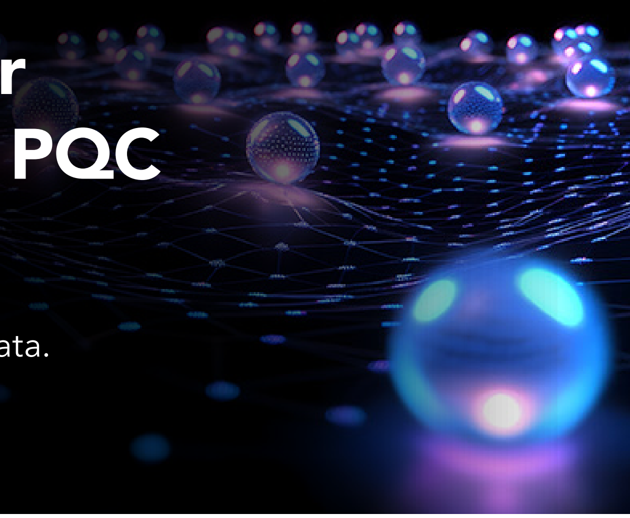
Government Readiness for Quantum Computing and PQC

A strategic guide to harnessing the benefits offered by quantum computing technology and implementing Post-Quantum Cryptography (PQC) to protect critical data.



For years, quantum technology remained largely confined to research labs and academic institutions, especially within national laboratories and government agencies. However, the landscape has shifted dramatically with the rise of cloud-based quantum computing. This development has broken down traditional accessibility barriers, empowering a broader community of developers and innovators to explore and build quantum-enabled solutions.

Alongside this technological evolution, there is a notable shift in mindset within government. Agencies are no longer merely funding or exploring quantum research—they are increasingly focused on how quantum technologies can address real-world operational challenges.

At the same time, the rapid pace of quantum advancement brings new urgency around preparedness. Governments must begin building quantum readiness, not only to take advantage of emerging capabilities but also to protect critical data and long-term investments from the disruptive potential of quantum breakthroughs, particularly in areas like cybersecurity and encryption.

In this report, four experts in quantum technology share their perspectives on how governments can strategically prepare for the quantum future to build both resilience and the ability to harness the full value of quantum innovation as it scales.

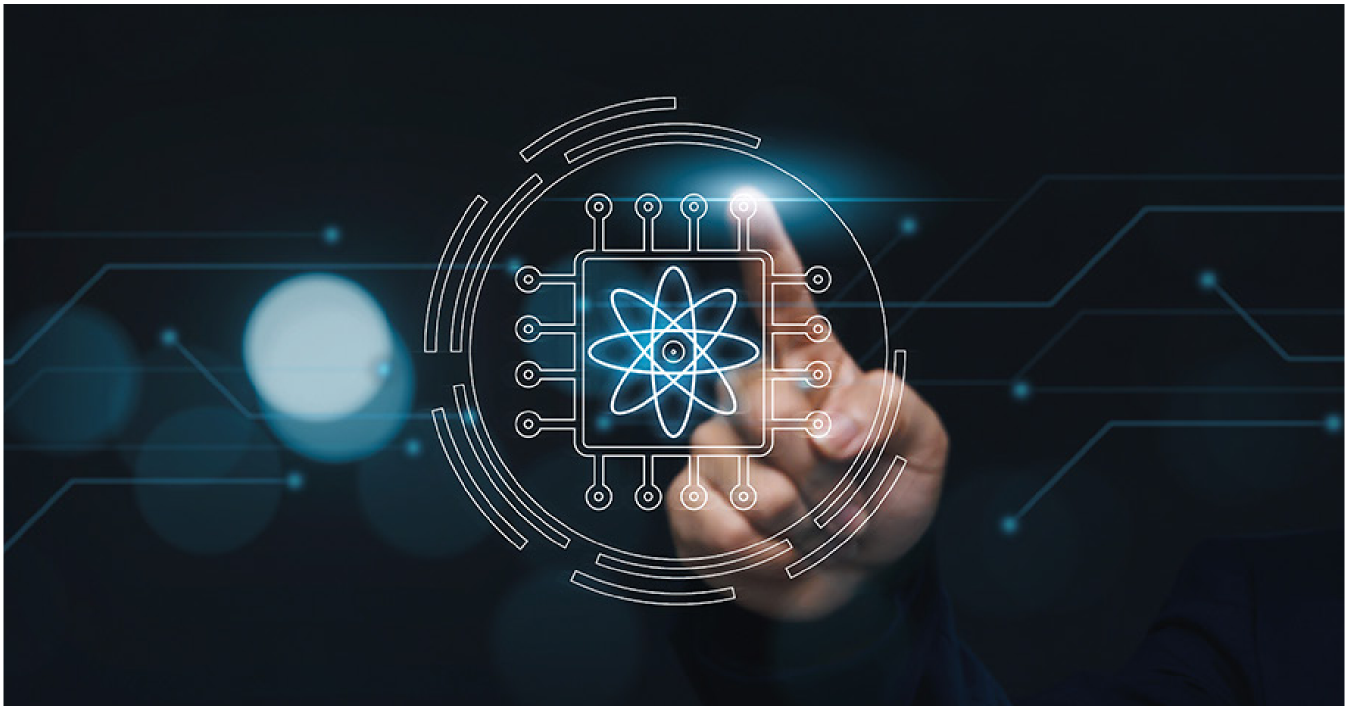
Quantum for Real-Time and Critical Applications

With the availability of quantum services in the cloud and the realization that classical computing is no longer sufficient for certain complex, time-sensitive, and resource-constrained problems, governments are now exploring how quantum technology can support mission-critical and real-time applications.

According to Allison Schwartz, global government relations and public affairs leader at D-Wave, another key motivator is the cost and energy efficiency offered by quantum, particularly for training artificial intelligence (AI) models. Quantum computing systems, especially annealing ones, are showing early potential as a key technology for accelerating and improving the efficiency of training large language models, which are expensive and computationally intensive when run on classical systems alone.

The integration of quantum computing with high-performance computing (HPC) and AI is also emerging as a practical and strategic solution, particularly as public-sector agencies grapple with shrinking budgets and growing demands for faster, more efficient service delivery.

> " There are a variety of applications that could benefit from the speed and the ability to look at all the different problems, and quantum can deliver those capabilities. "
>
> - Allison Schwartz, D-Wave



Schwartz highlights several examples where annealing quantum technology, like that offered by D-Wave, is helping or can help organizations and agencies optimize operations and make real-time decisions more effectively.

Category	Application Area	Use Case Examples	Quantum Benefit
Public sector optimization	Emergency response	Resource deployment during disasters	Real-time decision-making, broader scenario analysis
	Postal and cargo logistics	Mail delivery, cargo inspection, route planning	Faster, more efficient optimization
	Port operations	Cargo movement, crane scheduling, truck loading	Increased throughput, reduced delays
	Law enforcement resource management	Patrol planning, vehicle downtime reduction	Improved allocation, lower costs
National security and defense	Missile defense	Scenario analysis	Time-to-solution in seconds
	Military scheduling and maintenance	Fighter pilot shifts, helicopter readiness	Increased readiness, automated scheduling
	Defense logistics	Movement planning in contested areas	Rapid optimization under uncertainty
Telecom and infrastructure	Network optimization	5G/6G rollout, spectrum management	Real-time planning, cost savings

Category	Application Area	Use Case Examples	Quantum Benefit
Transportation and logistics	Traffic/transport planning	Vehicle routing, fuel usage planning	Scenario breadth, time savings
	Air traffic management	Aircraft routing	Congestion reduction, increased safety
	Fleet management	Planning preventative maintenance and scheduling repairs	Reduced maintenance costs, prioritizing repairs, and less vehicle downtime
	Government and contractor staff scheduling	TSA agent scheduling, law enforcement shifts	Time/cost savings, more effective personnel deployment
	EV charging station planning	Optimal station location planning	More scenarios evaluated
Disaster management	Wildfire mitigation	Fuel break line optimization	Less tree cutting, better containment
	Grid failure prevention	Cascading electrical outage prevention	Infrastructure resilience

“There are situations where a classical computing solution—whether it takes five minutes, five hours, or even five days—is perfectly adequate,” says Schwartz. “But in applications like real-time missile defense, emergency management, or scheduling a large workforce, where speed and complexity are factors, that is where you see quantum technology shine.”

Building Teams, Processes for Quantum Migration

When considering migration to quantum technologies, Gina Scinta, deputy chief technology officer at Thales Trusted Cyber Technologies (TCT), reminds us of what it was like when organizations were preparing for Y2K. “We knew that on January 1, 2000, some systems might break, and we just didn’t know what to expect.”

However, unlike Y2K, the timeline for quantum threats is uncertain. Scinta explains that the problem with quantum migration is that organizations don’t know when a cryptographically relevant quantum computer will be available. Experts estimate the year 2030, but adversaries may be ahead (or behind).

For this reason, agencies need to start coordinating and assigning dedicated resources, planning, taking inventory, prioritizing the most critical assets and data, testing solutions, and promoting cross-organizational collaboration to transition to PQC.

Agencies like the Cybersecurity & Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) have issued guidance, starting with manual cryptographic inventories. From there, agencies must prioritize systems that hold long-lived, sensitive data, such as healthcare records, intellectual property, and classified information. Scinta emphasizes, “the threat lies when bad actors steal data today and then decrypt it with a quantum computer later.”

The next step is to prepare for algorithm standardization. NIST’s standardization process began in 2016 and resulted in the release of three standardized PQC algorithms in 2024. Scinta points out that vendors have developed to the pre-standard, so now industry needs to tweak the algorithms to meet the standards. Agencies must choose solutions that incorporate crypto agility, enabling them to adapt seamlessly as algorithms evolve or become obsolete.

When testing, using a controlled environment is essential. Agencies should avoid testing in production environments and consider using dedicated PQC test setups. They may also need to upgrade some of their hardware, as many older systems may be using deprecated cryptographic algorithms and cannot support quantum-safe algorithms.

When considering hardware options, Scinta reminds agencies that hardware security modules and high-speed network encryptors, such as those offered by Thales TCT, are critical components in quantum-resistant infrastructure. They must support both classical encryption and PQC to maintain backward compatibility while adding quantum protection.

> “ Given the uncertainty surrounding the quantum timeline, agencies cannot afford to wait. The threat to long-lived data is already present, and adversaries may be stockpiling encrypted information today to decrypt in the future. ”
>
> - Gina Scinta, Thales TCT

However, by taking early, deliberate steps toward post-quantum cryptography, agencies can determine whether their critical systems and sensitive data will remain protected in the future.

Zero Trust and PQC

When implementing PQC, agencies must maintain the core tenets of Zero Trust, including continuous verification, least privilege, and breach containment. This includes:

- **Strengthened identity and access management:** Zero Trust relies heavily on strong identity proofing and secure session establishment. Most modern authentication methods, such as digital certificates, SSO platforms, and MFA devices, use public key infrastructure, which is vulnerable to quantum attacks. Migrating to PQC-compatible certificate chains and quantum-resistant identity mechanisms is essential for preserving integrity and trust in authentication workflows.
- **Quantum-safe certificate authorities:** To safeguard sensitive data and prevent any data loss, cryptographic key handling must be robust and secure. Any gaps or delays in key generation, storage, or exchange could undermine trust enforcement. Key management systems and hardware security modules must be upgraded to handle the new key formats and management practices required by PQC.
- **Secure communication channels:** Agencies should adopt updated versions of existing protocols and widely accepted standards, such as quantum-safe TLS (Transport Layer Security), SSH (Secure Shell), and IPsec (Internet Protocol Security), to implement quantum-resistant VPNs, secure tunnels, and other encrypted communication protocols to preserve the confidentiality and integrity of data flows across Zero Trust environments.
- **Secure software updates:** Zero Trust assumes continuous risk, even from sources within the agency's network. Post-quantum signature algorithms can be used to preserve the integrity and authenticate the source of software updates and patches.

By integrating PQC into these foundational elements, agencies can enhance their resilience against emerging threats, ensure long-term data protection, and maintain continuous trust, even in a future where quantum-enabled adversaries are a reality.

Use of Cryptographic Discovery Tools

With the advent of quantum computing—particularly cryptographically relevant quantum computers—current encryption methods are at risk of being easily broken, making sensitive government data vulnerable to threats like "harvest now, decrypt later" attacks.

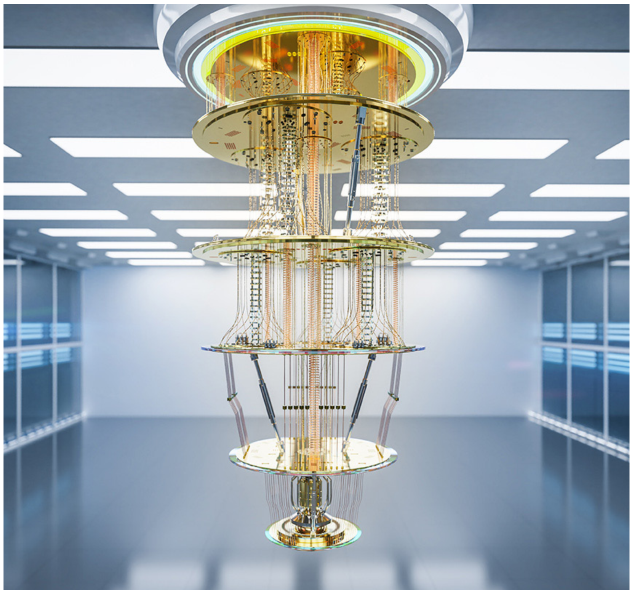
According to Vijay Viswanathan, vice president, product at ISARA, government agencies, particularly in the U.S., have begun addressing this threat. Initiatives like National Security Memorandum (e.g. NSM-10) and guidance from the Office of Management and Budget (OMB) and NIST are prompting agencies to inventory and assess their cryptographic assets.

However, current efforts are still in early stages, with many agencies struggling to compile accurate, comprehensive cryptographic inventories. Manual processes are proving inaccurate, lacking detail on plaintext communications, algorithms, protocols, key strengths, crypto assets, cryptography-consuming applications, and APIs. They also lack coverage. This shortfall hampers planning for migration to PQC and deploying Zero Trust architectures.

To achieve quantum readiness, agencies must start with an accurate inventory, followed by risk-based prioritization, roadmap development (for either mitigation or migration), integration of crypto agility, and alignment with Zero Trust principles.

Currently, most agencies remain at the inventory stage. Fortunately, solution providers like ISARA are offering options that automate inventory and prioritization through risk scoring, produce actionable insights, track roadmap progress, and validate quantum readiness. This allows agencies to move beyond manual, error-prone processes.

> " By having visibility into the cryptography used across their digital infrastructure, networks, systems, applications, data, etc., agencies can accurately assess their cryptographic needs, make data-driven decisions, protect their sensitive data, and become quantum-ready faster. "
>
> - Vijay Viswanathan, Isara



Pragmatic Approach to PQC-Readiness

Having an extensive list of assets, IP addresses, and algorithms is only part of the PQC process. According to Ben Packman, chief strategy officer at PQShield, agencies also need to examine their supply chain, which includes identifying and evaluating vendors that handle their most sensitive, long-lived data.

Packman recommends that agencies begin by identifying the data they care about most and mapping out which vendors and systems touch that data. This supply chain analysis offers the clearest and most actionable starting point for a PQC migration. From there, he suggests classifying vendors into three categories to streamline planning:

- **Infrastructure vendors (e.g., Cisco, Palo Alto, AWS):** These companies are already being pushed by U.S. federal mandates and will have PQC-enabled products. Agencies should contact these vendors, obtain roadmaps, and ensure any infrastructure refreshes already in budget are redirected toward PQC-compatible replacements.
- **SaaS vendors:** Though large in number, SaaS vendors often run on cloud-native infrastructure, making security upgrades more manageable. Since the SaaS market is highly competitive, vendors will likely adopt PQC to maintain feature parity. Agencies should utilize commercial leverage and regular contract renewals to promote the integration of PQC.
- **Custom or niche systems:** This category is the most complex and resource-intensive. These systems often involve long-term contracts or proprietary technology. Since change requests in this space can be costly, agencies should start by identifying bespoke applications that touch sensitive data and work with vendors like PQShield to plan PQC upgrades.

> " Take an 80/20 approach where you focus first on the systems and suppliers that handle the most valuable data and are within reach of influence. "
>
> - Ben Packman, PQShield

Procuring PQC Solutions

A critical yet often overlooked aspect of PQC migration is procurement. According to Packman, many failures begin with poorly framed RFPs or check-the-box questionnaires, such as "do you support PQC?"

Vendors can easily answer "yes" without delivering meaningful solutions. Instead, agencies must learn to ask more detailed questions, such as which parts of a device or system are PQC-enabled (e.g., bootloader, firmware, anti-counterfeiting chips), what algorithms are used, and their implications on performance and security.

Agencies don't need to become experts overnight; instead, they should work with vendors, trusted consultancies, and solution providers, like PQShield, to implement PQC in a way that's secure, scalable, and aligned with their mission. It is also important to recognize that this migration isn't purely a cryptographic exercise; some architectural changes may be necessary to fully optimize for new PQC schemes.

Preparing for the Quantum Future

As quantum computing transitions from theoretical research to real-world deployment, government agencies will gain the ability to solve complex optimization and simulation problems with significantly greater speed and efficiency.

However, preparing for quantum computing requires more than simply waiting for a cryptographically relevant quantum computer to arrive. Agencies must act now by assembling dedicated internal teams, allocating appropriate resources, and realigning their program and change management. They also need to start initiating foundational activities, such as automated inventories, comprehensive cryptographic visibility, and upgrades to their hardware, firmware, and software.

Equally important is ensuring that readiness extends beyond the IT department. Procurement teams, for example, must be equipped to ask nuanced and technically accurate questions about PQC capabilities in vendor offerings, going beyond checkbox compliance. Agencies must also verify that PQC solutions are aligned with Zero Trust principles, supporting continuous verification, least privilege access, and robust protection for sensitive data in transit and at rest.

Taking this proactive, organization-wide approach will help agencies not only build quantum readiness and harness the benefits of the technology but also strengthen long-term cyber resilience.

Carahsoft and its partners support Federal, State, and Local agencies, as well as Healthcare organizations and Education institutions as they migrate to quantum-proof encryption algorithms.

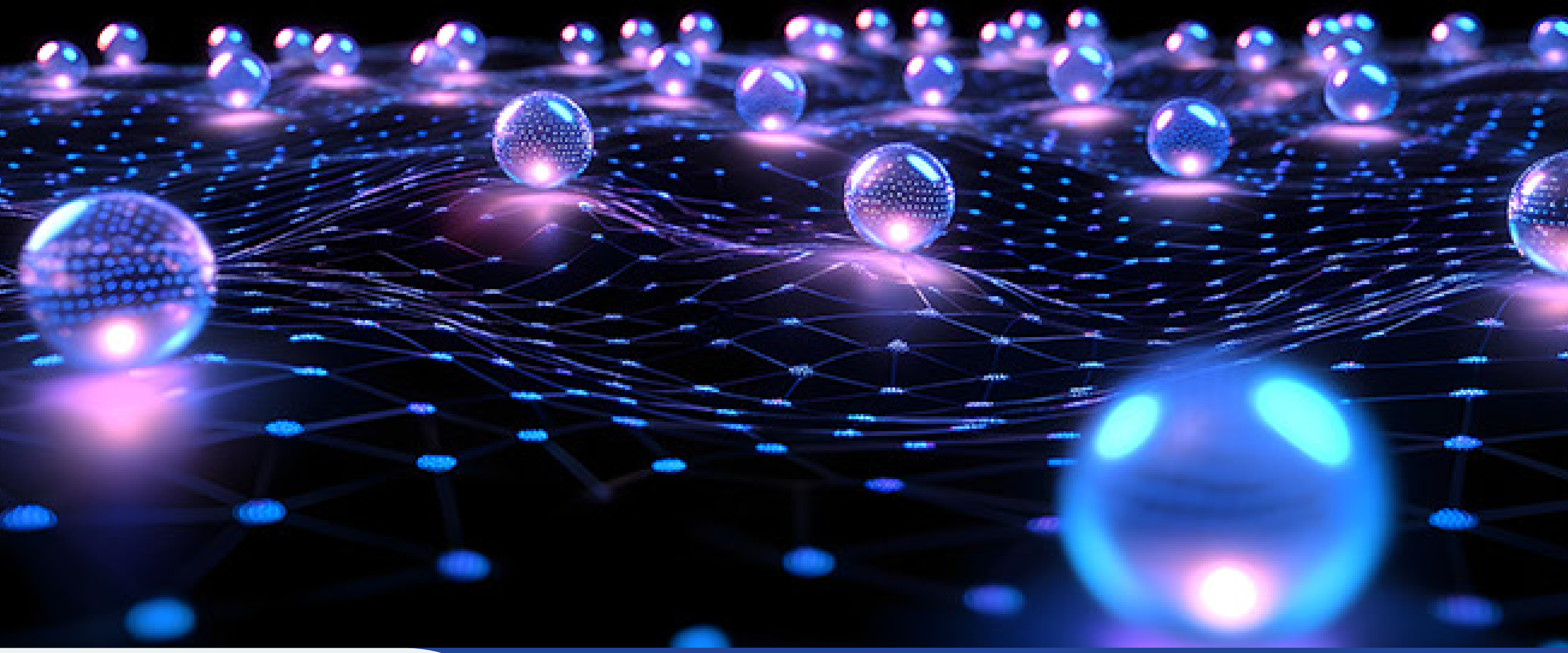
Contact the Quantum Team at Carahsoft to learn more.

✉ QuantumComputing@carahsoft.com

☎ (844) 214-4790

carahsoft.

Explore Carahsoft's portfolio of solutions at: **Carah.io/Quantum**



GovWhitePapers
Where Government Knowledge Gathers

Learn more about Quantum Computing on **GovWhitePapers.com**.