
# The Future at Quantum Speed

## Quantum Computing in the Federal Government

March 2025

Sponsored by:

**Accenture Federal Services**

# Why Quantum

Quantum computing, once a purely theoretical concept, is now poised to revolutionize technology and government with the ability to solve problems at never-before-seen speeds. Unlike traditional computers that process information in binary, quantum computers process information in qubits, which can exist in multiple states simultaneously. This enables quantum computers to conduct complex calculations and solve problems exponentially faster than classical computers ever could. Elements of quantum-based technologies are already used in things like Global Positioning Systems (GPS), Magnetic Resonance Imaging (MRIs), and semiconductors.

These unparalleled problem-solving capabilities have the potential to radically accelerate innovation in ways previously thought impossible. For the federal government, quantum could bring breakthroughs across nearly limitless potential use cases, including artificial intelligence (AI), weather forecasting, health sciences, cybersecurity, and many others.

# Beyond Encryption

While quantum computing and quantum information science promises a host of groundbreaking advancements, its arrival comes with considerable risks. One of the most alarming is its potential to undermine encryption methods currently used to safeguard data across every sector. Today's cybersecurity systems rely on cryptographic algorithms like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) to secure everything from emails to health data to military communications. When sufficiently powerful, quantum computers will be able to break these algorithms in mere seconds, exposing vast amounts of sensitive data.

## Preparing for a Post-Quantum Future

The U.S. government has already begun taking steps to prepare for a post-quantum world. A series of regulations and directives have been put in place to address vulnerabilities, secure funding for quantum-related projects, and set a timeline for the transition. Key regulatory frameworks include:

**National Security Memorandum 8 (NSM-8)**
Aimed at improving the cybersecurity of national security systems but mandating comprehensive assessments of quantum vulnerabilities across the Department of Defense and the Intelligence Community.

**National Security Memorandum 10 (NSM-10)**
Focused on promoting U.S. leadership in quantum computing while mitigating the risks posed to cryptographic systems by developing new, quantum-resistant cryptographic standards.

**HB7535 - The Quantum Computing Cybersecurity Preparedness Act**
Mandates compliance with M-23-02, signaling quantum cybersecurity as a clear federal priority.

Together, these regulations highlight quantum computing's double-edged sword: while it promises to enhance computational capabilities, it also presents existential risks to the current cybersecurity landscape.

These computers are also known as Cryptographically Relevant Quantum Computers (CRQC), and their emergence will mark a paradigm shift in cybersecurity, necessitating a swift transition to post-quantum cryptographic solutions.

To better understand how federal agencies are experiencing and interacting with quantum computing, Accenture Federal Services partnered with Market Connections to conduct a survey of 200 government technology decision-makers. Their responses paint a clear picture of how those at the forefront of quantum are addressing its rise.

# Insight 1:

## As global knowledge of quantum's capabilities grows and use cases increase, federal agencies are working to understand where quantum fits among their priorities.

The survey data indicates that there is already widespread understanding of quantum computing's potential. The majority (71%) of respondents recognize the benefits of quantum computing, and 61% agree that their organization understands the capabilities that quantum computing can offer. Most respondents see quantum as an enabler for AI/ML (Artificial Intelligence/Machine Learning) systems and predictive modeling, the most cited use cases for respondents (57% and 52%, respectively). These impacts are significant – the speed at which quantum computing can solve complicated problems, perform data-heavy analysis, and simulate complex systems like weather patterns or national security threats will be a game changer for agency decision-making capabilities. Respondents who are more IT-focused are more likely to call out quantum cryptography and key distribution and their related cybersecurity opportunities and threats.

However, despite this broad understanding of quantum's potential impact, 65% of respondents admit their organizations are slow to adopt quantum technology. One key reason may be that quantum computing is seen as more of a long-term opportunity than a short-term need, and agencies may be reluctant to divert resources from more immediate cybersecurity, modernization, or other competing priorities.

In fact, 58% of respondents categorize quantum computing as either a medium or low priority for the next 12–24 months. Although quantum represents a future threat to encryption, it is perceived as less of a priority compared to the more immediate needs of fortifying existing systems against present-day attacks, using present-day technology.

Investment levels reflect this hesitation. Forty-one percent of respondents report that their organization has made only minimal investments in quantum technology, while another 19% report no investment at all. This investment level is in stark contrast to the private sector, where big tech companies have been investing in quantum research and design (R&D) for years, including IBM, Microsoft, and Google.

Some agencies are leaning forward in this space, including NASA, where 54% of respondents indicated that quantum computing is a significant (although still not top) priority. NASA has made notable investments in quantum technology to advance its work in space exploration, optimization of spacecraft trajectories, and simulation of planetary systems, particularly through its Quantum Artificial Intelligence Laboratory (QuAIL). The Department of Energy also announced in September of 2024 that they were investing $65 million in funding for 10 projects, comprising 38 separate awards, and the 2024 National Defense Authorization Act included funding for a quantum pilot program.

For other agencies, however, quantum computing has not yet reached a tipping point that drives large-scale investment. This "wait-and-see" approach could potentially leave organizations unprepared for the rapid technological shifts that quantum breakthroughs may bring.

# Insight 2:

## Agencies expect serious threats from quantum computing in the near future.

While quantum adoption may be slow, there is widespread concern about the threats quantum technologies pose, particularly in cybersecurity. Many federal agencies recognize the magnitude of these threats, and they expect to face them sooner rather than later. Today's encryption methods are based on mathematical problems that would take even the most advanced classical computers an unreasonable timeframe to solve. Quantum computers, however, can solve these problems exponentially faster. A CRQC could decrypt sensitive information across defense systems, financial institutions, healthcare organizations and critical infrastructure within moments — a potentially catastrophic scenario for national security.

Respondents are highly aware of the threats potentially breakable encryptions pose. Respondents are most concerned about cyber espionage, with three quarters reporting that it is very concerning or their top concern. Espionage is closely followed by compromised key public infrastructure, the weaponization of quantum technologies, and cryptographic vulnerabilities (73% each) and data security breaches (72%).

And these are not considered distant threats. Survey results show that 57% of respondents expect quantum threats to manifest within the next 2-5 years, while 17% see quantum-related security risks as a concern within the next two years.

# Post Quantum Cryptography

The concern around encryption is particularly urgent given the growing concern that malicious actors are already engaging in "harvest now, decrypt later" tactics, where they collect encrypted data now in the hopes that a quantum computer will eventually be able to decrypt it. This poses a significant challenge to organizations managing sensitive or classified data, as information that remains secure today may be compromised in just a few years.

To combat this, it is more crucial than ever that agencies develop and implement post-quantum cryptographic algorithms that are resistant to quantum attacks.

While many agencies have begun preparing for this post-quantum future, survey results show a concerning gap between the acknowledgment of the risks and the actions being taken to mitigate them. Given the timeline for the arrival of cryptographically relevant quantum computers, federal agencies must act quickly to transition to quantum-resistant cryptography.

## NIST and PQC Standards

On August 13, 2024, NIST released its much anticipated post-quantum cryptography (PQC) standards, marking a significant milestone in quantum cybersecurity preparedness.

These standards include:

- **FIPS 203:** Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM)
- **FIPS 204:** Module-Lattice-Based Digital Signature Standard (ML-DSA)
- **FIPS 205:** Stateless Hash-Based Digital Signature Standard (SLH-DSA)

These standards define algorithms that are specifically designed to resist quantum attacks, ensuring that encryption and digital signature schemes can withstand the power of future quantum computers.

# Insight 3:

## Gaps in skills and education must be bridged for effective quantum adoption.

One of the most significant barriers to quantum computing adoption in the federal government is the skills gap. A majority (77%) of respondents believe that having the right talent and identifying skills gaps are significant barriers to their organization's ability to adopt quantum computing. Quantum computing is a highly specialized field, requiring knowledge of quantum mechanics, advanced mathematics, computer science, and cryptography.

Survey data reveals that federal agencies are acutely aware of the need for these skilled hires. Over half (59%) of respondents believe that their employees lack the technical knowledge necessary to implement quantum computing solutions. Two thirds (66%) of respondents state that their agency doesn't have enough resources to pursue quantum adoption effectively. This raises another problem: even if federal employees had the necessary knowledge, many agencies lack the budget or infrastructure to support quantum computing initiatives. For IT departments who often focus their constrained budgets on immediate needs such as cybersecurity, cloud migration, or infrastructure modernization, quantum computing may feel like a long-term goal with less immediate payoff.

Another major challenge is the lack of awareness surrounding key regulations and standards that are essential for quantum adoption. Just over half of respondents are familiar with M-23-02. Both regulations are critical to ensuring that federal systems will remain secure in a post-quantum future. This lack of familiarity suggests that there is a significant gap in both education and communication within federal agencies when it comes to understanding and preparing for quantum computing risks. These regulations are not simply guidelines; they represent a legal requirement for transitioning to post-quantum cryptography. Without a firm grasp of these mandates, agencies are at risk of falling behind in preparing for the quantum era, which could expose critical systems to breaches and other security vulnerabilities.

## Training and Workforce Development

The federal government's success in the quantum future will depend heavily on its ability to train and upskill its workforce, and respondents agree – 61% of respondents believe that training and educating the federal workforce is the primary factor in ensuring quantum adoption. This suggests that federal agencies understand that they need to take a proactive approach to workforce development, including identifying specific knowledge gaps, creating targeted training programs, and ensuring that employees are up to date on the latest developments in quantum computing and cryptography.

This development does not have to be done in a vacuum – in fact, the specialized expertise will likely require close collaboration between federal agencies, academic institutions, and private sector companies. As quantum computing continues to evolve, having the right talent, expertise, and partnerships in place will be essential for navigating the opportunities and risks that lie ahead. Harnessing the power of quantum will depend not only on technological innovation, but on a strong foundation of expertise.

# Best Practices for a Quantum-Ready Future

The rapidity of quantum's evolution, which is still nascent but growing exponentially, poses both challenges and opportunities. Federal agencies need to start preparing now, including building the infrastructure to support their effort. Preparing early for a quantum future means being able to harness its opportunities and insulate against its threats.

Key steps to take now include:

### CONDUCT CRYPTOGRAPHIC RISK ASSESSMENTS

Agencies should conduct thorough evaluations of their existing cryptographic systems, focusing on compliance with HB7535 and alignment with the latest NIST PQC standards. Inventorying encryption protocols is crucial for understanding the assets most vulnerable to quantum threats. Aligning with the latest quantum regulations is a crucial (and urgent) first step in any post-quantum migration plan.

### ALIGN WITH EXISTING ZERO TRUST EFFORTS

Agencies are required by M22-09 to develop a Zero Trust migration strategy, moving away from perimeter-based security. Agencies have an opportunity to align their Zero Trust and Post-Quantum Cryptography efforts by mapping how cryptography is used throughout each of the Zero Trust Pillars. In doing so, agencies can create an integrated ZT PQC Transition Strategy utilizing the same resources.

### EVALUATE AND ADDRESS THE SKILLS GAP

Shoring up a strong workforce is crucial. Agencies must evaluate their current talent pool, identify knowledge gaps, and look for ways to upskill their employees or bring in additional expertise. These educational and training interventions should not be one-offs, but rather long-term plans to build an adaptable and educated workforce that is able to evolve along with quantum computing itself.

**66%**
of respondents state their agency doesn't have enough resources to pursue quantum adoption effectively.

**61%**
believe training and educating the federal workforce is the primary factor in ensuring quantum adoption.

**59%**
believe their employees lack necessary technical knowledge to implement quantum computing solutions.

### BUILD STRATEGIC PARTNERSHIPS

Navigating quantum computing will require cooperation across all sectors. Collaboration with industry partners, academic institutions, and other government entities will be key to staying ahead in quantum innovation, developing solutions to shared problems, and mitigating risks.

### THINK INCREMENTALLY

Most respondents agree that, while agencies need to begin thinking about their quantum transformation now, its adoption should be incremental in order to reap the most benefits while mitigating the most risk. Using pilot projects for immediate use cases can help agencies find the benefits of quantum within their own missions as well as containing possible downsides as much as possible.

By taking these proactive steps, agencies will be well-positioned to both capitalize on quantum's vast potential and protect themselves from its inherent risks.

## Preparing for a Quantum-Resilient Future

Quantum computing presents a dual challenge: while it offers immense potential for advancing technology, it also poses a significant and near-term risk to cybersecurity. Federal agencies must prioritize quantum readiness, adopt post-quantum cryptography, and implement new security protocols if they are to stay ahead of this emerging threat and potential consequences, ranging from cyber espionage to the collapse of critical infrastructure systems. As the quantum era fast approaches, the time for agencies to prepare is now.

# About

## Accenture Federal Services

Accenture Federal Services is a leading US federal services company and subsidiary of Accenture LLP. We empower the federal government to solve challenges, achieve greater outcomes, and build a digital core that is agile, smart, and secure. Our 17,000 people are united in a shared purpose to advance our clients' mission-critical priorities that make the nation stronger and safer, and life better for people. We draw out the best of Accenture's global network in nearly every industry, bringing proven commercial innovation to solutions built with advanced R&D, emerging technologies, and human-centered design at speed and scale. Together, we help clients create lasting value for their workforce, customers, and partners and make a difference for the country and our communities.

See how we make change that matters at: www.accenturefederal.com.

Market Connections™
Research you can act on.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education.

For more information visit: www.marketconnectionsinc.com.