GENERAL DYNAMICS
Information Technology

RESEARCH STUDY

Quantum Waves

Agency Guide to Post-Quantum Cryptography

As quantum computing advances, it's bringing a wave of unprecedented risks and a pressing need for agencies to adopt post-quantum cryptography (PQC) to secure sensitive data. The stakes are high: the security of our nation's most sensitive data is at risk from adversaries who could exploit future quantum capabilities to decrypt information harvested today. With NIST's quantum-resistant algorithms now finalized, this report explores the proactive measures driving successful post-quantum cryptography migration ensuring national security in this new era.

In partnership with

IBM

Foreword

A wave of new risks is approaching as technology continues to advance. Quantum technologies promise enhanced innovation but also bring unforeseen risks. Encryption is a fundamental aspect to cybersecurity, securing intellectual property, financial data, health information, and national defense secrets. Without encryption, safeguarding data is nearly impossible. Encryption has become second nature and a mandatory requirement within almost all cybersecurity standards today.

However, quantum computers have the potential to break current cryptographic standards, exposing sensitive information to adversaries who are already harvesting encrypted data, with plans to decrypt it in the future—in hopes of accessing “cryptographically relevant” quantum computers. Post-quantum cryptography (PQC) is not just a technical upgrade; it is a critical step in protecting national security against these imminent risks.

This challenge brings new attention to the importance of encryption as new quantum algorithms are developed. There is a growing awareness of the risks, and government agencies are stepping up to meet these challenges—sifting through expert guidance, developing strategies, allocating resources, and adopting new capabilities to ensure their missions continue securely.

This report offers a comprehensive analysis of PQC readiness across government, combining the technical and mission-driven expertise of GDIT and IBM to deliver actionable strategies and practical measures to secure sensitive data.

Our research underscores the urgency of developing a robust PQC strategy, prioritizing and migrating at-risk data, and preparing both the workforce and enterprise for the challenges ahead.

As we face one of the most profound shifts in modern cybersecurity, achieving cryptographic agility is essential. By preparing now and building flexible, scalable strategies, agencies can ensure their missions remain resilient against future quantum risks.

DR. MATTHEW McFADDEN
Vice President
Cyber
GDIT

Executive Summary

Quantum technologies are poised to revolutionize industries by transforming weather forecasting with unprecedented accuracy, advancing healthcare through groundbreaking drug discovery, and securing the most sensitive communications. These advancements are just the beginning, with quantum computing, quantum communications, and quantum sensing offering government agencies unprecedented opportunities to enhance their capabilities.

However, alongside these advancements comes a formidable challenge. Quantum computers could also break the encryption methods currently used to protect our most sensitive data, making the transition to quantum-safe solutions both critical and complex. Government agencies are now at a critical juncture. While quantum computing offers immense potential for innovation, it also presents new security risks. Agencies must proactively transition to PQC to safeguard sensitive data against future risk, even as they explore the broader capabilities of quantum technologies.

The initial standards for PQC are ready for immediate use. Agencies now have the opportunity to move swiftly toward these modernized standards, ensuring they stay ahead of potential risks. While the path to PQC will require thoughtful planning and coordination, agencies are well-positioned to navigate this transition. This report provides clarity to understand how agencies are approaching the transition, covering strategy, resource alignment, and the necessary technologies for PQC migration.

NEW STANDARDS

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

ML-KEM (originally known as CRYSTALS-Kyber) and ML-DSA (originally CRYSTALS-Dilithium) were developed by IBM researchers in collaboration with several industry and academic partners.

WHO WE SURVEYED

GDIT's Digital Consulting Practice partnered with an independent research firm, to design an online survey of 200 cybersecurity experts working across the federal government — 100 at defense agencies, 50 at civilian agencies, and 50 at intelligence and homeland security agencies. Respondents were GS-12 and above and involved in either the selection or management of firms that provide enterprise IT or digital modernization services. These respondents represented a cross section of individuals who are highly knowledgeable of and directly participate in cybersecurity and post-quantum cryptography projects in their roles. The survey was conducted in July and August 2024.

1

STRATEGIC PLANNING IS UNDERWAY

50% of respondents report that their agencies are actively developing strategies for PQC readiness, while 35% are in the process of defining their plans and budgets. This reflects a growing awareness of the importance of preparing for quantum security challenges. As agencies continue to refine their approaches, they are laying the essential groundwork to protect critical systems against future quantum risks.

Agencies should focus on resourcing and strategizing toward quantum-resistant cryptography, prioritizing their most sensitive systems first.

2

GUIDANCE IS EVOLVING

37% of respondents cite a lack of formal guidance and strategic frameworks as a key challenge to PQC implementation. The relatively new nature of PQC means standards and best practices are still being defined. While agencies are aware of the importance of PQC, many agencies need clearer roadmaps and actionable strategies to make meaningful progress.

Establishing a well-resourced PQC governance team, supported by a formal strategy, will help agencies champion this transition and ensure critical systems are prioritized.

3

MODERNIZING LEGACY SYSTEMS

Modernizing legacy systems often poses a challenge for organizations, and 48% of respondents report this is a significant barrier to PQC adoption. Additionally, 29% of respondents point to operational technology (OT) systems as a complicating factor. In all, these systems were not designed to support modern cryptographic standards and often rely on specialized hardware and software, making them difficult to update.

Agencies should focus on a remediation strategy for legacy systems, exploring bolt-on solutions as interim measures, until these systems can be modernized to meet PQC standards.

4

PRIORITIZING VULNERABILITY MANAGEMENT

With 44% of respondents prioritizing vulnerability management, this capability is critical for identifying and addressing weaknesses in cryptographic systems before they are exploited. It allows agencies to create detailed inventories of assets, enabling them to better secure their environments against potential quantum risks.

While 21% cited challenges with automating discovery and risk assessment, agencies should continue maturing existing cybersecurity tools, like vulnerability management, to streamline risk identification, discovery, and assessment processes.

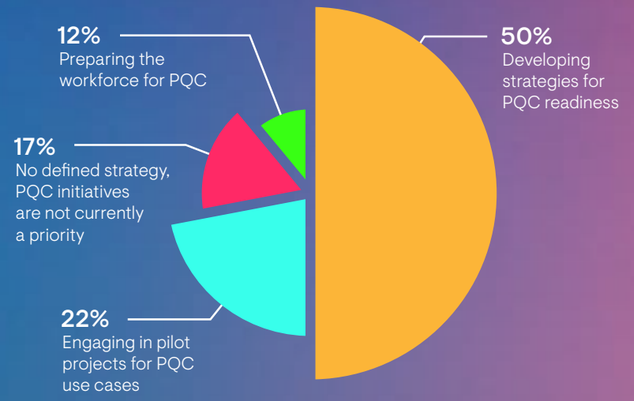
Navigating the Quantum Transition

As quantum computing draws closer, the need for government agencies to adopt PQC becomes increasingly urgent. Ensuring the security of sensitive information in the face of quantum risks requires comprehensive strategies, dedicated resources, and leadership.

Building Momentum

Half of the respondents surveyed are developing strategies for PQC readiness, yet many still lack clear roadmaps or dedicated resources. While 22% are engaged in pilot projects and 12% are preparing the workforce, nearly one in five (17%) has yet to prioritize PQC initiatives.

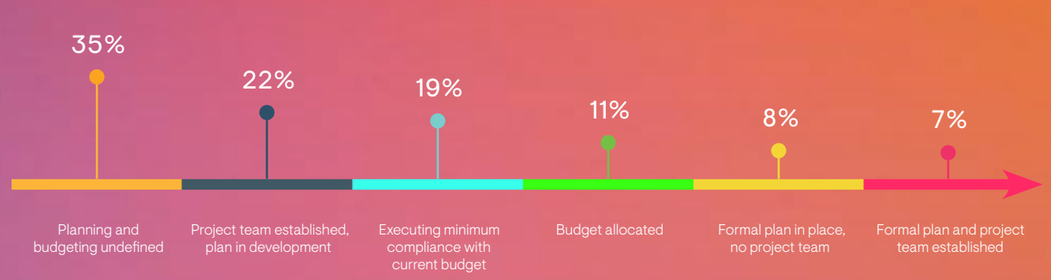
With the NIST standards for PQC now established and prioritized by the Office of Management and Budget (OMB), agencies must accelerate their efforts by allocating resources to create and implement quantum-resistant cryptography strategies, focusing on their most critical and high-value systems. Inventorying all vulnerable assets is important to make informed decisions about prioritization and resourcing.



Turning Awareness into Action

Although 35% of respondents have initiated planning and budgeting for PQC, most remain in the early stages of transition.

To ensure successful implementation, agencies need to establish well-resourced PQC governance teams to lead the transition. These teams should conduct comprehensive inventories, ensuring a clear understanding of the systems and assets at risk. In particular, agencies should move beyond lists of high-value assets to ensure the transition prioritizes legacy systems, ensuring that all vulnerable areas are addressed.



Facing the Future

Most respondents are still in the early stages of assessing their cryptographic risks—just 8% have fully integrated PQC standards.

As PQC standards continue to evolve, it is essential that agencies develop strategies to discover, assess, and manage cryptography risks continuously. This includes compiling a roadmap for PQC migration, identifying systems most vulnerable to quantum risks, and establishing a timeline for implementing quantum-resistant cryptographic solutions. The ability to consistently monitor and update cryptographic systems will be crucial as new algorithms and standards are adopted.

46%
We have identified key areas but have not begun formal assessment

37%
We have partially assessed risks but have not fully integrated new practices

10%
We have not yet examined cryptographic integration or assessed related risks

8%
We have fully assessed and integrated current cryptographic standards and risks

Streamlining PQC Integration

As agencies embark on the transition to PQC, integrating new cryptographic standards offers both opportunities and challenges. The process involves navigating their existing infrastructure while ensuring a thoughtful approach to planning and execution.

Strengthening Cryptography Management

Agencies face several critical challenges in transitioning to PQC that can stall progress if not addressed strategically.

37%
LACK OF PLANNING, GUIDANCE, AND STRATEGY

LACK OF FORMAL PLANNING

More than two-thirds of respondents (37%) reported an absence of formal guidance and strategic frameworks, making it difficult to effectively manage the PQC transition. Agencies should prioritize developing comprehensive PQC strategies that include long-term plans, clear guidelines, and a focus on discovery, assessment, and management of cryptographic assets.

24%
INTEGRATING PQC INTO SUPPLY CHAIN

INTEGRATING PQC INTO THE CYBERSECURITY SUPPLY CHAIN

For 24%, integrating PQC into the supply chain remains a significant challenge. Many have yet to incorporate PQC considerations into procurement processes. To ensure compliance with PQC standards, agencies should focus on selecting vendors who align with new FIPS standards, streamlining vendor selection, and reducing risks in product acquisition.

17%
POOR MANAGEMENT OF CRYPTOGRAPHY IMPLEMENTATIONS

MANAGING ENTERPRISE-WIDE CRYPTOGRAPHY

17% of respondents say their agency is struggling with managing cryptographic systems across their enterprises. This lack of visibility makes it difficult to prioritize PQC implementation effectively. By adopting automation tools, agencies can better assess and manage cryptographic assets dynamically, ensuring continuous oversight and progress toward PQC adoption.

14%
LIMITED AUTOMATION FOR RISK DISCOVERY AND ASSESSMENT

INSUFFICIENT AUTOMATION FOR CRYPTOGRAPHIC MANAGEMENT

14% lack sufficient automation tools to manage the discovery, assessment, and prioritization of cryptographic assets. Investing in automation technologies will provide agencies with holistic visibility into cryptographic systems, streamlining the PQC migration process and allowing for proactive risk management.

4%
LOW VISIBILITY INTO SYSTEM DETAILS

4%
NO CHALLENGES FACED YET

Adapting Legacy Systems for Quantum Readiness

Legacy systems often present challenges in digital modernization efforts across the government, from migrating to the cloud to implementing zero trust architectures. These older systems, while critical to operations, are not always compatible with new technologies, making upgrades difficult. Similarly, in the transition to PQC, 48% of respondents identified legacy systems as a significant barrier to achieving cryptographic readiness.

While these systems vary in complexity, a well-thought-out remediation strategy that includes both interim and long-term solutions will allow agencies to continue progressing toward PQC readiness.

However, agencies can mitigate this challenge by implementing interim solutions like bolt-on technologies, which provide a secure stopgap while full modernization efforts are underway. These technologies allow agencies to protect sensitive assets without needing immediate, large-scale system upgrades, ensuring progress continues without delay. As funding and resources become available, these strategies ensure that challenges don't become roadblocks, but instead, part of a phased, manageable transition plan.

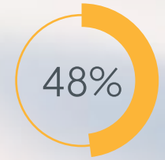
Securing Operational Technology

Operational technology (OT), used to control critical infrastructure, presents additional challenges, with 29% citing this as a complication. Many OT systems are not designed to meet modern cryptographic standards, but agencies can bridge this gap by implementing PQC-specific technologies. These solutions can secure connections between older OT systems and quantum-resistant cryptography, ensuring that essential infrastructure remains protected during the transition.

Managing Decentralized and Unknown Systems

Non-centralized systems (17%) and unknown systems (7%) further complicate PQC readiness. Without clear visibility into all cryptographic assets, agencies face difficulty managing and securing these systems. To address this, agencies should prioritize discovery and assessment tools that can provide a comprehensive inventory of cryptographic assets. Agencies can then phase in interim security measures while planning long-term solutions to ensure that all critical systems are protected.

GREATEST ANTICIPATED IT OR SYSTEMS-RELATED BARRIERS



Significant impact on legacy systems

Implications for operational technology

Difficulties with non-centralized systems

Challenges due to unknown systems

Building Quantum-Ready Defenses

As agencies progress toward PQC, building a resilient security framework requires identifying and prioritizing the most critical capabilities. These foundational capabilities are essential in navigating the complex PQC transition and ensuring long-term protection against quantum risks.

Powering Up PQC Readiness

Identifying and prioritizing the most critical capabilities is essential for ensuring a smooth and effective transition.

44%

Vulnerability Management

Vulnerability management allows for the remote discovery of cryptographic assets, including certifications and public-key cryptography, creating a comprehensive inventory of assets like algorithms, ciphers, hardware, and software. This capability has proven particularly effective in helping agencies respond to PQC inventory requests from the Office of Management and Budget (OMB).

Agencies should continue to enhance vulnerability management to mature the discovery and assessment process, ensuring they can identify and prioritize vulnerable post-quantum cryptographic assets.

41%

Security Information and Event Management (SIEM)

SIEM systems overlay PQC-related information onto existing security and vulnerability data, delivering an effective inventory of cryptographic assets.

Agencies should use SIEM to correlate and overlay information, enabling a clearer understanding of asset relationships, shared certificate information, and risks, which allows for more effective prioritization of their PQC migration strategy.

27%

Cybersecurity and Software Supply Chain Management

This capability manages cryptographic risks within the software supply chain, ensuring vendors align with the new PQC FIPS standards.

Agencies should focus on selecting product vendors that meet these standards, integrating supply chain considerations into the PQC transition process.

21%
Data Discovery

19%
Passive Monitoring

9%
Key and Certificate Management Solution

4%
Endpoint Discovery

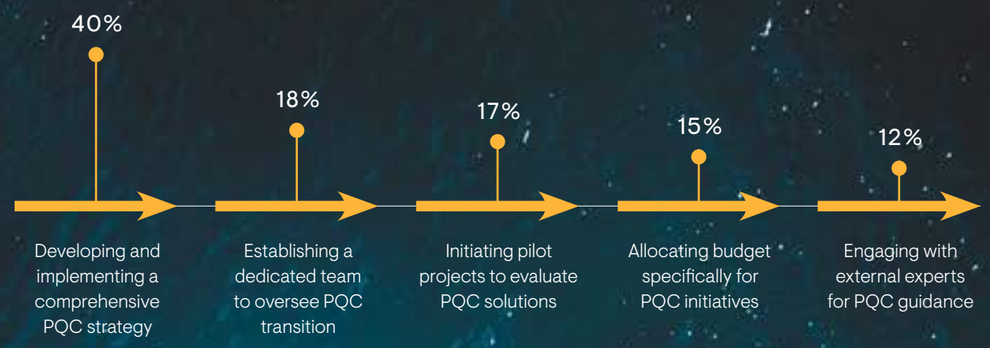
3%
Network Discovery

Mapping the Path to Quantum Security

A comprehensive PQC strategy is essential for success, and 40% of respondents say this is their agency's next step. Other agencies are making progress by establishing dedicated teams, launching pilot projects, and securing budgets for PQC initiatives. Agencies must also engage experts for PQC guidance to ensure that their strategies align with the latest standards and best practices.

With PQC standards in place, agencies are now focusing on compliance with evolving federal requirements, including the Risk Management Framework (NIST 800-53 Rev. 5) for system authorization and cryptographic control (SC-12). Agencies must implement the right PQC technologies to discover, assess, and manage cryptography across their environments. A key starting point is piloting PQC solutions and migrating initial systems to evaluate their effectiveness.

PRIMARY NEXT STEP TO ADDRESS RISKS ASSOCIATED WITH POST-QUANTUM CRYPTOGRAPHY



Next Steps

While some agencies have made significant progress, many are just beginning their journey toward a robust PQC strategy. For those in the early stages, the first step is gaining a clearer understanding of their environment's cryptographic landscape. Performing a cryptographic inventory across cloud and on-premises infrastructure, endpoints, and software applications—and integrating identified risks into existing strategies is critical. This can be done before finalizing a full PQC strategy, which will need to address legacy systems and operational technologies.

On a strategic level, agencies should broaden their awareness of quantum technologies to include quantum computing, quantum communications, and quantum sensing. These technologies represent a diverse range of capabilities that will shape the future of government operations. For quantum computing, agencies with relevant use cases should promote workforce familiarity with application software development for quantum environments. For PQC specifically, establishing a governance team within the agency's risk management portfolio will set the foundation for long-term success. Transitioning to PQC will take time, requiring education, sustained diligence, and active involvement from end-users and system owners as new standards evolve.

Developing a PQC-readiness roadmap ensures that agencies are equipped to reduce the impact of quantum risks effectively, focusing on the right strategy, technologies, and workforce to support cryptographic agility. This roadmap should take an iterative approach, starting immediately to address the most critical risks, while continuously adapting to address emerging challenges.

1

FORMALIZE YOUR PQC STRATEGY

Agencies must establish a formal PQC strategy that includes budget allocation and a dedicated project team to monitor progress. Prioritizing PQC-focused technologies will guide the overall assessment and migration process, helping manage the transition of potentially thousands of systems. A governance team is essential for overseeing this ongoing effort.

2

STRENGTHEN YOUR TECHNOLOGY FOUNDATION

Ensuring the right technologies are in place is critical for discovering, assessing, and managing cryptographic assets. Agencies should extend existing tools like vulnerability management and SIEM to support PQC requirements, alongside investing in solutions tailored for PQC discovery and management.

3

EMPOWER THE WORKFORCE WITH PQC EXPERTISE

Agencies must educate their workforce on the new PQC algorithms and how they impact risk management. While project teams may not directly implement PQC standards, they should be familiar with the potential changes and challenges these standards bring. Specialized engineers should lead the effort to address legacy migration concerns while ongoing training ensures the broader workforce is equipped for PQC-related challenges.

4

PRIORITIZE CRYPTOGRAPHIC DISCOVERY

Comprehensive discovery of all cryptographic assets, including devices, networks, and applications, is crucial to PQC readiness. Agencies should automate this process, validate findings with endpoint and network scanning, and prioritize high-risk systems. Given the continuous evolution of IT systems and cryptography, discovery must be an ongoing effort with dedicated tools.

5

ASSESS AND PRIORITIZE CRYPTOGRAPHIC RISKS

A comprehensive inventory of cryptographic assets is foundational to any PQC risk assessment. Involving stakeholders like cybersecurity managers ensures vulnerable assets, such as critical infrastructure and legacy systems, are prioritized. Advanced assessment tools can help map relationships and rank risks effectively, keeping focus on high-value assets.

6

MANAGE CRYPTOGRAPHY WITH THE RIGHT TOOLS

Agencies need cryptography management capabilities to maintain crypto-agility across their environments. This includes the ability to update cryptography dynamically as standards evolve, supported by secure technologies for scanning and monitoring. Key management systems (KMS) and hardware security modules (HSM) are essential to manage PQC algorithms and protect cryptographic keys.

About GDIT Digital Consulting

General Dynamics Information Technology (GDIT) stands at the nexus of digital consulting and mission-centric innovation in the public sector. GDIT's Digital Consulting Practice supports agencies, across more than 4,000 programs, navigating intricate landscapes and harnessing the transformative potential of AI, cybersecurity, cloud solutions, and emerging technologies. Through a network of GDIT's Emerge Labs, we advance technology research and development by enabling teams to interact, test, and demonstrate the latest technologies, collaborate with over 100 industry partners, and prototype advanced solutions. Partnering with visionary leaders across the public domain, we craft strategies that catalyze digital evolution, drive sustainable modernization, and position our clients at the forefront of excellence.

About GDIT

GDIT is a global technology and professional services company that delivers consulting, technology, and mission services to every major agency across the U.S. government, defense and intelligence community. Our 30,000 experts and consultants extract the power of technology to create immediate value and deliver solutions at the edge of innovation. We operate across 30 countries worldwide, offering leading capabilities in digital modernization, AI, machine learning, cloud, cyber, and application development. Together with our clients, we strive to create a safer, smarter world by harnessing the power of deep expertise and advanced technology. More information about GDIT is available at www.gdit.com.

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Thousands of government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity and service. More information about IBM is available at www.ibm.com.

Contact

GENERAL INQUIRIES

Christopher Aiello
Senior Marketing Manager
GDIT
Email: christopher.aiello@gdit.com

MEDIA INQUIRIES

Jay Srinivasan
Senior Public Relations Manager
GDIT
Email: jayendran.srinivasan@gdit.com