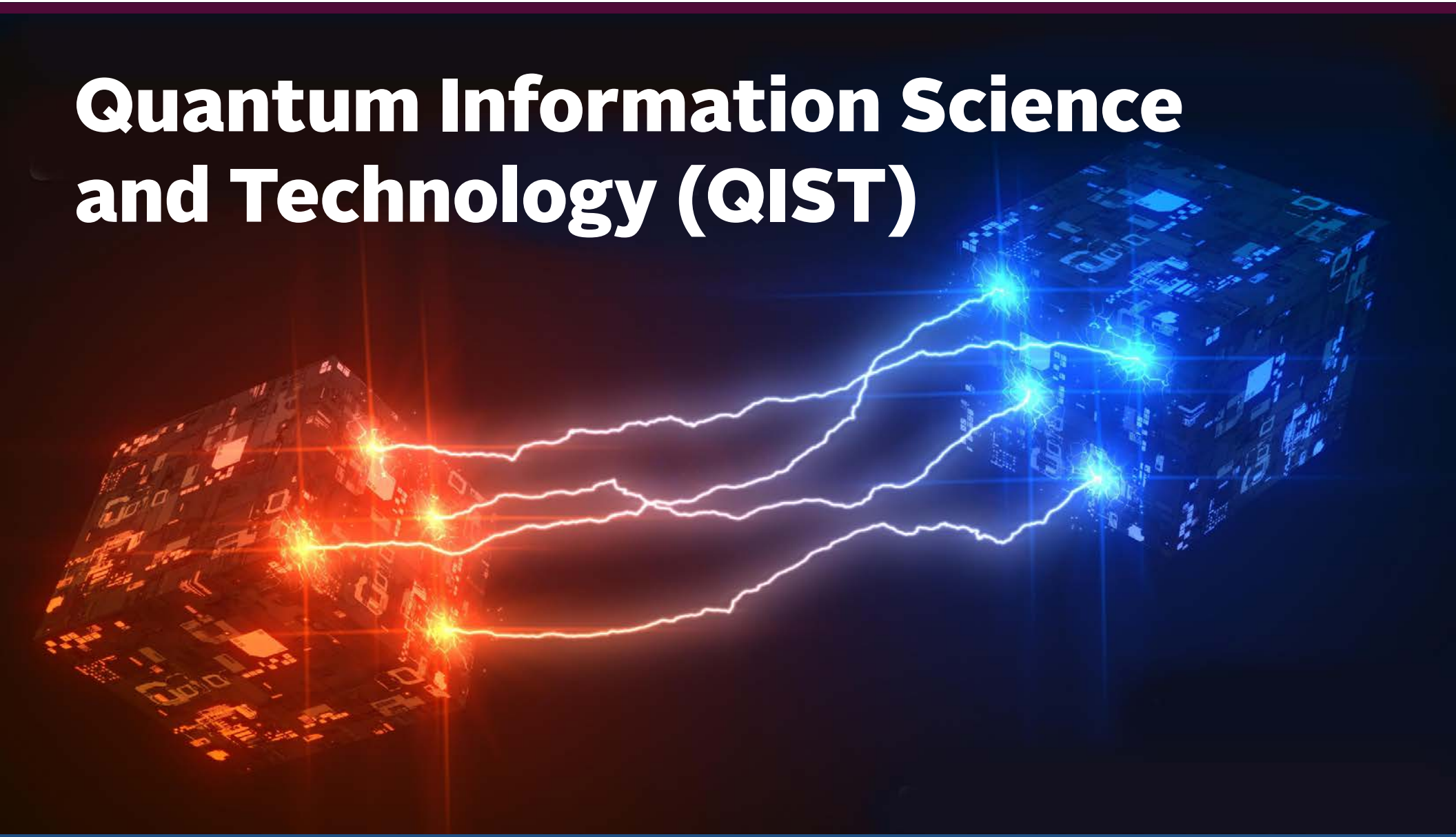
U.S. General Services Administration
Federal Acquisition Service (FAS)
Information Technology Category (ITC)

Quantum Information Science and Technology (QIST)



VERSION 1

AS OF MAY 23, 2024

Table of Contents

This document is intended to function as a single document or when needed as seven separate documents to meet the various needs of agencies and GSA.

Quantum Information Science and Technology (QIST) Introduction

This technology book aims to provide an overview for US federal agencies about QIST, with a particular emphasis on post-quantum cryptography (PQC). It contains a range of documents, including an executive summary, a white paper, use cases, and information on obtaining QIST products and services through GSA acquisition vehicles.

References to industry partners throughout this document are solely intended to emphasize the available QIST and PQC capabilities and do not constitute any endorsement of any industry partner.

1. EXECUTIVE SUMMARY

a. Considerations for Leadership

QIST is an umbrella for the theory, science, engineering, technology, infrastructure, and applications related to exploiting quantum effects in the areas of computing, communication, and measurement and sensing. Scientific experts recognize that building and scaling quantum-protected and enhanced communication networks are among the most essential technological frontiers of the 21st century. Quantum communications would allow for more secure communications, making information challenging to intercept. The international research community envisions an initial prototype global quantum network—the Quantum Internet—to be within reach over the next decade. However, a more immediate need exists to build and scale quantum-protected and enhanced communication networks.

The immediate QIST focus of the U.S. Federal Government is on PQC, which the Department of Energy (DOE) describes as extremely secure encryption—"a major attraction in an age where cybersecurity is constantly at risk"[1]. In advance of PQC standards being issued by the National Institute of Standards and Technology (NIST) in 2024, agency leadership has much to digest and consider. These standards will guide agencies in the transition of symmetric key algorithms and hash functions to protect against threats from quantum computers. Before the standards are issued, agencies must start inventorying vulnerable systems, identifying and assigning resources, calculating budget estimates, documenting current security protocols, and developing transition and implementation plans, to meet the guidance and directives in National Security Memorandum (NSM) - 10, which is required by Office of Management and Budget (OMB) Memorandum 23-02.

In 2022, NIST projected that it would take the government at least 5 to 15 years to complete a full implementation, and implementation of PQC standards is expected to be more problematic than introducing classical cryptographic algorithms. In the absence of significant implementation planning, it may be decades before federal agencies can replace the vulnerable public-key systems currently in use. At that point, it may be too late to protect critical systems and data.

Implementation considerations may include but are not limited to:

- **Increased Storage Requirements:** The information needed to decrypt the value, except the encryption key, is stored with the value, so the encrypted values use more storage space than the corresponding plain-text values.
- **Increased Network Latency:** Network latency, or simply "latency," represents the time delay (or lag) during data transmission over a network. Due to the increased sizes of the encrypted values, data packets will take longer to travel across the network, increasing network lag. Furthermore, encryption requires both the sender and the receiver to perform cryptographic operations, such as encryption, decryption, hashing, and verification. Thus, Encryption Latency will add processing delays, increasing network lag.

1 https://www.energy.gov/science/quantum-information-science

- **Compatibility Concerns:** Not all applications accommodate the implementation of certain forms of encryption, and there is always the risk that required encryption levels won't be compatible with existing networks and infrastructures.
- **Lack of Technical Expertise:** The government must hire or train qualified technicians to develop, implement, and maintain advanced PQC standards on government networks and infrastructure.
- **Increased Costs:** The additional storage requirements, network restructuring to accommodate compatibility, and hiring of qualified technicians will significantly impact the current budgets of government agencies.

  As such, Quantum Security as a Service (QSaaS) is emerging as an option to consider. QSaaS has the potential to offer multiple services to agencies to support PQC, such as Consulting and Planning, Implementation, Maintenance and Updates, Training and Education, and Quantum Computing Services (access to quantum processing power). For instance, QuSecure™ is a company that has developed an end-to-end PQC cybersecurity software solution. Based on their Small Business Innovation Research (SBIR) Phase III award from the Small Business Administration (SBA) in June 2022[2] they are the leading provider of PQC solutions to the federal government with contracts at more than a dozen agencies[3]. They are now teaming with public sector partners to bring solutions development and implementation to federal agencies to provide quantum resilience to encrypted communications and data on any device.

b. Strengths, Weaknesses, Opportunities, and Threats (SWOT)

SWOT analysis is a technique in strategic planning to help identify and focus on strengths, weaknesses, opportunities, and threats for an initiative or project. Below are the strengths, weaknesses, opportunities, and threats that have been identified for QIST:

TABLE 1: SWOT ANALYSIS

Strengths	Weaknesses	Opportunities	Threats
Improve agency networks and prevent attacks on secure data	Complex requirements are still being developed and understood	Upgrade current network security protocols to protect against attacks and breaches	Failure to implement may allow adversaries to gain access to sensitive data and communications
Prevent attacks on networks and data	Resource constraints for developing and implementing standards	Develop a reference guide of quantum-enabled applications that use encryption to help develop PQC implementation plans	Algorithms will need to be updated when technology changes
Improved Network Performance	Cost to develop and implement	Network modernization and cloud implementation for lower latency	Environmental interactions causing quantum decoherence, which introduces errors in calculations.
Meet the requirements of NSMNational Security Memorandum (NSM)-10	Industry partners are still developing solutions	Protect against Quantum enabled computers as attack vectors	

2 https://www.qusecure.com/qusecure-awarded-coveted-sbir-phase-iii-federal-government-procurement-contract-for-post-quantum-cybersecurity-solutions/
3 https://fedscoop.com/sbir-post-quantum-cryptography/

Strengths
PQC implementation will improve network security and better protect against brute-force attacks and data compromise. The implemented standards will protect against quantum-enabled computers and meet the requirements of NSM-10 for federal agencies as directed in OMB M-23-02.

Weaknesses
PQC is still under development and complex. Quantum skilled resources are in short supply throughout the United States, and developing those resources will take time. In addition to the human aspects, implementing PQC standards will take time and financial resources that agencies must contend with. Finally, public sector industry partners are still developing solutions and determining how best to implement complex solutions in all sectors, such as healthcare, finance, and government.

Opportunities
Implementation of PQC standards allows agencies to upgrade their current network security protocols and provide better protection against attacks and breaches. Additionally, agencies can continue the inventory of all systems and encryption protocols to prioritize systems and applications requiring upgrade to stronger encryption standards, prioritizing the most sensitive systems and protocols. Agencies that have yet to modernize and move to a cloud solution may use the increased cyber-attack threat as motivation to begin the process.

Threats
The greatest threat is that failure to implement PQC standards will result in a cyber-attack and data breach, allowing adversaries access to sensitive data and communications. There is also concern that due to the differences in system development, the algorithms could fail or need to be frequently updated as quantum computers advance.

2. OVERVIEW OF QIST

a. Description

QIST is the study and use of quantum mechanics to advance current technology, including more reliable navigation systems, more secure communications, and more powerful computing. It is a broad umbrella for the theory, science, engineering, technology, infrastructure, and applications related to exploiting quantum effects in the areas of computing, communication, and measurement and sensing. Quantum computers can potentially drive innovation in fields such as material science, pharmaceuticals, finance, and energy. America's ability to continue as a technological leader will depend on its ability to maintain a competitive advantage in quantum computers and QIST.

While quantum computers have the potential for benefits, there are also significant economic and national security risks. Quantum computers, also referred to as cryptanalytically relevant quantum computers (CRQC), are expected to be able to break much of the public-key security used in systems throughout the United States when they become available. These computers could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions

While the development of quantum computers continues, there is an immediate need to address the issue of PQC, which NIST defines as "cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks." Regardless of when quantum computing arrives, agencies must prepare information security systems to resist quantum computing[4]. Migrating computer systems to quantum-resistant cryptography will be a multi-year process. One focus of the standards will be on cryptographic agility to reduce the time required to transition and to allow for seamless updates for future cryptographic standards.

4 https://csrc.nist.gov/projects/post-quantum-cryptography - last accessed 3/27/2024

NIST has selected four algorithms[5] to withstand attack by quantum computers and has begun standardizing these algorithms to make them available so that organizations worldwide can integrate them into their encryption infrastructure. NIST released draft standards for three of the four algorithms in August 2023 and sought feedback on the drafts until November 22, 2023. While these are the first algorithms selected, they will not be the last, and NIST has already selected a second set of algorithms for evaluation. These additional algorithms are designed for general encryption and will offer an alternative defense if one of the selected algorithms shows weakness in the future.

b. Common Government Use

The National Quantum Initiative Act of 2018[6] established the National Quantum Initiative (NQI)[7] to develop a federal program to accelerate quantum research and development for the economic and national security of the United States. According to the NQI's annual report, the United States has invested in fundamental QIST research and development, with core efforts underway at over a dozen federal agencies. One focus of the NQI program is Quantum Technology, which includes efforts to understand and mitigate risks associated with quantum technologies with PQC.

The PQC program at NIST is crucial to securing public critical infrastructure once quantum computers are available. The expected timeline for publishing the final Federal Information Processing Standards (FIPS) PQC standards is 2024. They will specify the key establishment and digital signature schemes to protect against future attacks. Transitioning federal IT systems to these new standards will take time, resources, and commitment. National Security Memorandum (NSM)-10 outlines the plan to update infrastructure and implement these new standards.

OMB Memorandum 23-02, issued November 18, 2022, directs federal agencies to implement the requirements of NSM-10, which requires federal agencies to develop plans to safeguard intellectual property, research and development, and other sensitive information from adversaries. It includes specific actions for agencies as the multi-year process of migrating to PQC begins. Cryptographically relevant quantum computers (CRQC) will be capable of breaking much of the public-key cryptography used on digital systems and jeopardizing civilian and military communications, undermining supervisory and control systems, and defeating security protocols for most internet-based financial transactions.

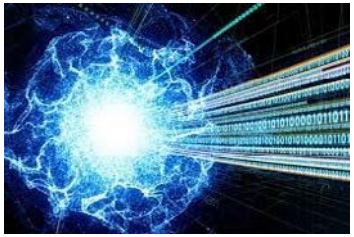
5 https://csrc.nist.gov/projects/post-quantum-cryptography - last accessed 3/27/2024
6 https://www.congress.gov/bill/115th-congress/house-bill/6227
7 https://www.quantum.gov

1. EXECUTIVE BRIEF

a. Emerging Radar Quadrant: Security & Cybersecurity - Includes areas such as digital safeguards and threat/vulnerability management.

b. Title: Quantum Information Science and Technology (QIST)

c. Problem: The expectation is quantum computers and other technologies will break much of the public-key security used in systems throughout the United States in the next few years. This technology will jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions.



d. Applications & Examples: The most important application for federal agencies will be implementing post-quantum cryptography (PQC) encryption to prevent cyberattacks, future-proof networks, and prepare for post-quantum threats. GSA conducted PQC market research through a request for information (RFI). The RFI was made available publicly through SAM.gov and directly to our current industry partners using GSA's market research as a service (MRAS). A few examples from the 52 respondents include:

i. QuSecure, QuantumXchange, and Sandbox AQ launched Quantum Security as a Service.

ii. Fortinet and Check Point Software are marketing Quantum SD-WAN.

iii. QuSecure's quantum-resilient SaaS is the first PQC solution available on GSA's Multiple Award Schedule (MAS) as of September 2023, and GSA is actively seeking additional PQC vendors.

iv. Air Force, Space Force, and NORAD are utilizing QuSecure's PQC algorithms on legacy systems and reporting 100-percent uptime in protecting data that previously used standard encryption, with no increased bandwidth or latency issues.

v. General Dynamics Information Technology (GDIT) is developing a framework for working with agencies to build a quantum-resistant implementation strategy that includes assessing and analyzing the environment and prioritizing and implementing approved quantum-resistant solutions.

e. Value and Use

TABLE 2: POST-QUANTUM VALUE AND USE

Post-Quantum Cryptography Value and Use
Protect critical infrastructure that transmits data by replacing public-key cryptography with PQC cryptographic algorithms.
Protect and secure civilian and military communications from outside threats.
Implement long-term solutions to avoid expensive, time-consuming migration projects in the future.
Update key security protocols with fast, efficient solutions and provide real-time threat analysis.

f. Lifecycle Stage –

QIST is an emerging technology primarily in the research, development, and testing phase. With the federal directive to prepare now for securing information in a post-quantum era, industry partners are developing use cases to bring to the federal marketplace to support the implementation of PQC.

Early solutions are being tested by federal agencies in conjunction with the Phase III SBIR award to QuSecure for their software QuProtect[8]. To ensure critical networks do not shut down, the White House encourages agencies to begin testing cryptography in production environments after the transition in the Office of Management and Budget (OMB) Memorandum on Migrating to Post-Quantum Cryptography (M-23-02). Analysis and feedback of the agency's initial budgets are under review by the Office of the National Cyber Director (ONCD). So, how far along agencies are in engaging support for the PQC transition has yet to be determined.

FIGURE 1: POST-QUANTUM CRYPTOGRAPHY TIMELINE[9][10]

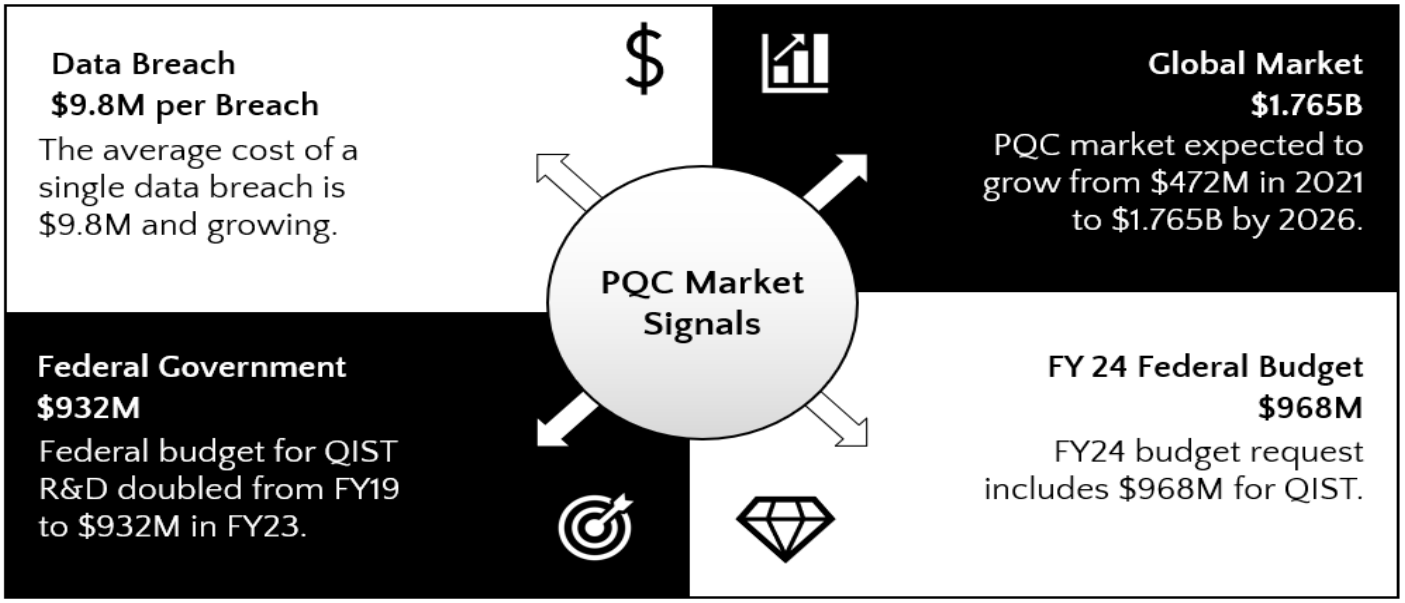
8 https://www.qusecure.com/qusecure-awarded-coveted-sbir-phase-iii-federal-government-procurement-contract-for-post-quantum-cybersecurity-solutions/
9 https://www.dhs.gov/publication/preparing-post-quantum-cryptography-infographic,
10 https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

g. Market Signals

All existing encrypted data is vulnerable to brute-force attacks in which all possible combinations of encryption keys are tried, a time-consuming process. Quantum computers will easily break cryptographic keys by calculating and exhaustively searching secret keys to compromise existing cryptographic algorithms breaking public-key cryptography in hours rather than years.11

The following table highlights the costs associated with a single data breach and the estimated spending expected in the coming years on QIST and PQC. The Federal budget for research and development has more than doubled since 2019 and the current fiscal year (FY) 24 budget includes a request for almost a billion dollars for QIST-related projects and research12. The global market is expected to grow from $472M in 2021 to $1.765B by 202613.

FIGURE 2: POST-QUANTUM MARKET SIGNALS



2. GSA IS HERE TO HELP

a. If you would like more information on the topics covered in this paper, please contact your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of QIST.

11 https://pswordpress-production.s3.amazonaws.com/2022/04/Quantum-Computing-and-Cybersecurity_-Preparing-for-Post-Quantum-Cryptography-PreScouter.pdf
12 https://www.quantum.gov/the-national-quantum-initiative-supplement-to-the-presidents-fy-2024-budget-released/
13 https://pswordpress-production.s3.amazonaws.com/2022/04/Quantum-Computing-and-Cybersecurity_-Preparing-for-Post-Quantum-Cryptography-PreScouter.pdf

QIST Slip Sheet
Quantum Information Science and Technology

Quantum Information Science and Technology (QIST) is the study and use of quantum mechanics to advance current technology, including more reliable navigation systems, secure communications, and powerful computing. It is a broad umbrella for the theory, science, engineering, technology, infrastructure, and applications related to exploiting quantum effects in the areas of computing, communication, and measurement and sensing. Quantum computers can potentially drive innovation in fields such as material science, pharmaceuticals, finance, and energy. America's ability to continue as a technological leader will depend on its ability to maintain a competitive advantage in quantum computers and QIST.

VALUE

QIST has the ability to ensure the security of critical infrastructure that transmits data by implementing and maintaining post-quantum cryptography (PQC) algorithms. By replacing vulnerable public-key cryptography, QIST can achieve secure critical infrastructure and interoperate with existing networks. Using PQC, QIST provides protection and security for civilian and military communications and data, safeguarding them against external threats. QIST also offers improved supply-chain optimization, research, and production, making it essential to implement our evolving networks successfully.

VALUE STATEMENT

Scientific experts recognize that building and scaling quantum-protected and enhanced communication networks are among the most important technological frontiers of the 21st century. Quantum communications would allow for more secure communications by making information challenging to intercept. The international research community envisions a first prototype global quantum network—the Quantum Internet—to be within reach over the next decade, and an immediate need exists to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

WHAT IS DRIVING QIST?

"Quantum information science (QIS) is a unification of quantum mechanics and information theory, two foundational fields underpinning modern technology. Together, these fields are producing transformative new types of computers, sensors, and networks, with the potential to advance the Nation's prosperity and strengthen its security."[14] An example of a need to strengthen security is that attackers use the technique of "harvesting now and decrypting later" by attacking systems to acquire sensitive data that has a long expiration date such as personally identifiable information, confidential data, and financial records. Attackers can hold onto the information until a quantum computer with enough power becomes available to break its encryption. When this occurs before the data's expiration, it could lead to significant data breaches in the future. The development of quantum computers with the capabilities to break public-key encryption protocols make it vital that agencies begin preparing for migration to PQC algorithms now before adversaries and threat actors steal sensitive data that they can decrypt later on.

14 https://www.quantum.gov/wp-content/uploads/2023/12/NQI-Annual-Report-FY2024.pdf

WHAT DOES QIST MEAN FOR AGENCIES?

The immediate focus of QIST for most agencies is on PQC, which is the development and implementation of cryptographic security for classical computers that can prevent attacks launched by quantum computers. Regardless of when quantum computers are fully developed, agencies must prepare information security systems to resist quantum computing. Migrating computer systems to quantum-resistant cryptography will be a multi-year process, including a focus on cryptographic agility to reduce the time required to transition and to allow for seamless updates for future cryptographic standards.

HOW CAN GSA HELP?

QIST and PQC are issues that the industry will have to deal with for their systems as they work simultaneously to develop solutions for their customers. Using approved NIST algorithms, PQC solutions are being developed and tested. Once finalized, NIST will incorporate these algorithms into the NIST-required standards. Agencies will work with industry-developed solutions to fully identify vulnerable systems and design and implement plans to transition to PQC. The National Quantum Initiative Supplement to President's FY 2024 Budget outlines the following essential components that need to be considered: Quantum Sensing and Metrology (QSENS), Quantum Computing (QCOMP), Quantum Networking (QNET), QIS for Advancing Fundamental Science (QADV), and Quantum Technology (QT).

WHAT IS NEXT FOR QIST?

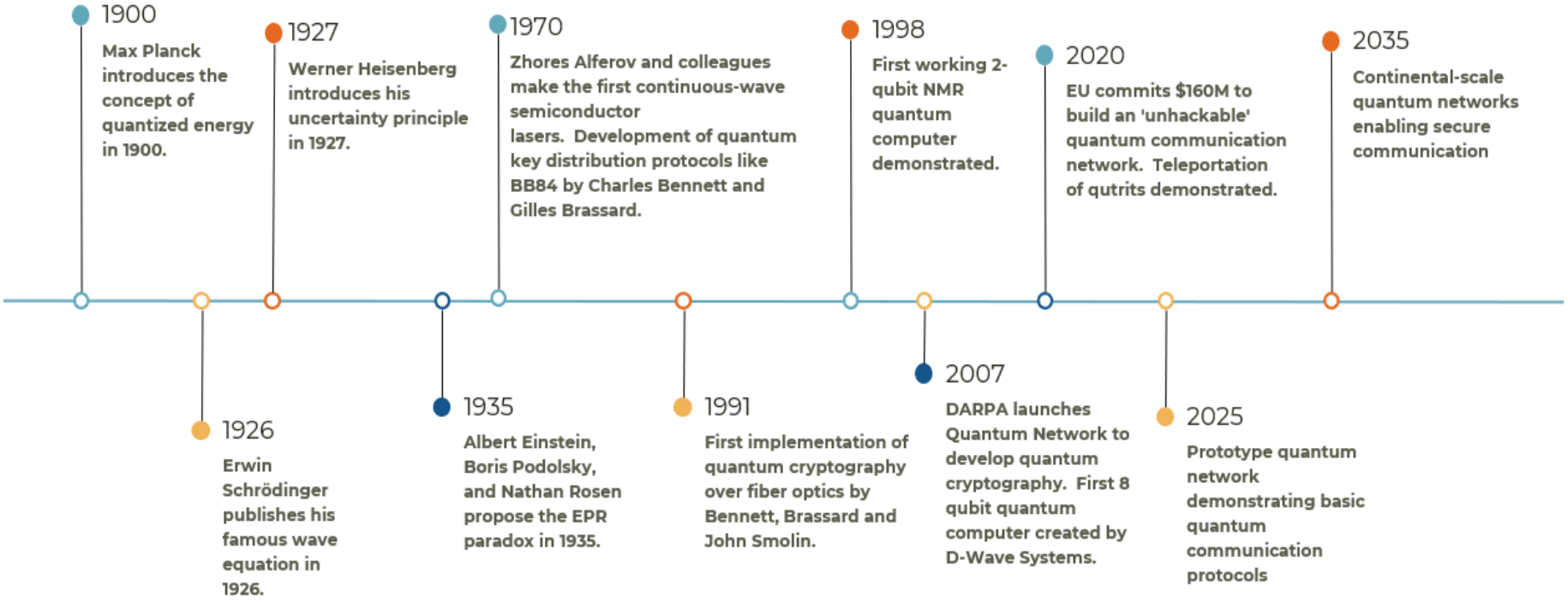
GSA offers agencies support in designing and implementing PQC as part of QIST solutions using its Best-in-Class (BIC) contracts through commercial providers. Agencies can use GSA's acquisition vehicles to design, implement, and support solutions for PQC.

NIST is working to finalize PQC standards for the algorithms selected to withstand attack from quantum computers to make them available so that agencies and other organizations can integrate them into their encryption infrastructure. In addition, NIST is continuing to evaluate a second set of algorithms designed for general encryption that will offer an alternative defense if one of the previously selected algorithms shows weakness in the future.

QIST White Paper

QIST is an umbrella for the theory, science, engineering, technology, infrastructure, and applications related to exploiting quantum effects in the areas of computing, communication, and measurement and sensing. Scientific experts recognize that building and scaling quantum-protected and enhanced communication networks are among the most essential technological frontiers of the 21st century.

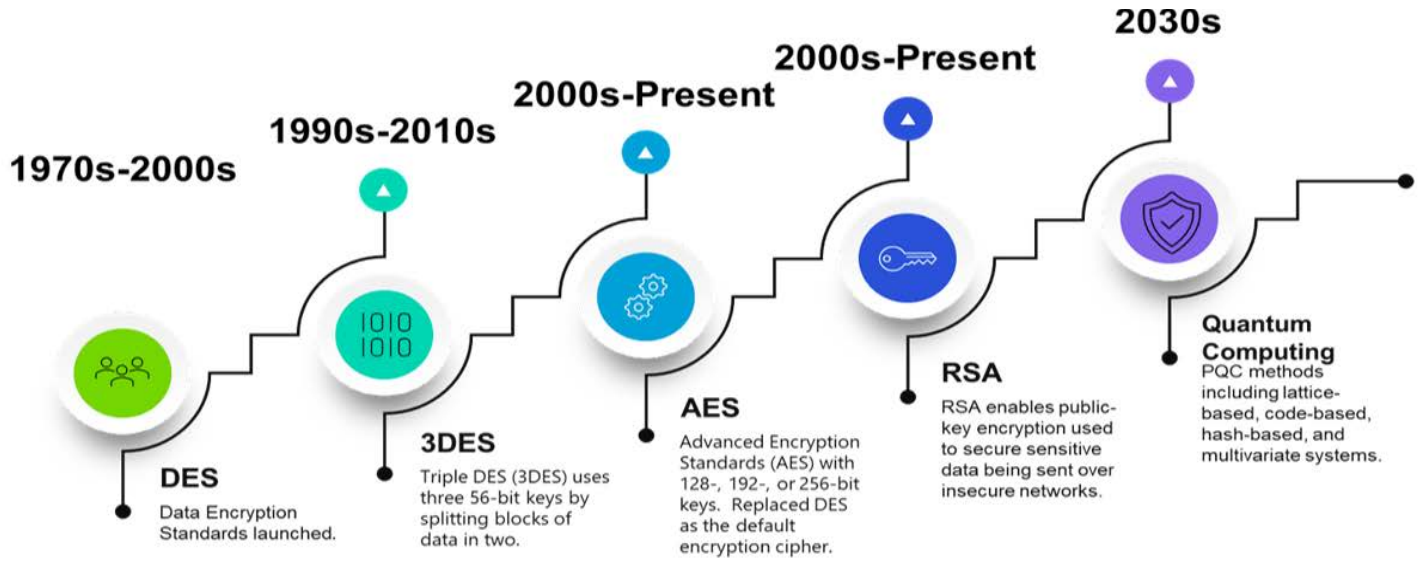
FIGURE 1: QUANTUM INFORMATION SCIENCE AND TECHNOLOGY TIMELINE



Quantum communications would allow for more secure communications, making information challenging to intercept. The international research community envisions an initial prototype global quantum network—the Quantum Internet—to be within reach over the next decade. However, a more immediate need exists to build and scale quantum-protected and enhanced communication networks.

The imminent Post-Quantum Cryptography (PQC) standards will allow information security systems to resist attacks that leverage quantum computing. Once quantum computing becomes available, public-key algorithms will be vulnerable to criminals, competitors, and other adversaries. Agencies must begin planning to replace all systems that use public-key algorithms to protect data and information.

FIGURE 2: ENCRYPTION TIMELINE[15]



NIST has selected four algorithms16 to withstand attack by quantum computers and has begun standardizing these algorithms to make them available so that organizations worldwide can integrate them into their encryption infrastructure. NIST released draft standards for three of the four algorithms in August 2023 and sought feedback on the drafts until November 22, 2023. While these are the first algorithms selected, they will not be the last, as NIST has selected a second set of algorithms for evaluation. These additional algorithms are designed for general encryption and will offer an alternative defense if one of the previously selected algorithms shows weakness in the future.
U.S. governmental agencies should be preparing their information security systems for migration to post-quantum cryptography (PQC).

In the National Cybersecurity Implementation Plan issued in July 202317, Strategic Objective 4.3: Prepare for our Post-Quantum Future prioritizes implementation of National Security Memorandum-10 (as required by OMB-M-23-02) and transitioning vulnerable public networks and systems to quantum-resistant cryptography-based environments, focusing first on federal information systems and National Security Systems (NSS).

15 https://www.darkreading.com/cyberattacks-data-breaches/post-quantum-cryptography-set-to-replace-rsa-aes-ecc
16 https://www.qusecure.com/qusecure-awarded-coveted-sbir-phase-iii-federal-government-procurement-contract-for-post-quantum-cybersecurity-solutions/
17 https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf

1. FEDERAL GUIDANCE AND EFFORTS SUPPORTING QUANTUM INFORMATION SCIENCE AND TECHNOLOGY

QIST has been a topic for many agencies and industry experts over the past several years; however, there has been a significant increase in activity over the past two years. The following documents provide recent examples of federal guidance and recommendations on the topic.

a. National Quantum Initiative Act of 2018

b. Executive Order 13885 of August 30, 2019, Establishing the National Quantum Initiative Advisory Committee

c. Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity

d. National Security Memorandum 8 of January 19, 2022, Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

e. National Security Memorandum 10 of May 4, 2022, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

f. Executive Order on Enhancing the National Quantum Initiative (NQI) Advisory Committee of May 4, 2022

g. Fact Sheet: President Biden Announces Two Presidential Directives Advancing Quantum Technologies of May 4, 2022

h. OMB Memorandum Migrating to Post-Quantum Cryptography on November 18, 2022

i. Quantum Computing Cybersecurity Preparedness Act of December 21, 2022

j. National Quantum Initiative Supplement to the President's FY 2023 Budget December 1, 2023

k. National Cybersecurity Strategy Implementation Plan of July 2023

l. Migration to Post Quantum Cryptography website National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE)

m. DRAFT NIST Special Publication 1800-38A, B, and C Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography

n. NIST Updates on efforts to support agencies in the transition to Post-Quantum Cryptography can be found at the NIST Cybersecurity Center of Excellence (CCOE)

o. Quantum-Readiness: Migration to Post-Quantum Cryptography

2. THE TECHNOLOGY MATURITY LIFECYCLE PHASE

a. **The lifecycle phases include emerging, research and development, early solutions, initial adoption, private sector experiments, government experiments, broad acceptance, decline, end of sale, and end of life. We also note the possibility of additional application paths. The definition of each lifecycle phase for the purposes of this paper is below:**

1. **Emerging Phase** - New technology is developed and early use cases are being identified. As the technology is introduced in the commercial market, its need builds in government organizations.
2. **Research and Development Phase** - Technology may still only exist in the lab environment.
3. **Early Solutions Phase** - Technology has moved out of the lab, initial applications (use cases) have been identified and are being tested
4. **Initial Adoption Phase** - Agencies start adopting the technology. Initial shortcomings are eliminated in this phase which will increase agency trust.
5. **Private Sector Experiments Phase** - Technology that for-profit companies are bringing into their systems but are not yet widespread
6. **Government Experiments Phase** - Technology that federal, state, local, and tribal governments are trying out as part of services delivery and operations
7. **Broad Acceptance Phase** - Technology is accepted across the federal government, and competitive and alternative technologies are developed. Additionally, this is the phase where technologies have had successful government experiments and are ready for widespread government acquisition
8. **Decline Phase** - The introduction of more advanced alternative technologies makes the current technology obsolete and takes the alternative technology to a phase where further investment and development can take place.
9. **End of Sale Phase** - Vendors no longer sell or install the service.
10. **End of Life Phase** - Product is no longer supported through normal processes
11. **Additional Application paths** – May be the turning point in the declining phase. This could involve working on increscent improvements such as a technology software update, upgraded specifications, or a redesign.

b. **GSA places the majority of QIST technologies in the Emerging Phase, because while research and development continue, solutions are beginning to move out of the lab into testing of initial applications and development of use cases. The next phase in the lifecycle, Initial Adoption, will come as agencies begin adopting the technology. QIST is in the process of testing cryptographic algorithms in the emerging technology phase, but with the issuance of NIST standards in 2024, it is anticipated that accepted solutions based on the NIST standards will become widely available for agency implementation. The full transition to cryptographic algorithm security solutions is expected to take years to complete and the lifecycle phase of Broad Acceptance, which follows Initial Adoption, will take several years to reach in federal agencies.**

3. TECHNICAL SPECIFICATIONS

PQC is an emerging technology with evolving applications and solutions. The specifications presented here are based on current information and guidance and may have been updated since initial publication.

PQC will involve the transition of active public-key encryption for systems that provide one or more of the following services: (1) creation and exchange of encryption keys, (2) encrypted connections, or (3) creation and validation of digital signatures. PQC will replace vulnerable public-key cryptography (PKC) algorithms in use today. The traditional algorithms primarily used for key establishment and digital signatures include advanced encryption standards (AES) and Rivest-Shamir-Adleman (RSA). Several algorithmic approaches to post-quantum cryptography, including lattice-based cryptography, hash-based cryptography, and elliptic curve cryptography, are explained in more detail below.

a. Lattice-Based Cryptography

Lattice-based is built on mathematical problems around lattices that resemble a graph paper grid - using a set of points located at the crossings of a lattice of straight lines. This grid is not finite and describes a pattern that continues into the infinite. Lattice-based cryptography is considered one of the most secure PQC encryption methods because while current algorithms, such as RSA (Rivest-Shamir-Adleman), rely on factoring large prime numbers, lattice algorithms rely on the difficulty of finding the right lattice point in a high dimensional vector space.[18]

FIGURE 3: HASHING FUNCTION

Lattice-based schemes are part of the NIST process for providing the fundamental primitives of encryption, key encapsulation, and digital signature schemes (DSSs). Lattice-based algorithms include the NIST-selected CRYSTALS-KYBER (a public key encryption and key-establishment algorithm) and CRYSTALS-Dilithium (a digital signature algorithm).

Lattice-based cryptography offers the following benefits[19]:

- **Improved Security** - offers improved security because lattices are more difficult to break than other mathematical structures commonly used for cryptography, such as elliptic curves.
- **Faster Computation Times** - can be computed much faster than other cryptographic algorithms, improving performance, especially in applications requiring real-time responses, such as streaming media or online gaming.
- **Lower Energy Consumption -** consume less energy than other types of cryptographic algorithms because they can be implemented in hardware that requires less power.
- **Flexible and Easy to Implement** - relatively easy to implement as opposed to other methods, such as elliptic curve cryptography which can be complex and require a large amount of computer resources.

b. Hash-based Cryptography

Hash functions are the basic tools of modern cryptography used in information security to authenticate transactions, messages, and digital signatures. Hashing is the one-way act of converting the data (called a message) into the output (called the hash) using a mathematical function with a fixed number of characters. It ensures data has not been tampered with, as even a small change in the message will create an entirely different hash value. It is very difficult to "reverse" a hash back to its original message, requiring extreme amounts of computing power.[20]

Hash-based cryptography has the following uses:

- **Verify and securely store passwords** – websites use hash passwords to store and verify passwords as hash values.
- **Verifying digital signatures** – hash values in digital signatures can be re-generated to verify that it matches the one sent. The simplest changes, such as a change in capitalization in a document, will result in a different hash value.

18 https://www.sonatype.com/launchpad/what-is-post-quantum-cryptography
19 https://www.makeuseof.com/what-is-lattice-based-cryptography/#:~:text=Lattice%2Dbased%20cryptography%20is%20a,structure%20encodes%20and%20decodes%20messages.
20 https://corporatefinanceinstitute.com/resources/cryptocurrency/hash-function/

- **Secure Blockchains** – a hash function is applied to a data block to provide a hashed value. Blockchains use random or semi-random numbers (nonces), and each transaction requires an additional data block to be hashed.
- **Discover Duplications** – hash functions can be used to examine similar data and locate modified files in data/file storage.

Hash-based cryptography offers the following benefits:

- **Ensure data integrity** – identify if data has been tampered with after creation.
- **Ensure data transmission integrity** - increases the trustworthiness of the data by ensuring the data sent is identical to the data received.
- **Verify authenticity** – ensure data has not been modified after being digitally signed.
- **Resists reverse computing** – it is very difficult to reverse compute an input message if you only know the hash value. Reverse computing using a manual method for searching requires a lot of trial and error and uses a greater amount of computing power to find the message with the hash value assigned.

c. Elliptic Curve Cryptography (ECC)

ECC is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. It is most often used for digital signatures in cryptocurrencies and one-way encryption of emails, data, and software. Public key cryptography, like ECC, uses a mathematical process to merge two distinct keys and use the output to encrypt and decrypt data. One is a public key known to anyone, and the other is a private key known only by the sender and receiver of the data.

ECC keys are generated through the elliptic curve equation instead of traditional methods like the RSA algorithm using large prime numbers. The U.S. government requires the use of ECC with a key size of 256 or 384 bits for internal communications, depending on the sensitivity of the data.[21]

ECC has the following uses:

- **Online banking and payments** - ECC can encrypt personal information before being sent via the internet ensuring data is confidential and secure.
- **Encrypt email** - ECC can encrypt email to protect it from being read by anyone other than the intended recipient(s).
- **Encrypt digital signatures** - ECC can encrypt digital signatures. It is one of the primary uses in the federal government.
- ECC has the following benefits:
- **Speed and Efficiency** – the primary benefits of ECC when encrypting and decrypting data.
- **Conserves Memory Resources** – ECC requires less processing power than other data encryption options like RSA.
- **Encryption Strength** – ECC is stronger than RSA key sizes in use today. The typical ECC key size of 256 bits is equivalent in security to a 3072-bit RSA key.

21 https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography

d. Other Encryption Options include Multivariate Cryptography and Code-Based Cryptography, both of which are easy to implement but considered the least secure options an organization can implement.[22]

4. SECURITY CONSIDERATIONS

Quantum-resistant protection through PQC algorithms seamlessly integrated into existing IT infrastructure is the focus of QIST and PCQ. OMB Memorandum M-23-02 directs agencies to respond to the requirements of NSM-10 for the transition of National Security Systems (NSS) and vulnerable public networks and systems to quantum-resistant cryptography-based environments. NSM-10 inventory requirements include current cryptographic methods used on IT systems, including system administrator protocols, non-security software and firmware that require upgraded digital signatures, and information on other key assets.

In addition, agencies have been directed to develop new standards, tools, and best practices for complying with the PQC standards and procedures criteria for cybersecurity described in the NSM-10. These guidelines must include criteria that can be used to evaluate software security, criteria to evaluate the security practices of the developers and suppliers and identify tools or methods to demonstrate conformance with secure encryption practices.

Assuming agencies have completed the inventory and guideline requirements, next is the challenge of assessing current encryption, planning for a transition to PQC encryption standards, estimating financial and human resource requirements, developing acquisition requirements and making contract awards, and implementing new PQC encryption standards. As it is anticipated that this initial set of PQC standards will not be the last, agencies also need to plan now to ensure future encryption standards are integrated into their IT infrastructure and to ensure maintenance and upgrades are completed in a timely manner.

5. RECOMMENDED ACTIONS FOR AGENCIES

Agency Chief Information Office (CIO) departments should now be planning for implementation of PQC standards and to meet the requirements of NSM-10/OMB M-23-02. Vendors with quantum expertise are available to work with agencies to accomplish the steps required to prepare, including:

- Learn about and understand the new cryptography.
- Complete cryptographic system inventory as required by OMB M-23-02 and outlined in NSM-10.
- Assess the current system environment, including identifying system architecture and security requirements.
- Develop standards, tools, and best practices for complying with PQC encryption standards.
- Develop a comprehensive plan for the implementation of PQC security measures.
    - Prioritize systems for implementation based on the sensitivity of data stored and identify the security of other systems that interact with the agency.
- Implement PQC cryptographic algorithms based on system prioritization.
- Manage and maintain updated systems to keep up with cryptographic security requirements, as required.

22 https://www.sonatype.com/launchpad/what-is-post-quantum-cryptography

Agencies should begin assessing and understanding what they need to do to protect their data and complete contract actions, as required. QuSecure's COO Skip Skanzeri offers several recommendations in addition to those above[23]:

- **Test new NIST algorithms** - there is insignificant risk in testing algorithms, and agencies can gain valuable hands-on experience through testing prior to permanent upgrades.
- **Be Crypto-Agile** - it is expected some algorithms will fail, some will need adjustment, and some will work. By being crypto-agile, agencies can switch to new cryptography and not have to commit to only one algorithm.
- **Avoid Rip and Replace -** find partners that can install quantum-resilient algorithms over existing cryptography to avoid 'rip and replace'.
- **Protect the entire network** - as outdated, vulnerable cryptography provides an attack point, consider all components. Examples include servers, switches, phones, laptops, cloud-based servers, and satellites.
- **Avoid installing edge devices -** Find partners that can deploy quantum-resilient algorithms without installing on edge devices, making securing the network easier and quicker.
- **Consider a hybrid approach** - consider leaving existing encryption in place while transitioning to quantum-resilient algorithms to ensure network safety.

CONCLUSION

Although quantum computers are in their infancy, adversaries plan to use the technology as it develops to crack encrypted data they have already taken from US systems. More must be done now to protect the communications and data of the federal government as this technology evolves.

Software-based solutions are emerging with the technology to work with NIST-approved algorithms. These solutions are being developed to provide end-to-end support that combines zero-trust, post-quantum-cryptography, crypto agility, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive cybersecurity suite. Agencies still have a lot of work to do in finalizing system inventories, developing PQC transition plans, and implementing those plans. Developing a path forward to meet the requirements of OMB M-23-02 and NSM-10 now is critical for agencies to ensure they are prepared to implement PQC encryption standards moving forward.

23 https://www.forbes.com/sites/forbestechcouncil/2023/11/14/cybersecurity-threats-just-got-worse/?sh=700e92d3ceeb

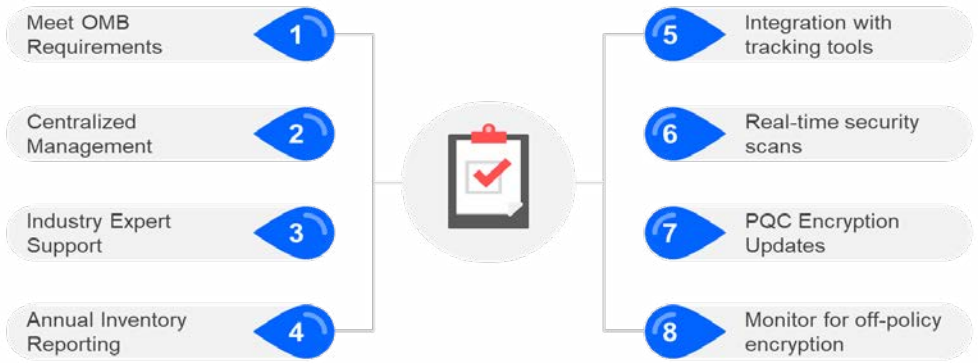
QIST Use Cases: Quantum Security-as-a-Service (QSaaS)

1. HIGHLIGHTS

a. Challenge - for agencies to upgrade their network and application encryption standards to protect against attacks using quantum computers, meet the requirements of OMB M-23-02 and NSM-10, and provide maintenance and updates as encryption standards change. The initial transition to post-quantum cryptography will require significant financial and human resources for federal agencies.

b. Possible Solution: Quantum Security as a Service offerings from commercial partners. This type of solution is currently in development, with initial solutions becoming available to federal agencies.

FIGURE 1: QUANTUM SECURITY-AS-A-SERVICE BENEFITS



c. Operational Benefits

i. Simplified operations with centralized cloud-based management and security.

ii. Annual reporting and ongoing maintenance of a centralized cryptographic inventory.

iii. Integration with issue tracking tools such as JIRA, GitHub, etc.

d. Security Benefits

i. Real-time identification of system vulnerabilities and cryptographic algorithms that do not adhere to OMB requirements.

ii. Easily adhere to new cryptographic requirements without additional development.

iii. Monitor and remediate off-policy algorithms.

2. CHALLENGE SCENARIO

a. Agencies have been tasked with preparing to implement post-quantum cryptography (PQC) encryption standards to secure federal data and information systems. The challenge is how to do this with current resource levels, expertise, and limited budgets.

3. CRITERIA FOR SUCCESS

a. Identify and inventory all systems and applications required to upgrade to PQC standards.

b. **Transition IT infrastructure to agile cryptography that adheres to all federal security requirements.**

c. **Centralize maintenance and updates based on new standards and simplified processes for the addition of new systems and applications.**

4. FINANCIAL CONSIDERATIONS

a. **Agency leadership will need to consider the cost of all aspects of implementing PQC and protection systems against threats from attackers using quantum computers. Leaders will need to assess if they have internal resources or current contracts with the skills to oversee and manage an implementation of this magnitude and identify the cost of contractor support to bridge gaps and ensure a successful implementation. Because a QSaaS solution would cover the full migration lifecycle (see Figure 2 QSaaS Support of Agency PQC Requirements) it could support these initial implementation requirements and ultimately reduce the long-term cost of maintaining and upgrading encryption standards as technology advances. In addition, the use of QSaaS will support agencies in meeting the annual reporting requirements outlined in NSM-10 and required by OMB M-23-02.**

5. OPERATIONAL CONSIDERATIONS

a. **A QSaaS solution can simplify implementing and maintaining PQC standards for the long term. Once implementation is complete, agencies can manage and maintain through a centralized, cloud-based console. Resources don't have to be on-site; the solution can easily integrate with tracking tools such as JIRA, GitHub, etc. QSaaS also simplifies annual reporting requirements and ensures compliance with NSM-10 as required by OMB M-23-02.**

6. SECURITY CONSIDERATIONS

a. **PQC standards are complex and still evolving. Once settled, you may require subject matter expertise to implement. Working with a qualified QSaaS vendor with trained quantum experts will alleviate the burden of hiring and training new resources in a timely manner to meet new PQC standard requirements. The QSaaS solution will ensure that once the initial inventory, assessment, and implementation are complete, ongoing maintenance includes implementing all future algorithm updates and meeting all future federal security requirements. QSaaS could be implemented as part of a larger Managed Network Service (MNS) as it would complement the services provided as part of managed security.**

7. WHERE TO BUY

a. **Enterprise Infrastructure Solutions (EIS)**

i. EIS is a multiple award, indefinite delivery, indefinite quantity (IDIQ), Best-in-Class Contract (BIC)

ii. Using EIS agencies can use GSA's acquisition tools to implement a QSaaS solution for quantum-safe security:

- Managed Security Services (MSS) on GSA BIC contracts can be leveraged to create QSaaS solutions to meet agency needs.
- Quick-start solicitation templates to modernize agency networks through the use of Managed Network Services (MNS) and MSS solutions.

- Solicitation Assist Tool to assist agencies in writing solicitation documents.

b. Governmentwide Acquisition Contracts (GWACs)

i. GSA's Alliant 2, VETS 2 and 8(a) STARS III GWACs are multiple-award, indefinite-delivery indefinite-quantity (IDIQ) contracts for information technology service solutions, including emerging technology.

ii. All GSA GWACs are designated as tier three Best-in-Class solutions.

iii. Agencies can utilize the GSA GWACs to develop turnkey solutions for quantum security as a service (QSaaS). These may include, but are not limited to: secure communications, cryptography/encryption, and quantum machine learning.

iv. Additional information regarding how to utilize the GSA GWACs can be found at www.gsa.gov/gwacs.

8. GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your Quantum Security as a Service implementation. Thank you for reading!

Information for this use case came from the following sites with QSaaS solutions:

https://www.sandboxaq.com/solutions/security-suite

https://quantumxc.com/phio-tx/

https://www.qusecure.com/quprotect/

QIST Use Case: Quantum SD-WAN

1. HIGHLIGHTS

a. **Challenge:** to provide quantum-safe security capabilities to Software-Defined Wide Area Networking (SD-WAN), making data transmitted between sites more secure against cryptographic threats, including quantum attacks.

b. **Proposed solution:** develop crypto-agile and crypto-diverse key delivery systems that support encryption keys generated and protected by any quantum method. An SD-WAN implementation can significantly lower agency costs with centralized network control and configuration which can reduce complexity. A Quantum SD-WAN provides the added benefits of improved security without significant costs to upgrade existing networks.

c. **Operational Benefits**

i. Simplified operations with centralized cloud-based management and security.

ii. Futureproof the network environment as quantum computers advance.

iii. Limited or no downtime for upgrades and rekeying of new algorithms.

d. **Security Benefits**

i. Provides an integrated, in-depth cybersecurity approach with continuous monitoring to ensure compliance with Federal security standards.

ii. Networks bypass brute-force attacks to protect sensitive agency data.

iii. Simplifies deployment of upgraded PQC standards as they change.

2. CHALLENGE SCENARIO

a. **Quantum computers are capable of breaking modern public key cryptography, and changing that encryption is difficult, disruptive, and resource intensive. This change can lead to downtime and lost productivity. The current transition to NIST-backed PQC algorithms may become an iterative process that requires ongoing swapping of cryptography. A quantum-based SD-WAN solution will allow agencies to migrate from hardware-based management to software-based technologies to future-proof their networks for the quantum era.**

3. CRITERIA FOR SUCCESS

a. **Successful implementation of a quantum-secure SD-WAN.**

b. **Stronger data security at the network edge, making data transmitted between sites secure against quantum attacks.**

c. **Seamless updates of quantum cryptography in real-time without service interruption.**

FIGURE 1: QUANTUM SD-WAN CHARACTERISTICS

4. FINANCIAL CONSIDERATIONS

a. **Quantum SD-WAN can lower the long-term total cost of ownership by providing agencies with a solution that continuously upgrades for next-generation cryptography without requiring network upgrades as technology changes (see Figure 1 Quantum SD-WAN Lifecycle). Human resources with the ability to manage an agency network and manage and maintain quantum-resistant cryptographic algorithms are already in short supply. An outsourced Quantum SD-WAN solution allows agencies to avoid expensive, multi-year cryptographic migration projects while being quantum safe and compliant with national security requirements.**

5. OPERATIONAL CONSIDERATIONS

a. **Quantum SD-WAN can provide the ultimate solution for protecting data, provide continuous upgrades for next-generation cryptography, and ensure agency networks comply with national security requirements. An SD-WAN solution is managed from the cloud with a single appliance for security and connectivity. To optimize network performance, IT staff can monitor and assess network health remotely and in real-time with overall network views and granular branch views.**

b. **Quantum SD-WAN can be implemented as part of a security and internet access solution.**

6. SECURITY CONSIDERATIONS

a. Quantum SD-WAN can support agencies in eliminating security gaps with embedded threat protection and prevention. They use security processors and threat-intelligence security services using artificial intelligence while providing full visibility into applications, users, and networks for both on-premises and remote workers.

7. WHERE TO BUY

a. Enterprise Infrastructure Solutions (EIS)

i. EIS is a multiple award, indefinite delivery, indefinite quantity (IDIQ), Best-in-Class Contract (BIC)

ii. Agencies can use GSA's acquisition tools to implement an SD-WAN solution with quantum-safe security.

- SD-WAN Overview and Ordering Guide.
- Quick-start solicitation templates to support SD-WAN as part of agency modernization.
- Solicitation Assist Tool to assist agencies in writing solicitation documents.

b. Governmentwide Acquisition Contracts (GWACs)

i. GSA's Alliant 2, VETS 2 and 8(a) STARS III GWACs are multiple-award, indefinite-delivery indefinite-quantity (IDIQ) contracts for information technology service solutions, including emerging technology.

ii. All GSA GWACs are designated as tier three Best-in-Class solutions.

iii. Agencies can utilize the GSA GWACs to develop turnkey solutions for SD-WAN). These may include, but are not limited to: secure communications, cryptography/encryption, and security assessments.

iv. Additional information regarding how to utilize the GSA GWACs can be found at www.gsa.gov/gwacs

8. GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your Quantum SD-WAN. Thank you for reading!

Information for this use case came from the following sites with QSaaS solutions:

Fortinet and Quantum Xchange Team to Deliver Quantum-Safe SD-WAN | QuantumXC

Quantum SD-WAN Datasheet (checkpoint.com)

QIST Use Case: Post-Quantum Cryptography (PQC) Planning and Implementation

1. HIGHLIGHTS

a. Challenge: to protect secure communications; such as health, financial, and national security data; from untrusted adversaries. It has become clear that current communication methods will not be secure once quantum computers reach their full potential, and it is necessary to prepare for that eventuality starting now.

b. Proposed solution: begin planning for implementation of NIST standards for approved complex cryptographic algorithms for post-quantum key encapsulation methods (KEM) and digital signature algorithms. Industry leaders have developed initial solutions for implementation of PQC algorithms in agency network environments.

c. Operational Benefits

i. Development of a comprehensive, centralized inventory of all systems, applications, databases, and other cryptographic assets.

ii. Documentation of policies and procedures for current and future system requirements.

iii. Planning and testing to avoid system disruption as a result of transition.

iv. Communication with stakeholders on transition plans.

d. Security Benefits

i. Identification of where and how public-key algorithms are being used in agency networks to allow for proper transition planning.

ii. Development of a comprehensive plan to protect sensitive data as adversaries are initiating Store Now, Decrypt Later (SNDL) attacks which could have catastrophic consequences for agencies and their customers, as well as national security in the future.

iii. Implementation of cryptographic agility, as part of the PQC transition, to support rapid adaptation of future cryptography into current network infrastructure.

2. CHALLENGE SCENARIO

a. When quantum computers become available, attackers will be able to use them to break existing public key encryption (PKE) and compromise sensitive national data on an unprecedented scale. As a result, the White House issued a National Security Memorandum (NSM 10) mandating that federal agencies comply with quantum-resistant encryption algorithms approved by the National Institute for Standards and Technology (NIST). The memorandum applies to critical infrastructure "so vital to the United States that their incapacitation or destruction would have a debilitating effect on the Nation's security, economy, public health and safety, or any combination thereof." System inventories and transition and implementation planning are critical to the success of agencies being ready to transition cryptographic assets to quantum safe cryptographic algorithms.

3. CRITERIA FOR SUCCESS

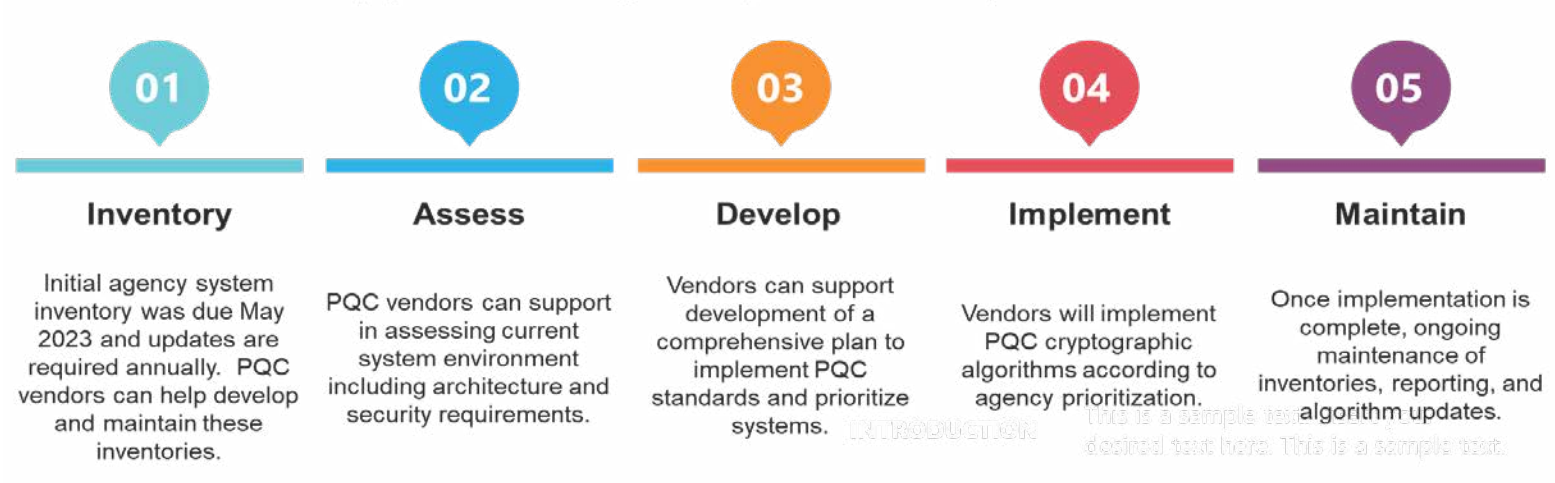
a. **Successful completion of complete cryptographic asset inventory.**

b. **Development of a comprehensive implementation plan.**

c. **Documentation of quantum-resistant cryptographic algorithm policies and procedures to support implementation.**

d. **Continuing maintenance of quantum-resistant cryptography.**

FIGURE 2: AGENCY SUPPORT FOR PQC IMPLEMENTATION



4. FINANCIAL CONSIDERATIONS

a. **Lack of preparation and identification of all phases of implementation can result in costly delays to update or redevelop implementation plans. Developing and deploying agile cryptography will allow for updates and changes without additional costs to develop new implementation plans. The cost of failing to implement PQC could mean loss of sensitive data to known and unknown adversaries.**

5. OPERATIONAL CONSIDERATIONS

a. **A complete PQC solution that supports inventory development, transition planning, implementation and continued maintenance will help agency CIO's meet current and future OMB and legislative requirements for PQC. Quantum-experienced resources are in short supply and the**

time required to hire and train personnel to complete the transition to PQC may be prohibitive. Contractor support through MSS or MNS will allow for PQC algorithm implementation to be tested and verified prior to deployment to avoid interruption of operations. Ongoing support and maintenance will free resources to concentrate on other mission-critical initiatives.

6. SECURITY CONSIDERATIONS

a. **Agency requirements for transition are complex and the use of PQC experts can alleviate the burden of hiring and training new resources in a timely manner to meet implementation timelines. In addition, once the initial inventory, assessment, and implementation are complete, ongoing PQC maintenance includes implementing all future algorithm updates and meeting all future federal security requirements. A complete crypto-agile PQC solution can be implemented as part of a larger Managed Network Service (MNS) as it would complement the services provided as part of managed security.**

7. WHERE TO BUY

a. **Enterprise Infrastructure Solutions (EIS) Contract**

   i. Multiple award, indefinite delivery, indefinite quantity (IDIQ), Best-in-Class (BIC) Contract.

   ii. Agencies can use GSA's acquisition tools to implement PQC solutions.

   - Managed Security Services (MSS) and Managed Network Services (MNS) on GSA BIC contracts can be leveraged to create PQC solutions to meet agency needs.
   - Quick-start solicitation templates to modernize agency networks through the use of MNS and MSS solutions.
   - Solicitation Assist Tool to assist agencies in writing solicitation documents.

b. **Highly Adaptive Cybersecurity Services SIN (HACS)**

   i. Multiple award, IDIQ Contract

   ii. Agencies can use GSA's acquisition tools to implement PQC solutions.

   - Request for Quote (RFQ) and additional solicitation templates (e.g., High Value Asset, Incident Response, and Cyber Hunt) with typical contract language that can be cut and pasted into solicitation documents.
   - HACS-specific Independent Government Cost Estimator (IGCE) tool
   - Cybersecurity subject matter and buyer's guides (eg., Advanced Persistent Threat, Cybersecurity Supply Chain Risk Management (C-SCRM), Zero Trust Buyer's Guide, and Application Security Testing (AST) Guide)

c. **Governmentwide Acquisition Contracts (GWACs)**

   i. GSA's Alliant 2, VETS 2 and 8(a) STARS III GWACs are multiple-award, indefinite-delivery indefinite-quantity (IDIQ) contracts for information technology service solutions, including emerging technology.

ii. All GSA GWACs are designated as tier three Best-in-Class solutions.

iii. Agencies can utilize the GSA GWACs to develop turnkey solutions for PQC.. These may include, but are not limited to: assessment, development and implementation of highly complex cryptography solutions.

iv. Additional information regarding how to utilize the GSA GWACs can be found at www.gsa.gov/gwacs

8. GSA IS HERE TO HELP

If you would like more information on the topics covered in this paper, please reach out to your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348 to get in touch. GSA has multiple offerings for products, services, and solutions to support your planning, implementation, and continued support of the components of your PQC planning and implementation. Thank you for reading!

Information for this use case came from the following sites with PQC solutions:
https://www.sandboxaq.com/post/agile-cryptography-for-financial-organizations?utm_source=googleADs&utm_medium=paidmedia&utm_campaign=BFSI_April&utm_content=Article_AgileCrypto_Financial&utm_term=agile_cryptography

https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)

How to Get QIST Products and Services

1. ORDERING GUIDANCE

a. Contract Vehicles

1. Enterprise Infrastructure Solutions (EIS)

   A. Multiple award, indefinite delivery, indefinite quantity (IDIQ) Contract

   B. Best-in-Class (BIC) Contract

   C. 7/31/17 – 7/30/32

   D. Vendors

      i. AT&T

      ii. BT Federal

      iii. Comcast

      iv. Core Technologies

      v. Granite

      vi. Lumen

      vii. MetTel

      viii. Verizon

   E. Benefits of Using EIS

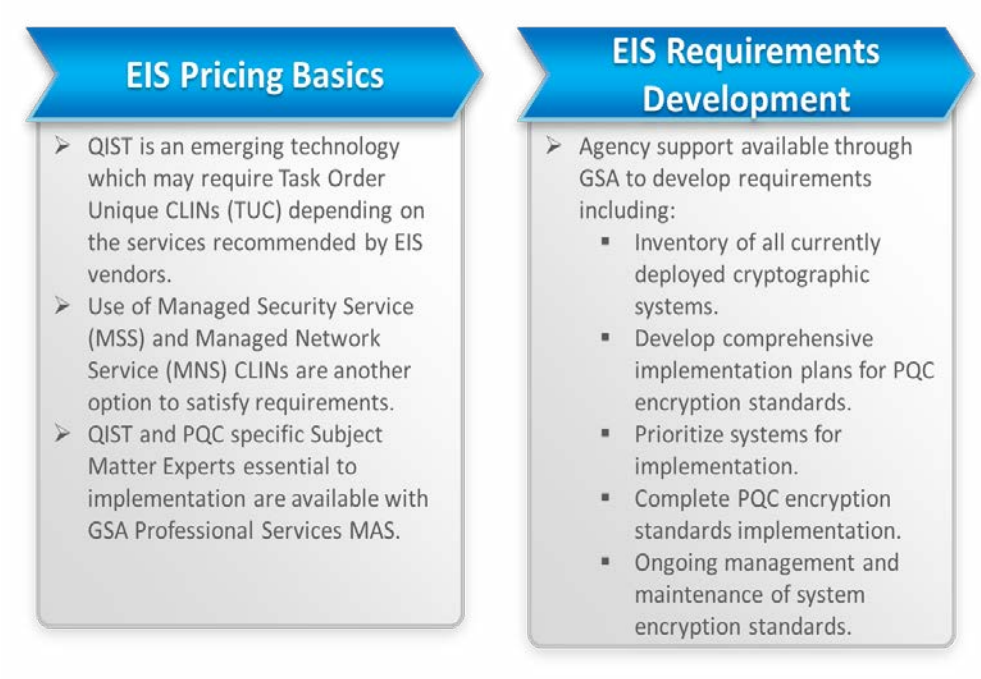
Benefits of Using EIS
Scope available to accommodate emerging technologies such as PQC encryption standards.
EIS prime contractors can bring on subcontractors providing expertise in PQC encryption standards.
GSA provides agency support with requirements development and scope review.
Long-term contract options.

F. Pricing Basics and Requirements Development

i. For support with requirements development reach out to your agency's Solutions Broker.

ii. To find your agency's Solution Broker's contact information, please visit Customer Support

FIGURE 1: EIS BASIC PRICING AND REQUIREMENTS



2. Special Item Number (SIN)

A. Agency support needs may include independent Quantum subject matter expertise, which can be obtained through other service contracts such as MAS IT Professional Services (54151S) or Highly Adaptive Cybersecurity Services (54151HACS) Special Item Numbers (SINs).

i. Ongoing support may include:

- Support the agency in completing an inventory of systems and security protocols.
- Provide support to agencies also working with EIS vendors in the development, implementation, and ongoing maintenance of PQC encryption standards.

ii. Pricing may be based on labor categories and the time required to complete the work. Initial support would be more labor intensive and drop off as standards are implemented and move to maintenance.

iii. These SINs provide agencies with options to meet various socioeconomic factors, receive small business credits, and ensure compliance with OMB Memo M-22-03.

3. Governmentwide Acquisition Contracts (GWACs)

A. GSA GWACs are long-term solutions for information technology services. The period of performance varies by contract.

B. The GWAC websites include information regarding industry partners, pricing, ordering procedures and more.

C. Each GWAC has specific labor categories which encompass a wide range of technology solutions.

D. Additional labor categories and CLINS may be added to a GWAC task order to meet agency needs

E. A dedicated program team can assist agencies with market research, review statements of work for scope compatibility, and provide agency training.

b. Developing QIST Requirements

PQC is still an emerging technology with some initial solutions being developed. As solutions and best practices evolve, creating acquisition templates to support agencies will be a key factor in promoting the use of EIS and other GSA contract solutions.

QIST Lessons Learned and Frequently Asked Questions (FAQ)

1. LESSONS LEARNED

FIGURE 1: QIST LESSONS LEARNED

Transition experience has shown that early assignment of resources and planning are critical to success. In addition to having a dedicated team to manage the QIST transition to post-quantum cryptography, agencies need to include 'worst case' scenarios in their planning to ensure minimal impact to operations throughout the transition. GSA has contract options and acquisition expertise to provide easy access to QIST industry experts and to assist in the development of acquisition packages including scope review[24].

2. FREQUENTLY ASKED QUESTIONS (FAQ)

a. Why is quantum computing a threat?

Current cryptographic algorithms used for online transactions, secure communications, and digital signatures will be vulnerable to attack as quantum computing evolves. As cryptographically relevant quantum computers (CRQC) become available they can be used by adversaries and threat actors to decrypt and read existing documents and files with sensitive information. They can also be used to falsify documents and digital signatures.

24 https://www.gsa.gov/system/files/TSMP_for_EIS_v51%20FINAL-508.pdf

b. Why is PQC important to my agency now?

Large technology transitions are complex and inevitably take longer than expected. Planning now for changes in security capabilities will ensure your agency is secure when CRQC becomes available. Planning now is an important step to ensure future readiness.

c. When will CRQC become available?

No one knows for sure, as a lot of information is being closely held by the United States and other countries working to develop CRQC. It is estimated that 6,000 stable qubits will be required to break public-key algorithms. Google has publicly stated its goal of building a 1,000 stable qubit machine by 2030.

d. What do agencies need to do now to prepare?

Agencies should be planning and preparing for the transition to understand their needs to future-proof the confidentiality of encrypted information sent over unsecured networks. Agencies should also ensure any new technology product procurements are cryptographically agile with encryption that is easily upgraded or replaced as standards change.

e. What will updating current encryption technology require?

Implementing PQC will be a multi-year process that will necessitate the identification and allocation of financial and human resources, detailed transition planning, working with trusted industry partners, continuous engagement from leadership, and ongoing communication with agency leadership, oversight agencies, and stakeholders.

3. ACRONYM LIST

Acronym	Full Phrase
AES	Advanced Encryption Standards
BIC	Best-in-Class
CLIN	Contract Line Item Number
CRQC	Cryptanalytically Relevant Quantum Computers
DOE	Department of Energy
EIS	Enterprise Infrastructure Solutions
FAQ	Frequently Asked Question
FIPS	Federal Information Processing Standards
GDIT	General Dynamics Information Technology
GWAC	Governmentwide Acquisition Contract
HACS	Highly Adaptive Cybersecurity Services
MAS	Multiple Award Schedule
MNS	Managed Network Service
MSS	Managed Security Service
NIST	National Institute of Standards and Technology
NQI	National Quantum Initiative

Acronym	Full Phrase
NSM	National Security Memorandum
NSS	National Security Systems
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
PKC	Public-Key Cryptography
PQC	Post-Quantum Cryptography
QIST	Quantum Information Science and Technology
QSaaS	Quantum Security-as-a-Service
RSA	Rivest-Shamir-Adleman
SBA	Small Business Administration
SBIR	Small Business Innovation Research
SD-WAN	Software-Defined Wide Area Network
SIN	Special Item Number
SWOT	Strengths, Weaknesses, Opportunities, Threats
TUC	Task Order Unique CLIN

Contributors

Organization	Introduction	Slip Sheet	White Paper	Use Cases	How To Get	FAQ/Lessons Learned
General Services Administration (GSA)	X	X	X	X	X	X
JPI Solutions (JPI)	X	X	X	X	X	X