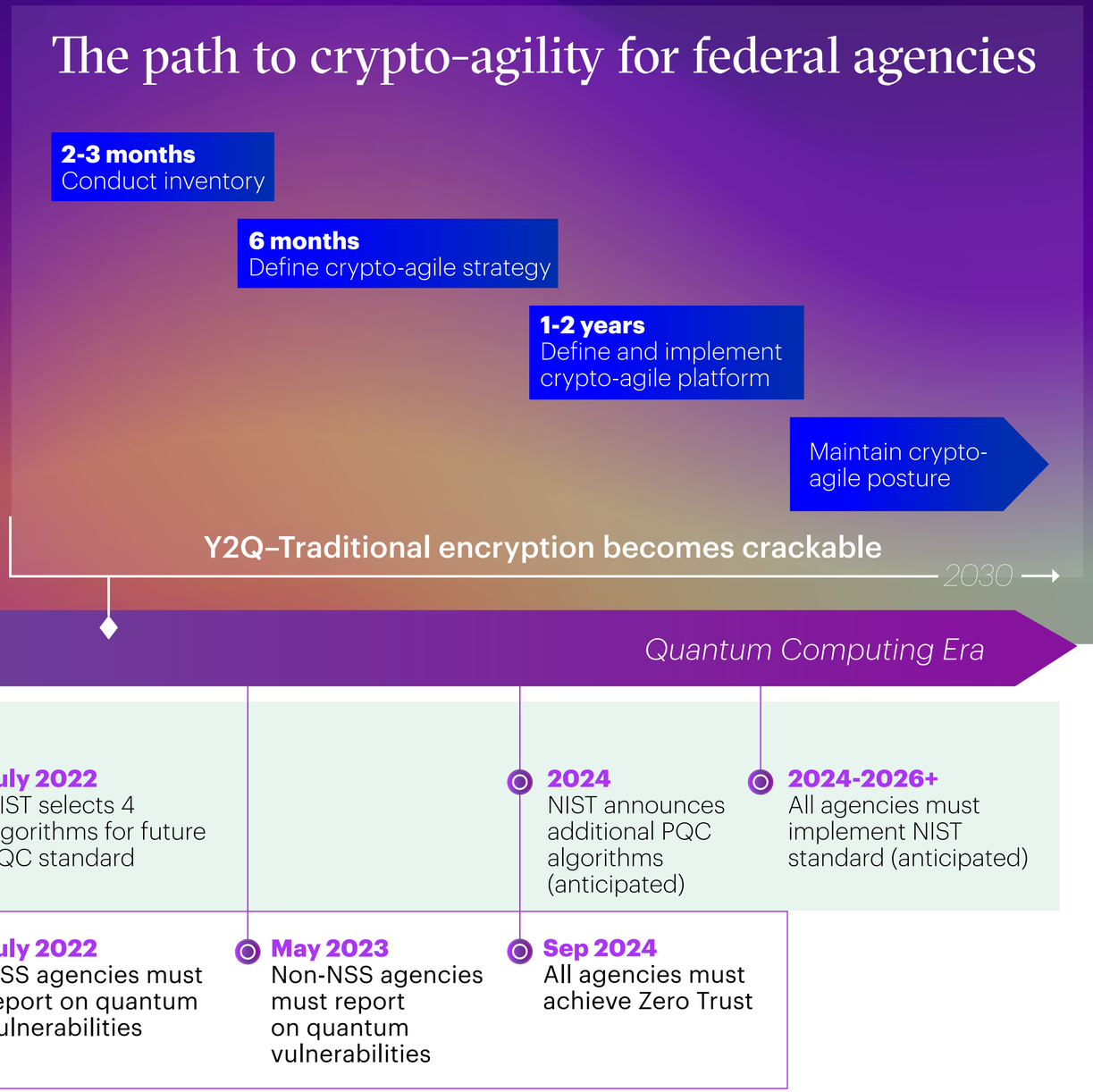
Empowered with a comprehensive inventory of their cryptographic posture, agency leaders can move forward with confidence, developing and implementing initiatives to achieve quantum-safe cryptosecurity and true crypto-agility. Critical outcomes of the inventory process will support agency planning and implementation efforts by:

Providing **critical inputs to formulate budgetary requests** to plan and implement a crypto-agile platform and operating model

Identifying systems **with legacy or out-of-date cryptographic standards** and other priority security updates

Prioritizing **updates to protect HVAs with quantum-resistant algorithms** (lattice-based and hash-based cryptography) to improve resiliency against quantum attacks

Timeline: Policy, compliance, and action on quantum computing



Enduring cyber-resilience for the American people

By adopting crypto-agility as a strategy, platform, and operating model, federal agencies can safeguard their information systems and communications against the post-quantum threats that are imminent today—and successor threats yet to be defined.

As federal agencies undertake efforts to comply with immediate-term requirements laid out by the White House, they can simultaneously perform the full scope of discovery needed to achieve crypto-agility—all as part and parcel of ongoing initiatives to achieve Zero Trust architecture and implement a modern, secure IT environment.

The aim—and result—of these efforts will be to imbue our Nation's cyber, economic, and national security with unprecedented and self-perpetuating resiliency.

Authors

Garland Garris
Senior Manager,
Quantum Security Lead

Accenture Federal Services

Major General George Franz (Ret.)
Managing Director, Defense
Cybersecurity Lead

Accenture Federal Services

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners, and communities. Visit us at **accenture.com**.

About Accenture Federal Services

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company headquartered in Arlington, Virginia. Accenture's federal business serves every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Visit us at **accenturefederal.com**.