U.S. General Services Administration

Post Quantum Cryptography

Buyer's Guide

GSA Federal Acquisition Service
Office of Information Technology Category

Version 1

June 2025

Table of Contents

1 Executive Summary

The Post-Quantum Cryptography (PQC) Buyer’s Guide for federal agencies is a resource designed to assist agencies in their efforts to prepare systems to protect sensitive data from potential attacks by future quantum computers. Once quantum computing becomes available, it will be capable of breaking much of the public-key cryptography currently used on digital systems jeopardizing civilian and military communications, undermining supervisory and control systems, and defeating security protocols for most internet-based financial transactions.

This Guide is a resource that will enable agencies to safeguard existing systems from both classical and quantum computer based attacks and ensure the confidentiality and integrity of data communications.

2 Purpose

The purpose of the PQC Buyer’s Guide is to provide federal agencies with practical guidance on acquiring products, services, and solutions that support the agency’s implementation of PQC encryption standards. It outlines the essential steps required to prepare for and implement a transition to PQC and provides General Services Administration (GSA) consumers with the knowledge they need to make informed decisions as part of the procurement process.

By following the recommendations outlined in this guide, federal agencies can ensure they are able to mitigate the risks that quantum computers pose by preparing for and developing the implementation plan to transition to quantum-resistant cryptographic standards. This guide emphasizes the importance of collaboration between agency stakeholders and industry partners to ensure successful implementation and alignment with the National Institute of Standards and Technology (NIST) PQC standards.

3 Audience

The audience for this guide includes Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Data Officer (CDO), Chief Privacy Officer, Information Technology (IT) managers, and Cybersecurity professionals who are responsible for protecting the data or critical infrastructure of a federal agency against the threat of adversaries using quantum computers to break the encryption methods used to protect sensitive information. This Guide is not intended to be a detailed discussion of quantum security but an overview to assist program and acquisition professionals seeking to acquire the capabilities through contracted industry partners.

The PQC Buyer’s Guide is suitable for federal agencies in any stage of the cycle of planning, designing and implementing PQC encryption standards. It provides practical guidance on the steps needed to acquire, implement, and maintain PQC products, services, and solutions. The guide assumes a basic understanding of public-key encryption, post-quantum encryption, and cybersecurity.

4 What is PQC

PQC is defined as a method of encryption developed to protect sensitive data from quantum computers, classical computers, and unauthorized access and is able to interoperate with existing communications protocols and networks. Cryptographically relevant quantum computers (CRQC) will be capable of breaking much of the public-key cryptography used on digital systems, jeopardizing civilian and military communications, undermining supervisory and control systems, and defeating security protocols for most internet-based financial transactions. Once quantum computing becomes readily available, public-key algorithms utilized with many federal systems will be vulnerable to criminals, adversarial foreign threats, and other bad actors looking to exploit sensitive data.

5 Current Federal Standards and Guidance for PQC

Public Law 115-368, The National Quantum Initiative Act of 2018

This act established the National Quantum Initiative (NQI) to develop a 10-year plan to accelerate quantum research and development for the economic and national security of the United States. One focus of the NQI program is Quantum Technology, which includes efforts to understand and mitigate risks associated with quantum technologies using PQC.

NIST PQC Standards

The PQC program at NIST is crucial to securing critical public infrastructure once quantum computers are available. NIST PQC standards were released on August 13, 2024 and include encryption algorithms, instructions on how to implement into products and encryption systems, and their intended uses. These standards include Federal Information Processing Standards (FIPS) 203 (https://csrc.nist.gov/pubs/fips/203/final), FIPS 204 (https://csrc.nist.gov/pubs/fips/204/final), and FIPS 205 (https://csrc.nist.gov/pubs/fips/205/final). These standards are the primary tools to protect against future attacks for general encryption and digital signature schemes. Transitioning federal IT systems to these new standards will take time, resources, and commitment.

Public Law 117-260, Quantum Computing Cybersecurity Preparedness Act

National Security Memorandum (NSM)-10, dated May 2022 and codified into law with the Quantum Computing Cybersecurity Preparedness Act in December 2022, outlines requirements for agencies to assess all uses of vulnerable cryptography in unclassified systems and develop a timeline to transition to quantum-resistant cryptography. Inventory requirements include identifying current cryptographic methods used on IT systems, system administrator protocols, non-security software and firmware that require upgraded digital signatures, and information on other key assets.

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

By aligning with these requirements, agencies can establish a foundational plan for system transition to PQC standards. They can inventory their systems and security protocols, identify public-key cryptography, and prioritize their systems based on organizational functions, goals, and needs. Agencies can also work to develop cryptographic agility, which is the ability of a system to adjust its encryption mechanisms quickly and easily. This includes the ability to change encryption keys, key lengths, encryption algorithms, and the libraries used for encryption.

NIST Internal Report (IR) 8547 Transition to Post-Quantum Cryptography Standards

This publication, issued in November 2024, is in its initial public draft which closed on January 10, 2025. It outlines NIST's expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes. It identifies existing quantum-vulnerable cryptographic standards and the quantum resistant standards to which information technology products and services will need to transition.

NIST anticipates that the timeline from algorithm standardization to full integration into information systems can take 10 to 20 years, which reflects the complexity of building these algorithms into products and services, procuring those products and services, and integrating into technology infrastructures. Adversaries are employing the "harvest now, decrypt later" approach to collecting encrypted data now with the goal of decrypting it once quantum computers are available. Since sensitive data remains relevant for years, this threat model is one of the primary reasons why transition to PQC is urgent.

NIST IR 8547 is the initial step in the strategy to manage and guide the transition to PQC. It includes guidance and timing on the deprecation, controlled legacy use, and eventual removal of quantum vulnerable algorithms currently in use. It also continues NIST's ongoing dialogue with industry, standards organizations, and relevant agencies to develop a clear roadmap and realistic timeline for transitioning to PQC. NIST aims to balance the urgency to adopt PQC standards with the need to minimize system disruptions.

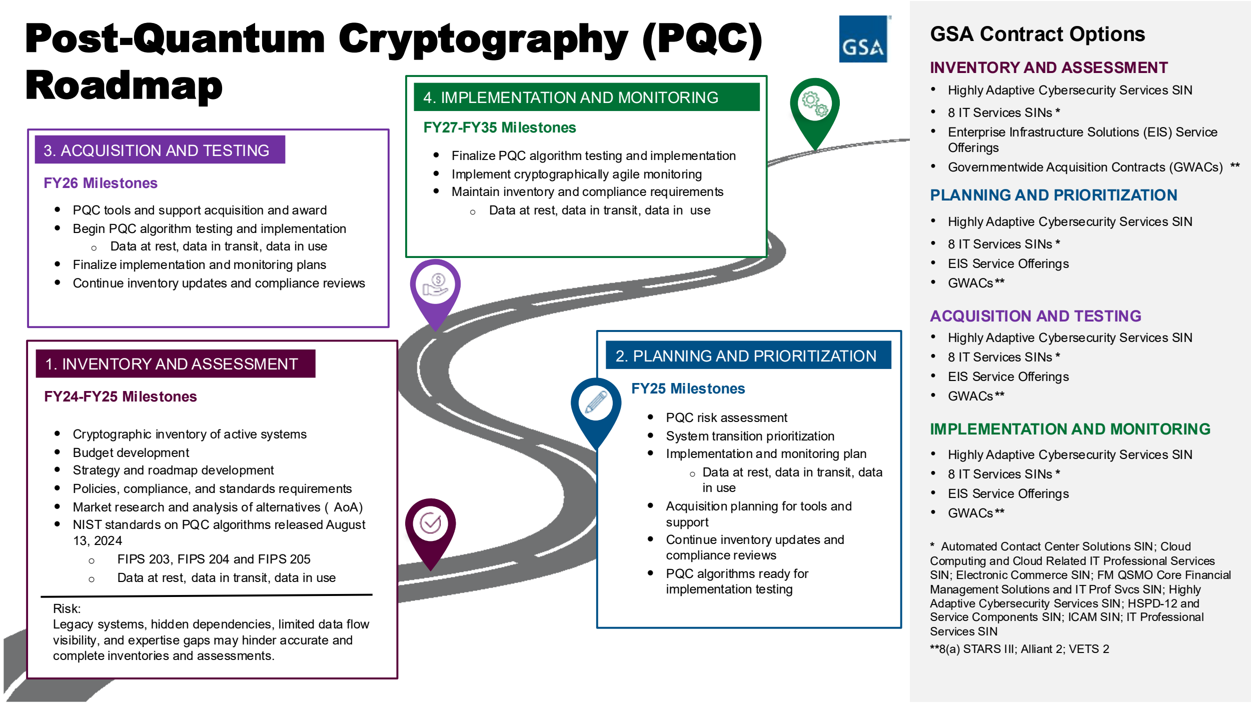
The tables and use cases in this document are helpful for agencies and vendors in understanding the current quantum-vulnerable cryptographic standards in use and the replacement quantum-resistant algorithms to replace them. It also includes useful timelines and definitions for acceptable, deprecated, disallowed, and legacy use algorithms moving forward. (IR 8547, Transition to Post-Quantum Cryptography Standards | CSRC)

6 PQC Implementation Components and Requirements

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 is still an emerging technology with evolving applications and solutions, however, accepted solutions will become available for agency implementation now that the final NIST PQC standards have been issued. The following sections highlight the actions agencies must take to prepare for transition.

Figure 1 PQC Roadmap



Post-Quantum Cryptography (PQC) Roadmap

1. INVENTORY AND ASSESSMENT

FY24-FY25 Milestones

- Cryptographic inventory of active systems
- Budget development
- Strategy and roadmap development
- Policies, compliance, and standards requirements
- Market research and analysis of alternatives (AoA)
- NIST standards on PQC algorithms released August 13, 2024
  - FIPS 203, FIPS 204 and FIPS 205
  - Data at rest, data in transit, data in use

Risk:
Legacy systems, hidden dependencies, limited data flow visibility, and expertise gaps may hinder accurate and complete inventories and assessments.

2. PLANNING AND PRIORITIZATION

FY25 Milestones

- PQC risk assessment
- System transition prioritization
- Implementation and monitoring plan
  - Data at rest, data in transit, data in use
- Acquisition planning for tools and support
- Continue inventory updates and compliance reviews
- PQC algorithms ready for implementation testing

3. ACQUISITION AND TESTING

FY26 Milestones

- PQC tools and support acquisition and award
- Begin PQC algorithm testing and implementation
  - Data at rest, data in transit, data in use
- Finalize implementation and monitoring plans
- Continue inventory updates and compliance reviews

4. IMPLEMENTATION AND MONITORING

FY27-FY35 Milestones

- Finalize PQC algorithm testing and implementation
- Implement cryptographically agile monitoring
- Maintain inventory and compliance requirements
  - Data at rest, data in transit, data in use

GSA Contract Options

INVENTORY AND ASSESSMENT

- Highly Adaptive Cybersecurity Services SIN
- 8 IT Services SINs *
- Enterprise Infrastructure Solutions (EIS) Service Offerings
- Governmentwide Acquisition Contracts (GWACs) **

PLANNING AND PRIORITIZATION

- Highly Adaptive Cybersecurity Services SIN
- 8 IT Services SINs *
- EIS Service Offerings
- GWACs**

ACQUISITION AND TESTING

- Highly Adaptive Cybersecurity Services SIN
- 8 IT Services SINs *
- EIS Service Offerings
- GWACs**

IMPLEMENTATION AND MONITORING

- Highly Adaptive Cybersecurity Services SIN
- 8 IT Services SINs *
- EIS Service Offerings
- GWACs**

* Automated Contact Center Solutions SIN; Cloud Computing and Cloud Related IT Professional Services SIN; Electronic Commerce SIN; FM QSMO Core Financial Management Solutions and IT Prof Svcs SIN; Highly Adaptive Cybersecurity Services SIN; HSPD-12 and Service Components SIN; ICAM SIN; IT Professional Services SIN

**8(a) STARS III; Alliant 2; VETS 2

Figure 1 above shows GSA's current Quantum Cryptography Roadmap, which is available in the EIS Public Pricer Resources.

6.1 Inventory of Critical Systems and Data

NSM-10 required agencies to submit a comprehensive, centralized inventory of all systems, applications, databases, and other cryptographic assets that are CRQC-vulnerable to the Office of the National Cybersecurity Director (ONCD) and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). These initial inventories were due May 4, 2023 and expected to include all of the following (whether operated by the agency or on the agency's behalf):

- High impact information systems
- High Value Assets (HVAs); or
- Any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks.

In addition, agencies were asked to provide additional details:

- Information systems or assets that:
    - Contain data expected to remain mission-sensitive in 2035; or
    - Are logical access control systems based in asymmetric encryption (such as Public Key Infrastructure).
- Lifecycle characteristics of the data contained in the system, including types of data (as described by national records management categories) and how long the data and associated metadata need protection (i.e., "time to live").
- Systems that may not be able to migrate to PQC as soon as possible to avoid delays in migrating other systems. The interconnected and interoperable nature of cryptography across agency networks may mean that one system that cannot be migrated may prevent others from migrating as well.
- System administrator protocols, non-security software and firmware that require upgraded digital signatures.

For these submissions, agencies were required to utilize CyberScope to submit inventories to CISA and ONCD through a spreadsheet format as mandated by the Office of Management and Budget (OMB) for FISMA compliance.

In addition to the system inventory, agencies needed to submit an assessment of the funding required to migrate systems to PQC. Both the inventory and funding assessments are due annually following the initial submission. Using agency inventory and cost estimates, the OMB published the White House Report on Post-Quantum Cryptography in July 2024 (Report on Post-Quantum Cryptography).

6.2 Assess Current System Environment

Agency documentation and identification of current cybersecurity and data security standards that will require updating to comply with NIST PQC standards (https://csrc.nist.gov/publications/fips) is a key next step in planning for the transition process. Agencies will need to develop new processes, tools, and best practices for complying with the standards for PQC implementation. Processes should include criteria to evaluate software security and the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

This step in the PQC process should also be used to develop a prioritization of systems for replacement based on organizational functions, goals and needs. The following factors need to be considered:

- Is the system a HVA based on organizational requirements?
- What is the system protecting (e.g. passwords, root keys, signing keys, personally identifiable information [PII], sensitive PII)?

- What other systems does the system communicate with? Are they inside or outside the agency?
- Does the system share data with other agencies or organizations outside the agency?
- Does the system support critical infrastructure?
- How long is data protection needed?

When interpreting responses to these questions, agencies should assess their systems holistically, considering immediate as well as medium- and long-term security needs. The responses should guide prioritization efforts for post-quantum cryptography (PQC) migration by identifying the most critical systems requiring early attention. Agencies should document in detail their findings to ensure alignment with risk management strategies, regulatory requirements, and agency goals. Agencies should use the responses to develop a phased implementation plan that addresses interdependencies and concerns regarding external data-sharing. This process will help agencies strategically allocate resources to safeguard sensitive data and maintain mission-critical operations in the evolving cryptographic landscape. Additionally, the number of HVA systems and the complexity of their interaction with other systems and the public are critical components required to engage with industry partners to understand how they can support and supplement agency resources throughout the transition process.

6.3 Develop Plan for Transition and Post-Transition Maintenance

The Quantum Computing Cybersecurity Preparedness Act instructs the Director of OMB to issue guidance requiring each executive agency to develop a plan, including interim benchmarks, to migrate information technology of the agency to post-quantum cryptography. Development of a comprehensive plan to implement PQC security measures will include the following key components:

- **Prioritizing systems for implementation:** Is completed while assessing the current system environment and carried forward as one of the first steps in developing the transition plan.
- **Test new NIST algorithms:** Include time for testing algorithms, as valuable hands-on experience is gained through testing prior to permanent upgrades.
- **Avoid Rip and Replace:** Assess options that can install quantum-resilient algorithms over existing cryptography to avoid "rip and replace" of the entire network.
- **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:** Consider implementation plans that deploy quantum-resilient algorithms without installing on edge devices, making securing the core network easier and quicker.

- **Consider a hybrid approach:** Consider leaving existing encryption in place while transitioning to quantum-resilient algorithms to ensure network safety. Finalize transition once there is confidence the new algorithms are performing properly.
- **Plan for the future:** The initial set of NIST PQC standards is not anticipated to be the last, and agencies must plan now to ensure future encryption standards can be integrated into their IT infrastructure through their maintenance and upgrade processes in a timely manner.
- **Communication:** Develop a communication plan and seek input from stakeholders on the development of a transition plan. Provide documentation with answers to common questions and talking points for agency leadership when discussing with users and the public.

The NIST Internal Report NIST IR 8547 (Initial Public Draft) Transition to Post-Quantum Cryptography Standards is another resource for agencies when developing their PQC transition plans.

6.4 Implement and Maintain PQC

Once inventory and planning are complete, implementation begins according to the system prioritization developed in the plan. Resources for the migration need to be available and system users informed as implementation proceeds.

Consideration of different implementation approaches based on the complexity and number of systems. One approach is a hybrid migration that uses Public Key Infrastructure (PKI) algorithms alongside PQC algorithms to ensure the new algorithms are performing as expected. In contexts where only exchanging of signatures (and no keys), transitioning to hash-based signature schemes may be more appropriate than the alternative hybrid approach, which is complicated and more difficult to implement. Working with qualified industry partners in the planning stages can assist in determining which approach is right for each transitioning system.

Depending on the solution chosen, post-implementation system maintenance is critical to continued system security. Industry leaders expect that some algorithms will fail, some will need adjustment, and some will work. Building crypto-agility into all phases of the PQC transition planning will allow agencies to switch to new cryptography and not have to commit to only one algorithm. In addition, continuous monitoring will allow for future updates as they become available and prevent the need to go through a complicated implementation process again.

6.5 Key Considerations for PQC Products, Services, and Solutions

When acquiring products, services, and solutions to support and align with PQC requirements, federal agencies should carefully evaluate a range of factors to ensure they meet their specific requirements. Section 6.6 of this document provides several use cases that may assist agencies in developing acquisition options for PQC planning, implementation, and maintenance.

The following key considerations may also help agencies make informed decisions and select the most suitable PQC products, services, and solutions:

Alignment with NIST Standards

Products being offered should be compliant with NIST standards. Vendors providing support for inventory, planning, implementation and maintenance should be evaluated on proven performance in understanding the complexity of the new NIST standards either in their company's past performance or through strong partnerships with companies that do.

NIST has a certification process through the NIST Cryptographic Module Validation Program (CMVP). The CMVP consists of an independent test to ensure that defenses using cryptographic algorithms are built correctly and function as intended. These tests are conducted by NIST-accredited testing labs and the results are sent to NIST for final certification. In addition to federal agencies, the governments of Canada, Japan, and several industry regulators use the CMVP certifications, driving international operability.

As vendors integrate these newly approved algorithms into hardware and software, NIST will evaluate these implementations under the CMVP. Vendors without a CMVP certification should be able to demonstrate how they meet the requirements included in the certification process.

The NIST Migration to Post-Quantum Cryptography project aims to demonstrate automated tools for identifying public-key cryptography use in hardware, software, and protocols within data centers. Target audiences include developers, integrators, and standardization bodies. It will showcase methods to discover public-key algorithms in network infrastructures, detail their purposes, and prioritize components for migration based on risk management principles. Organizations were invited to participate through a Federal Register call.[1] Respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement to collaborate with NIST in a consortium to build this example solution. Finally, the project will establish approaches for transitioning to quantum-resistant algorithms.

Vendor Expertise and Support

Agencies should evaluate the vendor's expertise, reputation, and record of accomplishment in developing and implementing PQC solutions. Consider its ability to provide ongoing support, updates, and timely responses to security vulnerabilities or emerging threats. PQC standards are complex and will require subject matter expertise to implement successfully.

Scalability and Flexibility

PQC is still an emerging technology and agencies should consider a vendor's ability to adapt to changes in requirements and deadlines. Vendors should be able to show how they can effectively adapt when changes and challenges occur.

[1] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Managed Service or as-a-Service Options

PQC implementation will be complex and require resources with expertise in designing, implementing, and maintaining system security. Agencies may consider working with vendors that offer MNS, MSS, or PQC as-a-service options. These options are scalable and place the burden of upkeep on the vendor providing the service which can free agency resources for mission critical priorities.

User Experience

Agencies will require a transition implementation that does not negatively impact on user experience and productivity. Vendor solutions should provide seamless access to authorized users while minimizing disruption and unnecessary authentication steps. Transition planning with clear communication, training, and support can contribute to a positive user experience throughout the process.

Cost and Return on Investment

Assess the total cost of ownership, including upfront costs, licensing fees, ongoing maintenance, and operational expenses. Consider the potential return on investment in terms of improved security, reduced risk, operations efficiency gains, and long-term sustainability.

Training and Documentation

Evaluate the availability of comprehensive training materials, documentation, and user guides to facilitate configuration, implementation, and ongoing management of the solution. Adequate training and support contribute to the successful adoption and future maintenance of PQC solutions. The GSA IT Training SIN is an exceptional resource for meeting your training needs.

Futureproofing

Can vendors provide solutions that address continuous improvement and the ability to address emerging security challenges. Ensure the vendor will be crypto-agile to allow agencies to switch to new cryptography and not commit to one algorithm as quantum capabilities advance and new algorithms are introduced by NIST to evolving threats.

6.6 Example Use Cases

This Buyer's Guide provides use case examples to help agency buyers understand some of the options available for PQC transition.

PQC Use Case: Automated Cryptography Discovery and Inventory (ACDI) Tools

1. **Highlights**
    a. ACDI tools that detect and inventory the types of cryptography in use on assets are in various stages of development across industry. There is ongoing research with CISA to develop standards on combining ACDI tools and continuous diagnostic and monitoring programs to lessen the resources required to generate cryptographic

inventories each year.

b. CISA has not been able to confirm the full scope of cryptographic algorithm detection capabilities that will be available via ACDI tools. For example, it is not clear if these tools will be able to detect the embedded algorithms used within software packages, such as custom- or government-developed software.

c. These tools could automate the collection of the cryptographic characteristics required for annual inventory submissions to ONCD and CISA.

d. Currently, OMB requires manual inventory reporting, however, dual inventory collections using both manual and automated tools will work to ensure completeness and accuracy of identifying cryptographic systems until standards are issued for use of ACDI.

2. **Operational Benefits**

   a. Simplified annual reporting and ongoing maintenance of a centralized cryptographic inventory.

   b. Reduction in resources required to complete the annual inventory process.

   c. These tools will also allow agencies to meet the annual inventory requirements of OMB-M-23-02.

3. **Security Benefits**

   a. Eliminates the need for security personnel to be familiar with all software, files, and applications in use by an agency.

   b. Helps verify findings from manual inventories and ensure nothing is missed.

   c. Provides continuous monitoring as new systems and applications are implemented.

4. **GSA Contract Options**

   a. 8(a) STARS III

   b. Alliant 2

   c. VETS 2

   d. Software Licenses (SIN 511210)

   e. Software Maintenance Services (SIN 54151)

   f. Electronic Commerce and Subscription Services (SIN 54151ECOM)

5. **Criteria for Success**

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

   b. Centralized monitoring and simplified processes for the addition of new systems and applications.

c. Supplement fully manual inventories by moving to a hybrid inventory approach.

6. Future Considerations

a. Currently, there are no known ACDI tools that can capture all nine (9) of the required data items used for reporting to ONCD and CISA. Once suitable ACDI programs are available a pilot program will be developed to integrate the tools into the Continuous Diagnostics and Mitigation (CDM) tool suite.

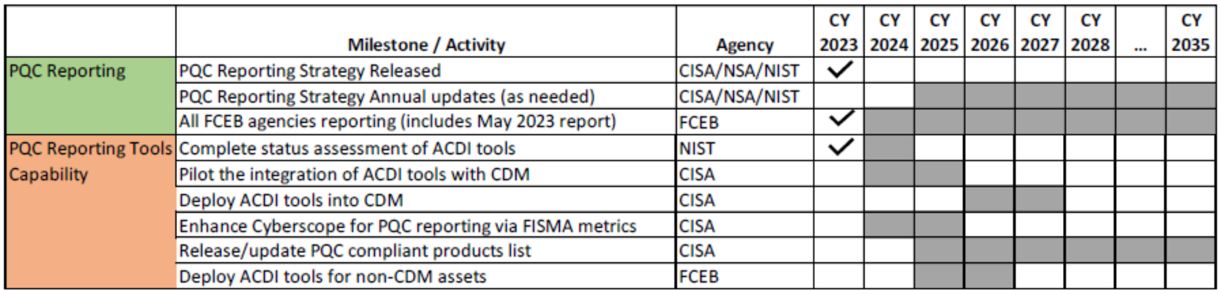
b. Once ACDI tools become available, they will be added to the CDM approved products list. Agencies will continue to manually report assets that cannot be discovered by CDM.

c. CISA will eventually use CDM dashboards and CyberScope reporting to identify systems and agencies struggling to implement the products necessary for the transition to PQC. CISA will be able to offer support to accelerate PQC adoption efforts and identify vulnerable systems for mitigation actions.

d. An ACDI system will ultimately reduce the number of staff necessary to complete the annual inventory and will support agencies in meeting the requirements of OMB M-23-02.

The following table from the CISA Strategy for Migrating to Automated PQC Discovery and Inventory Tools provides a notional timeline of the high-level activities required to achieve deployment of ACDI tools into CDM and meet FISMA requirements.

Table 1 Timeline



	Milestone / Activity	Agency	CY 2023	CY 2024	CY 2025	CY 2026	CY 2027	CY 2028	...	CY 2035
PQC Reporting	PQC Reporting Strategy Released	CISA/NSA/NIST	✓							
	PQC Reporting Strategy Annual updates (as needed)	CISA/NSA/NIST			▨	▨	▨	▨	▨	▨
	All FCEB agencies reporting (includes May 2023 report)	FCEB	✓	▨	▨	▨	▨	▨	▨	▨
PQC Reporting Tools Capability	Complete status assessment of ACDI tools	NIST	✓	▨						
	Pilot the integration of ACDI tools with CDM	CISA		▨	▨					
	Deploy ACDI tools into CDM	CISA				▨	▨			
	Enhance Cyberscope for PQC reporting via FISMA metrics	CISA		▨	▨					
	Release/update PQC compliant products list	CISA			▨	▨	▨	▨	▨	▨
	Deploy ACDI tools for non-CDM assets	FCEB			▨	▨				

GSA contract options are available for IT services that would support agencies in determining how to implement ACDI tools to supplement their manual inventory processes. As ACDI tools become available in the marketplace, these vendors will be able to assist in determining the best fit for agency needs.

PQC 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.

2. Operational Benefits

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

b. Document policies and procedures for current and future system requirements.

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

d. Communication with stakeholders on the transition plan.

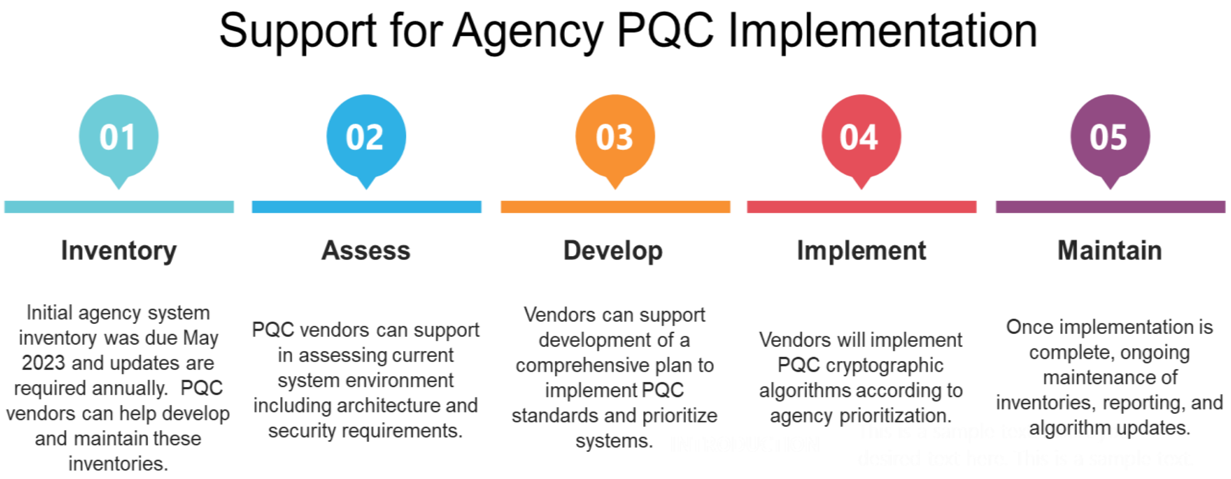
3. Security Benefits

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

b. Develop a comprehensive plan to protect sensitive data as adversaries are initiating "harvest now, decrypt later" attacks which could have catastrophic consequences for agencies and their customers, as well as national security, in the future.

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

Figure 2: Support Descriptions for PQC Implementation



Support for Agency PQC Implementation

01 **Inventory**

Initial agency system inventory was due May 2023 and updates are required annually. PQC vendors can help develop and maintain these inventories.

02 **Assess**

PQC vendors can support in assessing current system environment including architecture and security requirements.

03 **Develop**

Vendors can support development of a comprehensive plan to implement PQC standards and prioritize systems.

04 **Implement**

Vendors will implement PQC cryptographic algorithms according to agency prioritization.

05 **Maintain**

Once implementation is complete, ongoing maintenance of inventories, reporting, and algorithm updates.

4. GSA Contract Options

a. 8(a) STARS III

b. Alliant 2

c. Cloud Compute and Cloud Related IT Professional Services

d. Enterprise Infrastructure Solutions

e. Highly Adaptive Cybersecurity Services SIN 54151HACS

f. IT Professional Services SIN 54151S

g. VETS 2

5. 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.

6. Financial Considerations

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

7. **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 Managed Security Service (MSS) or Managed Network Service (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.

8. **Security Considerations**

   a. Agency requirements for transition are complex and the use of PQC experts through HACS or IT Professional Services can provide resources to meet immediate requirements while giving agencies time to hire and train in-house staffing levels. 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. An agency can implement a complete crypto-agile PQC solution as part of a larger MNS turn key solution as it would complement the services provided as part of managed security moving forward.

PQC 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 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. Proposed solution: Quantum Security-as-a-Service solutions are currently developing. When available to Federal agencies they are anticipated to be subscription based IT solutions added to an agency's in house network operations.

2. **Operational Benefits**

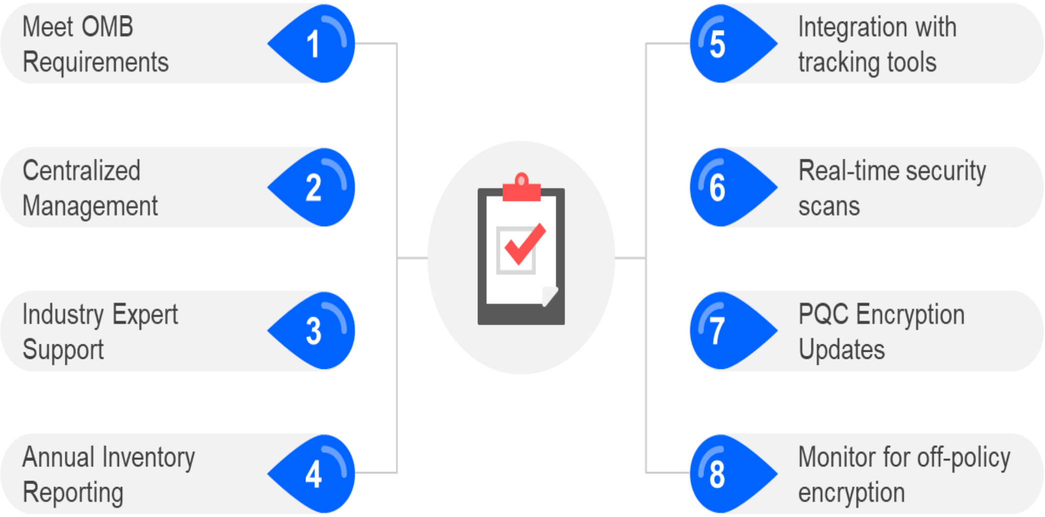
   a. Simplified operations with centralized cloud-based management and security.

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

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

3. **Security Benefits**
    a. Real-time identification of system vulnerabilities and cryptographic algorithms that do not adhere to OMB requirements.
    b. Crypto-agility and the ability to easily adhere to new cryptographic requirements without additional development.
    c. Monitor and remediate off-policy algorithms.

Figure 3 Quantum-Security-as-a-Service Benefits



4. **GSA Contract Options**
    a. 8(a) STARS III
    b. Alliant 2
    c. Enterprise Infrastructure Solutions
    d. VETS 2

5. **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. Centralized maintenance and updates based on new standards and simplified processes for the addition of new systems and applications.
    d. A well trained workforce is a key contributor to success. The GSA IT Training SIN can be a valuable resource for meeting an agency's IT training needs.

6. **Financial Considerations**
    a. Agency leadership will need to consider the cost of all aspects of implementing PQC and protection of systems against threats of quantum computers. Leaders will need to assess if they have internal resources with the skills to oversee and manage implementation of this magnitude. Costs would include the contractor support needed to bridge the gap in expertise while the agency trains their IT workforce to manage the new PQC requirements.
    b. A QSaaS solution would cover the full migration lifecycle and 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.
7. **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.
8. **Security Considerations**
    a. PQC standards are complex and will require subject matter expertise to implement. The QSaaS solution will ensure that once the initial inventory, assessment, and implementation are complete, ongoing maintenance would include implementing all future algorithm updates and meeting all future federal security requirements.
    b. Implementation of QSaaS as part of a larger MNS would complement the services provided as part of managed security.

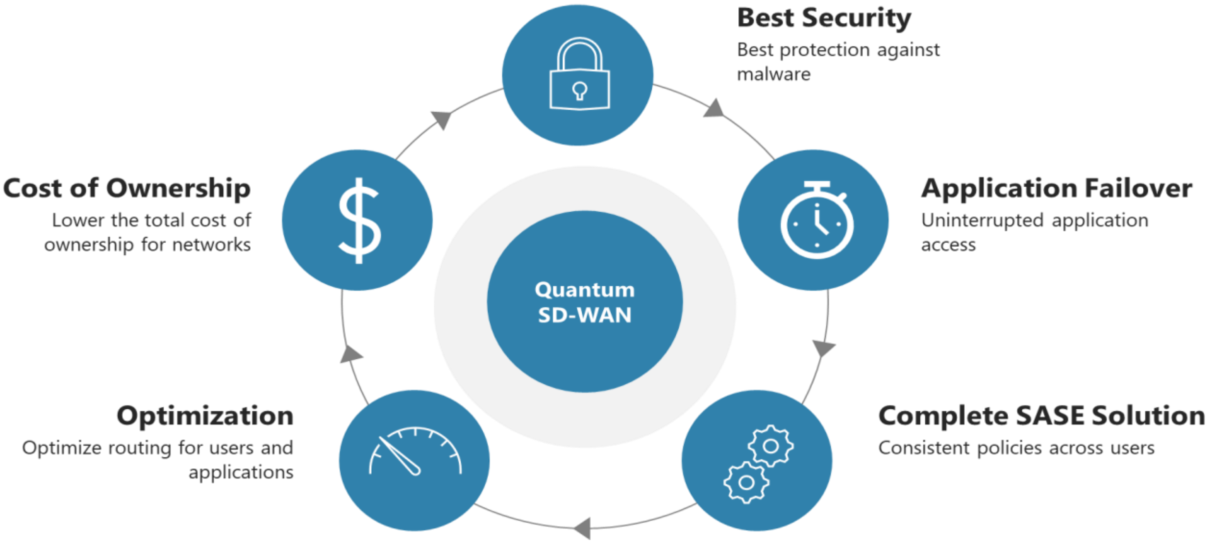
PQC Use Case: Quantum SD-WAN

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.

2. **Operational Benefits**
    a. Simplified operations with centralized cloud-based management and security.
    b. Futureproof the network environment as quantum computers advance.
    c. Limited or no downtime for upgrades and rekeying of new algorithms.
3. **Security Benefits**
    a. Provides an integrated, in-depth cybersecurity approach with continuous monitoring to ensure compliance with Federal security standards.
    b. Networks bypass brute-force attacks to protect sensitive agency data.
    c. Simplifies deployment of upgraded PQC standards as they change.
4. **GSA Contract Options**
    a. 8(a) STARS III
    b. Alliant 2
    c. Enterprise Infrastructure Solutions
    d. VETS 2
5. **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.
    d. A well trained workforce is a key contributor to success. The GSA IT Training SIN can be a valuable resource for meeting an agency's IT training needs.

Figure 4: Quantum SD-WAN Cycle


Best Security
Best protection against malware
Application Failover
Uninterrupted application access
Complete SASE Solution
Consistent policies across users
Optimization
Optimize routing for users and applications
Cost of Ownership
Lower the total cost of ownership for networks
Quantum SD-WAN

6. **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 4 Quantum SD-WAN Lifecycle). A Quantum SD-WAN solution allows agencies to avoid expensive, multi-year cryptographic migration projects while being quantum safe and compliant with national security requirements.

7. **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. Implementation of Quantum SD-WAN as part of a security and internet access solution.

8. **Security Considerations**

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

PQC Use Case: Quantum PQC and Zero Trust Architecture (ZTA)

1. **Highlights**
    a. Challenge: agencies need to implement both ZTA and PQC with limited resources and budgets making prioritization a challenge.
    b. Proposed solution: implementation of both ZTA and PQC requires trusted identity, access and encryption using continuous monitoring. Cryptography, including PQC algorithms, offer a foundation for ZTA, and building systems with crypto agility in mind are designed to quickly incorporate new protocols without requiring significant change to system infrastructure.
2. **Operational Benefits**
    a. Flexible solution with centralized cloud-based management and security.
    b. Futureproof the network environment as security compliance requirements advance.
    c. Limited or no downtime for upgrades and implementation of upgrades.
3. **Security Benefits**
    a. Provides an integrated, in-depth cybersecurity approach with continuous monitoring to ensure compliance with Federal security standards.
    b. PQC will harden zero trust in identity and access management (IAM), privileged access management (PAM), micro segmentation, multi-factor authentication (MFA), protecting log data and communications encryption, and data security, including protecting data at rest.
    c. Seamless modernization as technology continues to change and adversaries grow more sophisticated.
4. **GSA Contract Options**
    a. 8(a) STARS III
    b. Alliant 2
    c. Cloud Compute and Cloud Related IT Professional Services
    d. Enterprise Infrastructure Solutions
    e. Highly Adaptive Cybersecurity Services SIN 54151HACS
    f. Homeland Security Presidential Directive-12 and Service Components SIN 541519PIV
    g. Identity, Credentialing and Access Management SIN 541519ICAM
    h. VETS 2

5. Criteria for Success

a. Ensure agency systems align with the core principle of Zero Trust while incorporating PQC to provide granular access control, strong authentication, continuous monitoring, and least privilege access.

b. Compliance with CISA and NIST ZTA Standards as well as impending NIST PQC standards.

c. Continuous improvement to address emerging security threats with a solution that can evolve with threats and technological advancements.

Table 2 Shared Principles of Zero Trust and Crypto-agility

Zero Trust Principle	Crypto-Agility Principle
Presume Breach	Encrypt sensitive data and mitigate breaches with micro-segmentation.
Analyze Behavior	Ensure compliant cryptography is used in development.
Architectural Alignment	Enforce policies and security guarantees with an access control architecture.
Least Privilege	Know what cryptography is used where, how, and by whom.
Verify Explicitly	Reliably control cryptographic validation in authentication mechanisms.
Simplify and Automate	Update and replace PQC algorithms using automation.

d. Initial implementation can strain resources, including specialized expertise, security tools, and infrastructure upgrades. The long-term benefits of a more secure and resilient infrastructure often outweigh the initial challenges. Combining ZTA and PQC may help alleviate the cost of completing each implementation separately. Agencies can leverage the same types of resources to implement both concurrently and reduce the risk of missing key components of one or the other if implemented separately.

6. Operational Considerations

a. A centralized key management system that has implemented post quantum algorithms as part of its core capabilities allows for effective cryptographic asset enumeration and cryptographic agility as it allows for the rapid adoption of PQC algorithms as part of an agency's security posture and the implementation of an effective transition strategy from "traditional" public key algorithms to PQC ones.

b. A centralized key lifecycle management and cryptographic provider provides an identity management system with the capacity to generate hybrid certificates that utilize PQC cryptographic keys in conjunction with "traditional" public key cryptography (i.e. RSA or elliptic curve keys) while allowing for automation, monitoring and logging capabilities to accommodate large, enterprise-scale deployments.

7. **Security Considerations**
    a. Planning now to strengthen ZTA frameworks with PQC will help close security gaps in legacy approaches to cryptography. This will be central to the future of identity-based security scaling beyond endpoints.
    b. PQC algorithms will further harden the encryption technologies that zero-trust's reliability, stability, and scale rely on. PQC secures data in transit and at rest which also strengthens zero trust.

7 PQC Buyer's Guide Contact Information

For questions related to any aspect of this guide, or PQC products, services, or solutions, contact the GSA National Customer Service Center at: 855-482-4348 email: ITCSC@gsa.gov and reference the GSA Schedules identified in Appendix A of this PQC Buyer's Guide.

Appendix A: Current GSA Offered Products, Services, and Solutions for PQC

GSA offers agencies support in designing and implementing PQC solutions using its Best-in-Class (BIC) contracts. Agencies can utilize GSA's acquisition support tools to design, implement, and support solutions for PQC. Links to applicable contract options are located in **Appendix D**.

Table 1: GSA Offered Services and Contracts

Services	Description	GSA Contracts
Inventory of Critical Systems and Data	NSM-10 inventory requirements include current cryptographic methods used on IT systems as well as: ● High impact information systems ● HVA; or ● Any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks. ● Agencies should include information systems or assets that: ○ Contain data expected to remain mission-sensitive in 2035; or ○ Are logical access control systems based in asymmetric encryption (such as Public Key Infrastructure). ● Lifecycle characteristics of the data contained in the system, including types of data (as described by national records management categories) and how long the data and associated metadata need protection (i.e., "time to live"). ● System administrator protocols, non-security software and firmware that require upgraded digital signatures.	● 8(a) STARS III ● Alliant 2 ● Automated Contact Center Solutions SIN 561422 ● Cloud Computing and Cloud Related IT Professional Services ● Electronic Commerce SIN 54151ECOM ● Enterprise Infrastructure Solutions ● Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services (518210FM) ● Highly Adaptive Cybersecurity Services SIN 54151HACS ● Homeland Security Presidential Directive-12 and Service Components SIN 541519PIV ● IT Professional Services SIN 54151S ● VETS 2 ● Software Licenses SIN 511210 ● Software Maintenance Services SIN 54151
Assess Current System Environment	Develop new standards, tools, and best practices to comply with PQC standards and procedures criteria for cybersecurity described in the NSM-10. Guidelines must include: ● Criteria that is used to evaluate software security,	● 8(a) STARS III ● Alliant 2 ● Automated Contact Center Solutions SIN 561422 ● Cloud Computing and Cloud Related IT Professional Services ● Electronic Commerce SIN 54151ECOM

Services	Description	GSA Contracts
	● Criteria to evaluate the security practices of the developers and suppliers and identify tools or methods to demonstrate conformance with secure encryption practices.	● Enterprise Infrastructure Solutions ● Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services 518210FM ● Highly Adaptive Cybersecurity Services SIN 54151HACS ● Homeland Security Presidential Directive-12 and Service Components SIN 541519PIV ● IT Professional Services SIN 54151S ● VETS 2 ● Software Licenses SIN 511210 ● Software Maintenance Services SIN 54151
Develop Plan for Transition and Post-Transition Maintenance	Development of a comprehensive plan to implement PCQ security measures including the following components: ● Prioritizing systems for implementation: ● Test new NIST algorithms ● Avoid Rip and Replace ● Protect the entire network ● Avoid installing edge devices ● Consider a hybrid approach ● Plan for the future ● Communication planning	● 8(a) STARS III ● Alliant 2 ● Automated Contact Center Solutions SIN 561422 ● Cloud Computing and Cloud Related IT Professional Services ● Electronic Commerce SIN 54151ECOM ● Enterprise Infrastructure Solutions ● Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services (518210FM) ● Highly Adaptive Cybersecurity Services SIN 54151HACS ● Homeland Security Presidential Directive-12 and Service Components SIN 541519PIV ● IT Professional Services SIN 54151S ● VETS 2

Services	Description	GSA Contracts
		● Software Maintenance Services SIN 54151
Implement and Maintain PQC	Implement PQC according to the prioritization of systems based on the sensitivity of data stored and the security of other systems that interact with the agency. Transition IT infrastructure to agile cryptography that adheres to all federal security requirements. Centralized maintenance and updates based on new standards and simplified processes for the addition of new systems and applications.	● 8(a) STARS III ● Alliant 2 ● Automated Contact Center Solutions SIN 561422 ● Cloud Computing and Cloud Related IT Professional Services ● Electronic Commerce SIN 54151ECOM ● Enterprise Infrastructure Solutions ● Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services (518210FM) ● Highly Adaptive Cybersecurity Services SIN 54151HACS ● Homeland Security Presidential Directive-12 and Service Components SIN 541519PIV ● IT Professional Services SIN 54151S ● VETS 2 ● Software Licenses SIN 511210 ● Software Maintenance Services SIN 54151
Managed Network and Managed Security Services	Enable agencies to outsource all or a portion of planning, design, implementation, maintenance, operations, and customer service to improve IT services and lower costs.	● Enterprise Infrastructure Solutions
X-as-a-Service Offerings	As-a-service offerings can provide streamlined, scalable, cost-effective solutions that place the burden of infrastructure implementation and maintenance on the provider, including compliance and security updates. PQC as-a-service solutions are being developed and may be an option for agencies to explore.	● 8(a) STARS III ● Alliant 2 ● Cloud Compute and Cloud Related IT Professional Services SIN 518210C ● Enterprise Infrastructure Solutions ● Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions

Services	Description	GSA Contracts
		and IT Professional Services (518210FM) ● Software Licenses SIN 511210 ● VETS 2
IT Training	Enable agencies fill gaps in the skill sets of their current workforce and to maintain a well trained IT workforce in the future.	● IT Training SIN (611420)

Appendix B: NIST PQC Algorithms

NIST released the first three finalized PQC algorithm standards on August 13, 2024, with Federal Information Processing Standards (FIPS) 203, FIPS 204, and FIPS 205. Each of the selected algorithms are specialized for different applications for optimal computer interoperability and cybersecurity as described below.

- **FIPS203** (https://csrc.nist.gov/pubs/fips/203/final): This is intended as the standard for general encryption for secure communications. It is based on the CRYSTALS-Kyber algorithm, renamed ML-KEM (Module-Lattice-Based Key-Encryption Mechanism). ML-KEM is an algorithm that uses lattice-based cryptography to enable small key sizes that target resource-constrained devices and allows for comparatively small encryption keys that exchange quickly and easily between two parties. It is a faster algorithm than elliptic curves and Rivest-Shamir-Adleman (RSA), both in software and hardware.
- **FIPS204** (https://csrc.nist.gov/pubs/fips/204/final): ML-DSA, is a lattice-based digital signature algorithm for applications that require a digital signature rather than a written signature. It is based on the CRYSTALS-DILITHIUM algorithm and can be used to generate and verify digital signatures. It is believed to be secure against adversaries in possession of a large-scale fault-tolerant quantum computer. ML-DSA's scheme can be used to detect unauthorized modifications to data and to authenticate the identity of the signatory (one bound to the possession of the private-key).
- **FIPS205** (https://csrc.nist.gov/pubs/fips/205/final): This is also designed for digital signatures. It is based on the Sphincs+ algorithm, which has been renamed SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). SLH-DSA is an alternative approach to ML-DSA, using an entirely different mathematical principle - this time a hash-based cryptography - which allows stateless verification. It has been created in case future weaknesses are found in ML-DSA but has larger signature sizes and is arguably less mature compared to the other algorithms. It is intended as a backup to ML-DSA in case it proves vulnerable. The SLH-DSA algorithm is not approved for any use in National Security Systems per the CISA NSA Commercial National Security Algorithm Suite 2.0 published in December 2024.

Lattice-Based Cryptography

Lattice-based cryptography 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 one of the most secure PQC encryption methods because while current algorithms, like RSA, rely on factoring large prime numbers, lattice algorithms rely on the difficulty of finding the right lattice point in a high dimensional vector space.

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:

- **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** - computes 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 implementation in hardware 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.

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.

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 re-generated digital signatures 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.
- **Secure Blockchains**: application of a hash function to a data block provides a hashed value. Blockchains use random or semi-random numbers (nonces), and each transaction requires hashing an additional data block.
- **Discover Duplications**: hash functions are used to examine similar data and locate modified files in data/file storage.

Hash-based cryptography offers the following benefits:

- **Ensure data integrity**: identify tampered data 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 no modification of data 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.

Appendix C: References

This buyer's guide was developed in accordance with the following references.

Public Law 115-368 National Quantum Initiative Act of 2018
National Security Memorandum 10, May 4, 2022, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems
Fact Sheet: Presidential Directives Advancing Quantum Technologies of May 4, 2022
Public Law 117-260 Quantum Computer Cybersecurity Preparedness Act of December 21, 2022
OMB Memorandum M-23-02 Migrating to Post-Quantum Cryptography, November 18, 2022
National Quantum Initiative Supplement to the President's FY2023 Budget December 1, 2023
Migration to Post Quantum Cryptography Website 44National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE)
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
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)
OMB Report on Post-Quantum Cryptography July 2024
FIPS 203, FIPS 204, and FIPS 205 August 13, 2024
CISA Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools August 15, 2024
NIST Internal Report Transition to Post-Quantum Cryptography Standards Initial Public Draft November 2024

Appendix D: Current GSA Vehicle Reference

Multiple Award Schedule – Information Technology

Multiple Award Schedule (MAS) Information Technology (IT) shortens procurement cycles, ensures compliance, and delivers the best value on over 7.5 million innovative IT products, services, and solutions from over 4,600 pre-vetted vendors. It offers federal, state, local and tribal governments innovative solutions for their information technology needs. Below are the MAS IT Solutions and Special Item Numbers (SINs) categorized based on government mandates, industry evolution, and buying trends that have been identified:

- **Cloud Services**
  Cloud Compute and Cloud Related IT Professional Services (SIN 518210C)
- **Electronic Commerce**
  Electronic Commerce (SIN 54151ECOM)
- **Financial Management Services**
  Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services (SIN 518210FM)
- **IT Services**
  Health IT Services (SIN 54151HEAL)
  Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS)
  IT Professional Services (SIN 54151S)
- **IT Software**
  Software Licenses (SIN 511210)
  Software Maintenance Services (SIN 54151)
- **IT Solutions**
  Automated Contact Center Solutions (SIN 561422)
  Identity, Credential and Access Management (ICAM) (SIN 541519ICAM)
  Public Key Infrastructure (PKI) Shared Services Provider (SSP) Program (SIN 541519PKI)
  Homeland Security Presidential Directive 12 Product and Service Components (SIN 541519IPIV)
- **IT Training**
  IT Training SIN (611420)

  Source:https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it

2nd Generation IT Blanket Purchase Agreements

2nd Generation IT (2GIT) BPAs offers in-scope, pre-competed commercial hardware, software, and ancillary services:

- Software License - Term Software & Perpetual (511210)
- Software Maintenance Services (54151)
- OLM - Order-Level Materials

The 2GIT BPA also offers access to mission-critical, best-value IT from a diverse pool of more than 70 industry partners, solutions that meet current procurement policies, incorporating best practices like collecting prices paid data, and options that support the FY19 SECURE Technology Act and other federal cybersecurity efforts.

Source: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/2git-bpa

Governmentwide Acquisition Contracts (GWAC)

Governmentwide Acquisition Contracts (GWAC) are cost-effective, innovative solutions for IT requirements available to the federal government. GWACs provide access to pre-competed Best-in-Class IT solutions to include: System Design; Software Engineering; Information Assurance; and Enterprise architecture solutions. Below are the GWAC contracts:

- 8(a) STARS III
- Alliant 2
- VETS 2 (SDVOSB)

Source:https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/gwacs

Telecommunications and Network Services

Telecommunications and Network Services provides cost-effective communications infrastructure and network needs. Below are the telecommunication and network services contracts:

- Enterprise Infrastructure Solutions (EIS)

Source:https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/telecommunications-and-network-services

Glossary

Acronym	Description
2GIT	2nd Generation IT Blanket Purchase Agreement
ACDI	Automated Cryptography Discovery and Inventory
BIC	Best-in-Class
BPA	Blanket Purchase Agreement
CCOE	Cybersecurity Center of Excellence
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COTS	Commercial Off the Shelf
CRQC	Cryptographically Relevant Quantum Computers
DEOS	Defense Enterprise Office Solutions Blanket Purchase Agreement
DoD	Department of Defense
DSA	Data Structures and Algorithms
DSS	Digital Signature Scheme
EIS	Enterprise Infrastructure Solutions
FIPS	Federal Information Processing Standards
FY	Fiscal Year
GSA	General Services Administration
GWAC	Governmentwide Acquisition Contracts
HVA	High Value Asset
IAM	Identify and Access Management
IT	Information Technology
KEM	Key Encapsulation Mechanism
MFA	Multi-Factor Authentication
ML-DSA	Module-Lattice-Based Digital Signature Algorithm

Acronym	Description
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MNS	Managed Network Service
MSS	Managed Security Service
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technologies
NQI	National Quantum Initiative
NSM	National Security Memorandum
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
PAM	Privileged Access Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography