United States Government Accountability Office

Report to the Ranking Member, Joint Economic Committee

October 2026

QUANTUM COMPUTING

Federal Actions Needed to Prepare for Emerging Cyber Threat

Errata statement - Revised on October 14, 2026 to clarify the summary on the highlights page as well as pages 5 and 43 of our coordination with executive branch agencies to obtain agreement that sensitive information was appropriately removed.

AMERICA250 & GAO
Informing Democracy Through Oversight

GAO-27-108740

GAO Highlights

QUANTUM COMPUTING

Federal Actions Needed to Prepare for Emerging Cyber Threat

GAO-27-108740 October 2026

A report to the Ranking Member, Joint Economic Committee

For more information, contact: Marisol Cruz Cain at cruzcainm@gao.gov

What GAO Found

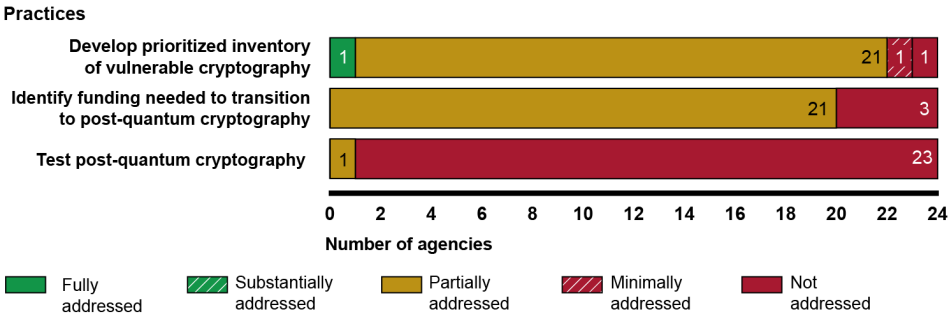
Quantum computers leverage qubits (the quantum equivalent of classical computer bits) to solve specific problems significantly faster than classical computers. However, the emergence of quantum computers could undermine the cryptography (e.g., encryption) that federal agencies use to secure their systems. Today's quantum computers cannot yet break this cryptography. But a future quantum computer of sufficient size and sophistication—referred to as a cryptographically relevant quantum computer (CRQC)—could potentially do so for certain cryptography.

Most industry experts believe that a CRQC will be developed, possibly as soon as the 2030s. However, development estimates vary widely due to several factors, such as uncertainty in the rate of growth for qubits and how many qubits will be needed. Once a CRQC is developed, its use could have devastating impacts to federal systems reliant on vulnerable cryptography. For example, a malicious actor could use a CRQC to

- compromise systems that ensure the authenticity of system users—thus allowing the actor to gain access to sensitive information; and
- decrypt (or unlock and view) data that the actor acquires and stores prior to the development of such a computer.

To address the threat posed by a CRQC, it is important that agencies transition existing systems to more secure cryptography (referred to as post-quantum cryptography). Using Office of Management and Budget guidance, GAO created an evaluation framework of three practices that agencies should address to prepare for this transition. However, none of the 24 selected agencies fully addressed these practices (see figure).

Extent to Which the 24 Chief Financial Officer Act Agencies Addressed Preparatory Practices for Migrating to Quantum Computing



Source: GAO analysis of agency information. | GAO-27-108740

The incomplete implementation of these practices is due in part to a lack of (1) cryptography expertise, (2) processes for developing cryptography inventories and identifying funding needed to transition to post-quantum cryptography, and (3) plans to guide post-quantum cryptography testing. Until the selected agencies address these weaknesses, they will not be well-positioned to address the threat of CRQCs to cryptography that agencies rely on to protect sensitive information.

Why GAO Did This Study

Federal agencies rely on cryptography to protect sensitive data and systems. However, some experts predict that a quantum computer capable of breaking certain cryptography may be developed within the next 10 to 20 years.

GAO was asked to review the threat of quantum computing to federal agency cryptography. This report describes (1) the threats quantum computers pose to cryptography on federal agencies' information systems and (2) the extent to which federal agencies have begun preparing for this threat consistent with federal guidance.

GAO also evaluated cryptography inventories, funding assessments, and other planning documentation at each of the 24 Chief Financial Officer Act agencies to determine the extent to which they had addressed transition preparatory practices consistent with federal guidance.

This is a public version of a sensitive report that GAO issued in September 2025. GAO coordinated with the executive branch agencies included in this review from September 2025 through September 2026 to obtain concurrence that sensitive information was appropriately removed.

What GAO Recommends

In the sensitive report, GAO made 89 recommendations to 23 agencies to, among other things, establish and implement processes to develop inventories of vulnerable cryptography and identify funding for post-quantum cryptography. Twelve agencies agreed with GAO's recommendations, two partially agreed, seven neither agreed nor disagreed, and one disagreed with three of its four recommendations. GAO maintains that all recommendations are warranted. GAO is not making any additional recommendations in this public version.

Contents

Letter		1
	Background	5
	Quantum Computers Pose Significant Threats to Cryptography on Federal Systems	12
	Agencies Have Not Fully Implemented Preparatory Practices for Addressing Quantum Cyber Threats	20
	Conclusions	33
	Recommendations for Executive Action	34
	Agency Comments and Our Evaluation	34
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	Summary of China's Efforts to Prioritize Quantum Information Science Development	44
Appendix III	Summary of National Quantum Computing Cybersecurity Strategy	47
Appendix IV	Comments from the Department of Homeland Security	50
Appendix V	Comments from the Social Security Administration	52
Appendix VI	GAO Contact and Staff Acknowledgments	53

Tables

Table 1: Examples of Several Techniques Threat Actors with a Cryptographically Relevant Quantum Computer Could Use to Compromise Systems for Ensuring Authenticity	13
Table 2: Examples of Techniques That Threat Actors Could Use Now to Acquire Data to Later Be Decrypted by a Cryptographically Relevant Quantum Computer (CRQC)	14

Table 3: GAO Evaluation Framework of Post-Quantum Cryptography (PQC) Transition Preparatory Practices and Associated Activities 21
Table 4: GAO Evaluation Framework of Post-Quantum Cryptography (PQC) Transition Preparatory Practices and Associated Activities 39

Figures

Figure 1: A Simple Illustration of a Public-Key Cryptography Method Used to Protect Data 6
Figure 2: Units for Processing Information Used in Classical Computing Versus Quantum Computing 9
Figure 3: Thirty-Two Quantum Experts' Predicted Timeline for the Development of a Cryptographically Relevant Quantum Computer, as of December 2024 17
Figure 4: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Preparatory Practices for Migrating to Quantum Computing 22
Figure 5: Ranked Number of Quantum Computing Patents Filed Prior to June 2023 45
Figure 6: Share of Global Quantum Computing Articles Published between 2011-2020 46
Figure 7: The Three Central Goals of the U.S. National Quantum Computing Cybersecurity Strategy 47
Figure 8: Central Goals Outlined in the Documents That Comprise the U.S. National Quantum Computing Cybersecurity Strategy 48

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
CFO Act	Chief Financial Officers Act of 1990
CRQC	cryptographically relevant quantum computer
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
PQC	post-quantum cryptography

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

October 6, 2026

The Honorable Margaret Wood Hassan
Ranking Member
Joint Economic Committee

Dear Ranking Member:

Federal agencies depend on technology systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security. Agencies rely on cryptography (e.g., encryption) to help secure these systems and data.

However, the emergence of quantum computers could undermine the security of certain cryptographic methods.[1] Some experts predict that a quantum computer capable of breaking vulnerable cryptography—referred to as a cryptographically relevant quantum computer (CRQC)—may be developed in the next 10 to 20 years, putting agency systems that rely on this cryptography for security at risk. Furthermore, adversaries could copy data currently protected by vulnerable cryptography and store it with the intention of accessing and decrypting it later using a CRQC, once one is developed.

Recognizing the potential impact of this issue, we and others have highlighted the threat of a CRQC to cryptography. Since 2021, we have emphasized the threat of quantum computers as part of our Ensuring the Cybersecurity of the Nation high-risk area.[2] In addition, in November 2022

[1]A quantum computer is a device that leverages the properties of quantum physics to solve selected problems significantly faster than classical computers.

[2]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021); *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, GAO-23-106415 (Washington, D.C.: Jan. 19, 2023); and *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 13, 2024). In October 2021, we also assessed the maturity of these technologies and policy options that could help foster their development. GAO, *Quantum Computing and Communications: Status and Prospects*, GAO-22-104422 (Washington, D.C.: Oct. 19, 2021).

the Office of Management and Budget (OMB) called for federal agencies to prepare for the migration to cryptography that is resistant to quantum computers—referred to as post-quantum cryptography (PQC)—by

- developing prioritized inventories of vulnerable cryptographic systems,
- producing funding assessments to migrate to PQC, and
- testing PQC.[3]

You asked us to review the threat of quantum computing to the cryptography used by federal agencies. Our objectives were to (1) describe the threat quantum computers pose to cryptography on federal agencies' information systems, and (2) evaluate the extent to which federal agencies have implemented preparatory practices for addressing this threat.

This report is a public version of a sensitive report that we issued in September 2025.[4] Ten agencies in our review determined certain information in our September report to be sensitive, which must be protected from public disclosure. Although the information provided in this report is more limited, this report addresses the same objectives as the sensitive report and is based on the same audit methodology.

To address the first objective, we conducted a literature search for publicly available information on quantum computing and development of CRQCs in the U.S. and internationally. We reviewed relevant public reports, threat assessments, and other related documentation to obtain information on when a CRQC may be built and the impacts of such a computer.

Additionally, we interviewed knowledgeable officials and summarized documentation from federal agencies with responsibilities for (1) identifying and assessing cyber threats to federal agency systems—including threats posed by a CRQC, and/or (2) promoting quantum computing research and development. Those federal agencies are the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), the National Security

[3]Office of Management and Budget, *Migrating to Post-Quantum Cryptography*, M-23-02 (Washington, D.C.: Nov. 18, 2022).

[4]GAO, *Future of Cybersecurity: Federal Actions Needed to Prepare for Quantum Computing Threat*, GAO-25-107392SU (Washington, D.C.: Sept. 11, 2025).

Agency, the Office of the Director of National Intelligence, and the Office of Science and Technology Policy.

To address the second objective, we assessed the 24 Chief Financial Officers Act (CFO Act) agencies' preparation efforts against a framework we developed based on OMB guidance.[5] To compile the framework, we primarily reviewed relevant OMB guidance.[6] We also reviewed our prior work on IT system transition planning.[7] We then summarized this guidance and our prior work into three transition preparatory practices and eight associated activities. The practices were to (1) develop and annually update a prioritized inventory of agency systems with vulnerable cryptography, (2) conduct assessments to determine the funding needed to transition vulnerable cryptography on priority systems to PQC, and (3) test PQC in agency environments to help ensure that the algorithms will work in practice.

We then evaluated the 24 CFO Act agencies' efforts to address these three preparatory practices and the associated activities as follows:

- **Develop and annually update a prioritized inventory of agency systems with vulnerable cryptography.** To assess the first three of five activities in this practice, we collected and analyzed system inventories from the 24 CFO Act agencies and interviewed or collected written responses from knowledgeable officials regarding missing data and controls used to develop and maintain the

[5]The 24 CFO Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; the Social Security Administration; and the U.S. Agency for International Development.

[6]Office of Management and Budget, *Migrating to Post-Quantum Cryptography*, M-23-02.

[7]GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays*, GAO-20-155 (Washington, D.C.: Apr. 7, 2020).

inventories. To assess the remaining two activities, we selected 15 systems for further review at six agencies.[8]

We then randomly selected three systems[9] from five of the six selected agencies' prioritized inventories.[10] We asked knowledgeable agency officials to provide us with documentation that corroborated the information contained in the inventory for the selected systems.

- **Identify and annually update the funding needed to transition vulnerable cryptography on priority systems to PQC.** To assess the activity in this practice, we collected and reviewed agency funding assessments and interviewed or collected written responses from knowledgeable officials regarding missing data and controls used to develop and maintain the inventories.
- **Test PQC in agency environments to help ensure that the algorithms will work in practice.** To assess the two activities in this practice, we reviewed agencies' test plans and the results of any PQC testing. We also interviewed or collected written responses from knowledgeable officials regarding factors that prevented them from testing PQC.

We presented the results of our assessment to the 24 CFO Act agencies as well as OMB and the Office of the National Cyber Director (ONCD) and solicited their input and explanations for the results. Further details on our objectives, scope, and methodology are provided in appendix I.

The performance audit upon which this report is based was conducted from February 2024 to September 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a

[8]To select the agencies, we divided the fiscal year 2023 IT budgets of the 24 CFO Act agencies into three strata: (1) the eight agencies with the largest budgets, (2) the next eight agencies with moderate sized budgets, and (3) the last eight agencies with the smallest budgets. We then randomly selected six agencies for review—two from each stratum.

[9]In selecting these systems, we divided them into three strata: (1) high-value assets, (2) high-impact systems, and (3) other systems that agencies determine are likely to be particularly vulnerable to CRQC-based attacks. We then selected one system from each stratum.

[10]We were not able to select systems from the remaining agency because the agency had not developed an inventory of prioritized systems.

reasonable basis for our findings and conclusions based on our audit objectives.

We subsequently coordinated with executive branch agencies included in this review from September 2025 to September 2026 to obtain agreement that the contents of this public version of the original report, which was marked with controlled unclassified information designations, may be publicly released. This public version was also prepared in accordance with these standards.

Background

Technology systems have transformed how the federal government operates over the past 3 decades. The federal government uses IT systems to collect and disseminate funds, transfer benefits, enable tax filings, collect revenue, and procure goods and services. In addition, federal agencies use operational technology systems (i.e., programmable systems and devices that interact with the physical environment) to monitor building safety, generate and transmit electricity, and manufacture weapons.

However, technology systems supporting federal agencies are inherently at risk:

- These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed.
- This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.
- Compounding the risk, systems and networks used by federal agencies are often interconnected with other internal and external systems and networks, including the internet.
- Many of these systems are aging systems that may operate with known vulnerabilities that are either technically difficult or prohibitively expensive to address (referred to as legacy systems).

Threat actors are increasingly willing and capable of conducting cyberattacks on these complex and interconnected federal systems. According to the Intelligence Community: China, Russia, Iran, North Korea, and transnational criminal organizations pose the greatest cyber threats to the nation.[11] Attacks from these actors can facilitate

[11]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 25, 2025).

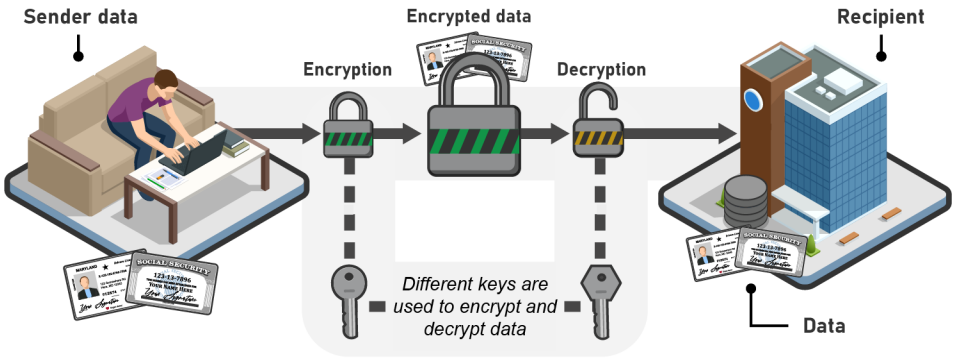
cybersecurity incidents with a range of consequences, such as disruption of critical operations and inappropriate access to and disclosure, modification, or destruction of sensitive information.

Overview of Cryptography

If properly implemented, cryptography can help to mitigate cybersecurity risks to federal technology systems. Cryptography protects information by transforming it using mathematical functions that create a series of characters referred to as “keys”. These keys are used to lock (encrypt) and unlock (decrypt) data in transit, as well as to “virtually sign” and authenticate documents. Only those who have access to the keys can view, access, and authenticate the data and documents.

Cryptographic techniques can generally be divided into two basic types: symmetric key and public-key cryptography.[12] Symmetric key cryptography uses the same private key to encrypt and decrypt data. By contrast, public-key cryptography works by using a private and public version of these keys. Information can be transmitted freely with the public key applied. However, it only becomes accessible when received by an individual or organization that has the other key (private) in the pair. When both these keys are combined, the information or data is successfully “unlocked” and can be used accordingly (see figure 1).

Figure 1: A Simple Illustration of a Public-Key Cryptography Method Used to Protect Data



Sources: GAO analysis; Golden Sikorka/stock.adobe.com (sender and recipient illustrations); vladwel/stock.adobe.com (key illustrations); Comauthor/stock.adobe.com (lock illustrations); GAO (all other illustrations). | GAO-27-108740

[12]Although there are more than two cryptographic techniques, we generally focus on symmetric and public-key cryptography for the purpose of our report.

Public-key Infrastructure

Public-key infrastructure uses cryptographic techniques to generate and manage electronic "certificates," which link an individual or entity to a given public key. These certificates are then used to verify digital signatures (providing authentication and data integrity) and facilitate data encryption (providing confidentiality). A properly designed and implemented public-key infrastructure can also be used to ensure that a given digital signature is still properly linked to the individual or entity associated with it (providing nonrepudiation).

In a small environment where everyone knows everyone else, users can individually give their public keys to the people they wish to deal with. In large-scale implementations, it is impractical to expect that each user will have previously established relationships with all of the other potential users in order to obtain their public keys.

One way around this problem is for all public-key infrastructure users and reliant entities to mutually agree to trust a third party who is known to everyone. The basic technical components for achieving third-party trust include (1) digital certificates, which link an individual to their public key, (2) certification authorities, which create these certificates and vouch for their validity to the entities relying on the public-key infrastructure, (3) registration authorities, which are in charge of verifying user identities so that the appropriate key pairs and digital certificates can be created, and (4) certification paths, which are used for recognizing and trusting digital certificates issued by other public-key infrastructures in order to create larger, connected networks of trust.

Source: Prior GAO work. | GAO-27-108740

Public-key cryptography is essential for maintaining the confidentiality and authenticity of federal systems and data.[13] For example:

- **Confidentiality.** Public-key cryptography is used to encrypt data in transit, such as emails, virtual meetings, and traffic to and from websites. This cryptography provides increased assurance that attackers cannot view sensitive data that is intercepted.
- **Authenticity.** Public-key cryptography is used to help ensure that software, users, and machines are authentic. For example, public-key cryptography is used to authenticate federal websites by issuing them certificates, typically via public-key infrastructure, which can later be verified. (See the sidebar for more information on public-key infrastructure.)

Symmetric and public-key cryptographic methods in use today are nearly impossible for conventional computers to break within the span of a human lifetime. For example, certain public-key cryptography, such as the Rivest-Shamir-Adleman algorithm,[14] relies on the fact that classical computers are very poor at factoring large numbers.[15] As such, it can take a conventional computer trillions of years to factor the large numbers used in cryptography and defeat these methods.

However, CRQCs may be able to considerably speed up the process for breaking some cryptographic methods. Most notably, public-key cryptography is theoretically vulnerable to "Shor's algorithm." In 1994, Peter Shor, a researcher at Bell Labs, introduced an algorithm that could more quickly factor very large numbers if executed on a quantum

[13]Public-key cryptography is also used to ensure that messages, files, or code has not been altered by a malicious actor. Specifically, one party can use a private key to digitally sign information that can be verified with a public key. Any alterations to the information will lead to the public key not verifying the signature.

[14]The Rivest-Shamir-Adleman algorithm is a widely used public-key encryption method for exchanging of sensitive information.

[15]Factoring a number involves finding the unique set of prime numbers that can be multiplied together to produce that number.

computer of sufficient size and sophistication.[16] By contrast, although an algorithm has been developed that can speed up the process for identifying the key used in symmetric key cryptography (Grover's algorithm), experts state that it is extremely unlikely that large quantum computers will lead to a practical way to defeat currently used symmetric key systems.[17]

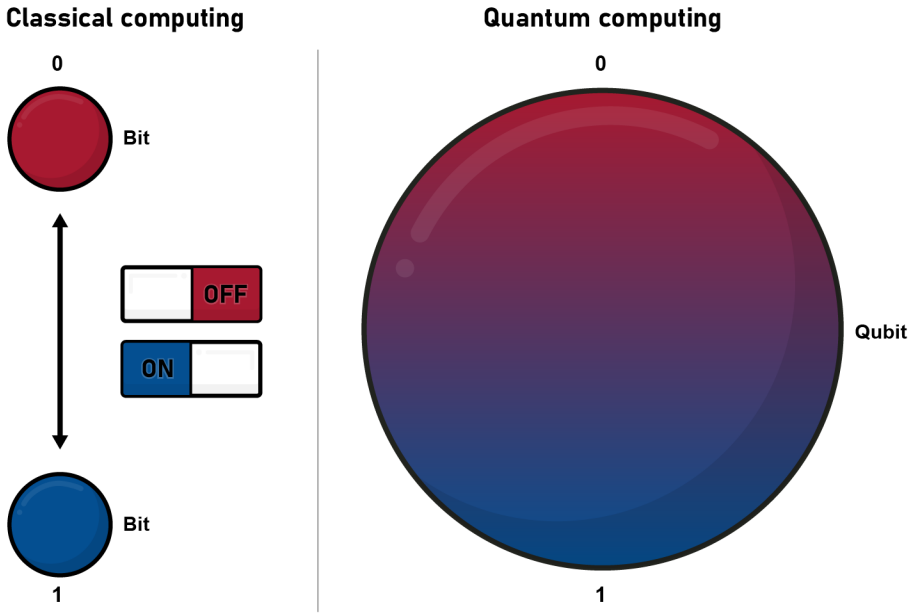
Overview of Quantum Computing

Quantum computers leverage the properties of quantum physics to solve selected problems significantly faster than conventional computers. The building block for a quantum computer is a qubit (the quantum equivalent of a classical computer bit). Classical computers process information through "bits" that can only be 0 or 1. By contrast, a quantum computer processes information through qubits, which can be any combination of 0s and 1s simultaneously (see figure 2).

[16]P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science,* Santa Fe, Nov. 1994: 124-134.

[17]Grover, Lov K., "A fast quantum mechanical algorithm for database search," *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, May 1996 (revised in November 1996): 212-219.

Figure 2: Units for Processing Information Used in Classical Computing Versus Quantum Computing



Sources: GAO analysis; Ka Han/stock.adobe.com (illustrations). | GAO-27-108740

Scientists are working to create quantum technologies, including quantum computers, by creating physical qubits from a variety of systems. However, quantum information is fragile and prone to errors. Quantum error correction techniques attempt to use many error-prone physical qubits working together to create a system that mimics a robust and stable single qubit—known as a logical qubit.

Several foreign nations have made large investments in quantum technologies. One such country is China—a nation-state actor that our intelligence community has consistently highlighted as the top cyber threat to the U.S. government.[18] According to the intelligence community, China seeks to become a world science and technology superpower—including in the area of quantum information science—and to use this technological superiority for economic, political, and military gain. (See

[18]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*.

appendix II for additional details on China's efforts to prioritize quantum information science.)

Federal Roles and Responsibilities for Adopting Cryptography and Supporting Quantum Computing

Various federal laws and policies establish roles and responsibilities that form a framework for the adoption of cryptography to protect agency systems and support quantum computing research. For example, the Federal Information Security Modernization Act of 2014 (FISMA) is intended to provide a comprehensive framework for ensuring the effectiveness of security controls, including cryptography, over technology resources that support federal operations and assets.[19] The act establishes responsibilities for NIST, CISA, OMB, and other federal agencies.

- **NIST.** FISMA assigns responsibility to NIST for developing comprehensive information security standards (e.g., federal cryptographic standards) and guidelines for federal agencies.
- **OMB.** FISMA directs OMB to oversee agencies' information security policies and practices. Among other things, FISMA requires OMB to develop and oversee the implementation of policies, principles, standards (e.g., NIST cryptographic standards), and guidelines on information security in federal agencies, except with regard to national security systems.
- **CISA.** FISMA requires the Department of Homeland Security (DHS), in consultation with OMB, to oversee the implementation of agency information security policies and practices for non-national security information systems (e.g., cryptographic policies and procedures). DHS's CISA is to do this by assisting OMB in carrying out its oversight responsibilities.[20]
- **Federal agencies.** FISMA assigns responsibility to the head of each agency to provide information security protections (e.g., cryptographic protections). These protections are to be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information

[19]The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[20]The Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168, 4169 (Nov. 16, 2018), adding sec. 2202 to the Homeland Security Act of 2002, codified at 6 U.S.C. § 652.

systems used or operated by an agency or on behalf of an agency. FISMA requires agencies to comply with OMB policies and procedures and NIST federal information standards and guidelines.

In addition, other key federal agencies and offices play a critical role in the federal government's efforts to adopt cryptography in support of quantum computing. In particular:

- **Office of the National Cyber Director (ONCD).** In January 2021, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 established ONCD within the Executive Office of the President.[21] The act created the position of the National Cyber Director to head the office and gave the director the responsibility of leading the coordination of implementation of national cyber policy and strategy by
  - monitoring and assessing, in coordination with the heads of relevant federal departments and agencies, the effectiveness of the implementation of national cyber policy and strategy by federal departments and agencies—such as a policy and strategy on cryptography; and
  - reviewing the annual budget proposals for relevant federal departments and agencies and advising their heads on whether those proposals are consistent with national cyber policy and strategy.
- **National Security Agency**. National Security Directive 42 establishes the National Security Agency's leadership role in cryptography.[22] Specifically, the directive designates the Director of the National Security Agency as the National Manager for National Security Telecommunications and Information Systems Security. In fulfilling this responsibility, the agency is to act as the U.S. government's focal point for cryptography.

Additionally, the Office of Science and Technology Policy plays an important role in federal efforts to support research and development for quantum computing. In 2018, Congress passed the National Quantum Initiative Act to establish a government-wide approach to quantum

[21]Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021), codified at 6 U.S.C. § 1500.

[22]The White House, *National Policy for the Security of National Security Telecommunications and Information Systems*, National Security Directive 42 (July 5, 1990).

information science and technology.[23] The act established a 10-year national quantum initiative to invest in quantum workforce development, among other things. The Office of Science and Technology Policy is responsible for overseeing interagency coordination of the initiative.

Quantum Computers Pose Significant Threats to Cryptography on Federal Systems

Threats from a CRQC could have devastating impacts to federal systems reliant on vulnerable cryptography. However, industry experts had varying estimates of when a CRQC will be built.

Threat Actor Use of a Quantum Computer Would Have Devastating Impacts to Federal Systems

Threat actors could use a CRQC to achieve two types of devastating impacts to federal systems that rely on vulnerable cryptography. Specifically, a CRQC could be used to (1) compromise systems that are foundational for authenticating users, machines, and software, or (2) decrypt data that is acquired prior to the development of such a computer.

A Quantum Computer Could Be Used to Compromise Authentication Systems and Sensitive Data

Once a CRQC is available, a threat actor could use several techniques to impact the authenticity of users, machines, and software. For example, a threat actor could

- use a CRQC to derive the private key for the server used to authenticate users from the public key;
- use that private key to create and sign authentication certificates for users with privileged access to a network;
- use that certificate to authenticate as those users; and
- use the privileged access to modify, destroy, or collect sensitive data on the network.

Similar malicious activity has been previously observed. Table 1 identifies several techniques that threat actors with a CRQC could use to compromise systems for ensuring authenticity.

[23]National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092, 5094 (2018), codified at 15 U.S.C. § 8811.

Table 1: Examples of Several Techniques Threat Actors with a Cryptographically Relevant Quantum Computer Could Use to Compromise Systems for Ensuring Authenticity

Threat technique	Definition	Prior examples
Forge code signatures	Code signing is the use of digital signatures to vouch for the authenticity and integrity of software. Adversaries can forge an authorized party's digital signature to sign malicious code.	• In 2015, a networking manufacturer accidentally leaked a private code-signing key. Malicious actors used that key to sign their malware and make it appear to be a legitimate application from the networking manufacturer. • In 2001, a certificate authority issued two Microsoft code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee.
Forge digital certificates	A digital certificate is an electronic credential that can provide the authenticity of a user, device, server, or website. Adversaries may forge certificates used for authentication to access remote systems or resources.	• In 2023, a Chinese threat actor generated digital certificates for accessing Microsoft user accounts after obtaining the private key needed to sign those certificates. The actor then used those certificates to gain access to the Microsoft Exchange Online mailboxes of 22 organizations and over 500 individuals. • In 2011, a threat actor compromised a certificate authority based in the Netherlands—including Dutch Government certificates. The actor issued 531 rogue certificates, including one that the actor may have used to access unencrypted access traffic of more than 300,000 Iranian-based users of Google's Gmail services.

Source: GAO analysis of publicly available information. I GAO-27-108740

Compounding this threat, agencies face challenges in their ability to detect attacks involving a CRQC. For example, using a CRQC to derive a private key from a public key is not an event that can be detected by the victim organization's cybersecurity tools.

Data Could Be Acquired Now to Decrypt Gradually Once a Quantum Computer Is Developed

While a CRQC does not currently exist, threat actors can exploit vulnerabilities to "harvest" or acquire data now that can later be decrypted over time by a CRQC. As shown in table 2 below, there are several methods that threat actors can use to acquire data in transit for this purpose.[24]

[24]Of note, data at rest is generally protected by symmetric cryptography, which is not currently projected to be vulnerable to a CRQC.

Table 2: Examples of Techniques That Threat Actors Could Use Now to Acquire Data to Later Be Decrypted by a Cryptographically Relevant Quantum Computer (CRQC)

Threat technique	Definition	Prior examples
Reroute traffic	Threat actors could potentially exploit vulnerabilities in a key internet routing protocol—the Border Gateway Protocol—to reroute traffic so that it flows through a device owned by the threat actor that stores the traffic until a CRQC is developed.	In June 2024, the Federal Communications Commission highlighted a report by the Departments of Defense and Justice that a Chinese telecommunications company used Border Gateway Protocol vulnerabilities to misroute U.S. internet traffic at least six times.[a]
Supply chain compromise	Threat actors could potentially compromise the technology supply chain by using network devices with malicious functionality that are designed to route traffic to a separate device for storage until a CRQC is developed.	In 2020, the Federal Communications Commission highlighted the presence of hundreds of vulnerabilities and backdoors in software used to operate network devices developed by a Chinese technology corporation.[b]
Eavesdropping on wired or wireless connections	Threat actors with access to physical wire used to transmit federal agency information could potentially compromise those connections with the intention of capturing and storing that information. In addition, threat actors in close physical proximity to radio frequency communications with federal agency information could potentially capture those communications with specialized hardware.	In November 2022, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector stated that if an application for landing a subsea cable in Cuban territory was successful, "the Government of Cuba would be well positioned to collect all U.S. persons' communications and sensitive data traversing [. . .] the cable."[c]

Source: GAO analysis of publicly available data. I GAO 27-108740

[a]Federal Communications Commission, FCC 24-62, Reporting on Border Gateway Protocol Risk Mitigation Process (June 7, 2024). The Federal Communication Commission has proposed a number of steps to improve the security of Border Gateway Protocol routing, including proposing that providers of broadband internet access services create Border Gateway Protocol security risk management plans for that protocol and regularly report key data.

[b]Federal Communications Commission, DA 20-690, Protecting Against National Security Threats to the Communication Supply Chain Through FCC Programs – Huawei Designation (June 30, 2020). The Federal Communication Commission issued a rule that the Universal Service Fund may no longer be used to purchase products or services produced by Huawei. In addition, the Department of Commerce has added more than 100 non-U.S. persons or organizations affiliated with Huawei to the department's Entity List, which restricts the U.S. export, re-export, or transfer of certain items to these entities. In addition, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits executive branch agencies and government contractors from procuring, obtaining, extending, or renewing a contract to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. The act defines "covered telecommunications equipment or services" to include telecommunications equipment produced by Huawei Technologies Company (Huawei), ZTE Corporation, or any of their subsidiaries or affiliates.

[c]Federal Communications Commission, Recommendation of the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector to Deny the Application, File No. SCL-MOD-20210928-00039 (filed Nov. 29, 2022). In addition, according to the Federal Communications Commission, three of the 84 licensed submarine cable systems land in mainland China or Hong Kong, as of October 2024. Further, there are nine cable landing licensees that reported to the Federal Communications Commission that they were directly or indirectly owned by the Chinese government or other entities incorporated by China, according to a November 2024 notice of proposed rulemaking from the Federal Communications Commission.

Once collected, the data would be stored until a CRQC is available. At that time, threat actors will be able to gradually decrypt data that has been collected (e.g., a single key over the course of hours to days)—

potentially causing significant impacts to organizations whose data is impacted.

Although a CRQC by definition would be capable of decrypting stored data,[25] threat actors may face challenges doing so across a large volume of data due to the following three reasons.

- **A CRQC could only decrypt a small amount of information at a time.** In particular, breaking a single public key could take many hours. Estimates for deriving a private key from a public key using a CRQC range from several hours to more than 200 hours—depending on the cryptographic algorithm and key size.[26] In addition, many public-key implementations rotate public and private keys often—further diluting the utility of a single key pair. However, if a threat actor is able to identify a particularly important key, an organization's protected data could be at significant risk.
- **Malicious actors would likely need to guess if stolen data will be valuable in the future.** Because encrypted data is currently unreadable, malicious actors would likely need to guess which stored stolen data would be valuable in the future. The widespread practice of encrypting all data in transit over the internet makes it even more difficult to guess if captured encrypted data is sensitive and should be prioritized for a CRQC.[27] Nevertheless, threat actors could harvest sufficient amounts of data to eventually include instances of highly valuable data.

[25]More precisely, a CRQC recovers private keys. These keys would then likely be used by traditional computers to decrypt stored data. For ease of readability, we are characterizing this two-step process as a CRQC's ability to decrypt data.

[26]See e.g., National Academies, *Quantum Computing: Progress and Prospects* (2019) and RAND, Homeland Security Operational Analysis Center, *Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantum Computer* (April 2023). Of note, estimates for the number of physical qubits required to perform this operation are around 10^7 physical qubits, or 10 million physical qubits.

[27]Of note, collecting large amounts of data (for the purposes of decrypting the data later) may be cost-prohibitive for non-nation-state cyber threat actors. For reference, in 2016, the networking company Cisco reported that daily internet traffic was 710 petabytes (i.e., 760 billion megabytes), and estimated that this traffic would grow to 2.1 exabytes by 2021. In 2023, the scientific research institution CERN told several media outlets that it reached an exabyte of storage—split across 111,000 devices—for its data center. Such data centers are often categorized as "hyperscale" (i.e., significantly larger than traditional data centers located on-premise at an organization). These large data centers can have initial construction costs that range from hundreds of millions to billions of dollars.

- **Energy costs associated with using a CRQC could be high.** In April 2023, the RAND Homeland Security Operational Analysis Center estimated that running a CRQC would consume approximately 1 gigawatt of electrical energy and cost $64,000 to derive a single private key from a public key.[28] In contrast, according to NIST officials, theoretical proposals show that this estimate may be reduced by a factor of 10.[29] NIST officials also explained that continued advancements could further reduce resourcing needs, and thus further reduce the necessary energy and costs. In either case, a threat actor with sufficient infrastructure and support could be able to generate the necessary energy and funds to operate a CRQC at such a scale.

Estimates Vary on When a Cryptographically Relevant Quantum Computer Will Be Developed

Thirty-two industry experts surveyed by the Global Risk Institute as part of its December 2024 report generally believe that a CRQC will eventually be built.[30] Most industry experts said that the probability that a CRQC will be developed by 2040 is greater than 50 percent.[31] However, a small minority of those experts believe that a quantum computer could be built much sooner (see figure 3).

[28]RAND Homeland Security Operational Analysis Center, *Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantum Computer*. For reference, the Department of Energy estimated that a gigawatt of power could be used to light 100 million lightbulbs.

[29]Craig Gidney, "How to factor 2048-bit RSA integers with less than a million noisy qubits," arXiv.org (May 2025), https://arxiv.org/abs/2505.15917. This article is a preprint and has not undergone peer review as of August 2025.

[30]Some experts question whether a CRQC will ever be built. See, e.g., Xavier Waintal, "The quantum house of cards." *Proceedings of the National Academy of Sciences 121*, no.1 (2024).

[31]The survey respondents' statements were based on the likelihood of a CRQC being developed somewhere in the world, such as the United States, the European Union, Japan, or China. Global Risk Institute, *Quantum Threat Timeline Report 2024* (December 2024).

Figure 3: Thirty-Two Quantum Experts' Predicted Timeline for the Development of a Cryptographically Relevant Quantum Computer, as of December 2024

Likelihood Estimate	Within 5 years (2030)	Within 10 years (2035)	Within 15 years (2040)	Within 20 years (2045)	Within 30 years (2055)
Extremely unlikely (<1% chance)	18	4	1	0	0
Very unlikely (<5% chance)	5	11	3	1	1
Unlikely (<30% chance)	6	7	7	2	0
Neither likely or unlikely (50% chance)	2	5	10	10	3
Likely (>70% chance)	1	3	6	8	12
Very likely (>95% chance)	0	2	4	7	10
Extremely likely (>99% chance)	0	0	1	4	6

Source: GAO analysis of Global Risk Institute report. | GAO-27-108740

Other industry literature and officials from one agency with knowledge in this area highlighted several factors contributing to this uncertainty:

- **The rate of growth for physical qubits has not yet been established.** In 1965, the co-founder of Intel Corporation, Gordon Moore, predicted that the number of transistors (i.e., the building blocks of classical computers) would double every 2 years.[32] Semiconductor advancements progressed consistent with "Moore's law" through 2010—with some arguing that industry has maintained

[32]Intel Corporation manufactures semiconductor chips.

this pace, to date. By contrast, there is not a widely accepted "Moore's law" for the rate of advancement in physical qubits.[33]

Instead, companies, agencies, and stakeholders have published quantum technology development roadmaps that describe how development may proceed. For example, one company reported plans to develop a quantum computer with 100,000 qubits by 2033. Another company announced a series of milestones (without associated time frames) that it intends to achieve, with the final being 1,000,000 physical qubits.[34]

- **It is unclear how many physical qubits will be needed for a logical qubit.**[35] As previously mentioned, quantum information is fragile and prone to errors. Quantum error correction techniques attempt to use many error-prone physical qubits working together to create a system that mimics a robust and stable single qubit—a logical qubit. The combination of a more efficient error correction scheme with lower error rates for physical qubits would mean that fewer physical qubits would be needed for a logical qubit.[36] However, industry predictions on advancements in error correction in the coming years are varied, making it difficult to accurately predict the number of physical qubits needed for a logical qubit. [37]
- **It is difficult to determine the validity of industry predictions for CRQC development timelines.** Some companies predict that they will be able to implement quantum computers with thousands of logical qubits in the 2030s. However, officials from one agency told us

[33]Olivier Ezratty, "Is there a Moore's law for quantum computing?", arXiv.org (March 2023), https://arxiv.org/abs/2303.15547.

[34]As discussed in more detail later in this report, it is difficult to determine the validity of industry predictions for CRQC development timelines. Of note, most research publications involving quantum computers describe devices involving about 100 qubits or less.

[35]Current state of the art technology would need thousands of physical qubits for a logical qubit. See, e.g., Gidney and Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum 5*, 433 (2021) and National Academies, *Quantum Computing: Progress and Prospects*.

[36]According to some security researchers, to perform fault-tolerant quantum computation such as the factorization of a 2,000-bit number (such as those used in public-key cryptography), the logical error rate of qubits needs to be reduced to about 10^{-12} per logical operation.

[37]According to industry experts, quantum error correction is an active research area with several error-correction schemes being implemented, such as surface code or Quantum Low-Density Parity-Check codes. Some experts believe Quantum Low-Density Parity-Check codes are promising but it is in early stages and still has challenges.

that these objectives do not contain sufficient supporting detail to determine their feasibility. Officials from that same agency also told us that the concrete value of commercial applications for quantum computing is still being assessed, resulting in uncertainty in long-term funding for research and development in this area.

- **Additional technology may be required for CRQCs to work, including hardware and software that has yet to be developed.** We reported in October 2021 that it would likely take at least a decade and cost billions to develop quantum technologies for more complex uses.[38] These technologies include the following:
  - quantum channels or ways of transporting quantum information from one point to another in a reliable and stable way;
  - quantum memory that can store quantum information without that information degrading or decaying for extended periods of time;
  - improved qubit control equipment that converts (1) signals from a classical computer into signals needed for a quantum computer to operate and (2) qubit measurements from the quantum computer into data;
  - improved cooling systems designed to host superconducting qubits and related electronics;[39] and
  - extensive software, including several layers of software, programming languages, and algorithms.
- **Artificial intelligence could accelerate CRQC timelines**. Officials from one agency told us that artificial intelligence could speed up the development of a CRQC.

[38]GAO-22-104422.

[39]We reported in October 2021 that technologies supporting cooling systems, such as dilution refrigerators that could support large systems, would be needed to meet the goal of a full-scale quantum computer. GAO-22-104422.

Agencies Have Not Fully Implemented Preparatory Practices for Addressing Quantum Cyber Threats

To address the threat posed by a CRQC, it is important that agencies quickly transition existing systems to PQC and identify systems that cannot be migrated to PQC (e.g., legacy technology systems) to inform plans for replacing them.[40] To this end, various documents over the past 9 years have contributed to an emerging U.S. national strategy for addressing the threat of quantum computing to cryptography on unclassified systems.[41] (See appendix III for a summary of the strategy.) One of these documents—OMB's November 2022 guidance—highlights practices for preparing for this transition and their associated activities.[42] We primarily relied on this guidance to develop an evaluation framework of three key practices and eight associated activities (see table 3).[43]

[40]According to OMB's July 2024 *Report on Post-Quantum Cryptography*, a key aspect of the cryptographic inventory process is early identification of systems that may not be able to migrate to PQC. These include legacy systems (1) with cryptographic implementations that cannot be changed or (2) that lack the processing speed, memory, or bandwidth necessary to implement PQC. According to OMB's report, replacing hardware, software, and digital systems that are not PQC-compatible will likely be a time- and resource-intensive process. See Office of Management and Budget, *Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260* (July 2024).

[41]In November 2024, we reported that the strategy partially addressed the desirable characteristics of a national strategy. GAO, *Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy*, GAO-25-107703 (Washington, D.C.: Nov. 21, 2024). Accordingly, we recommended that the Office of the National Cyber Director take the lead in coordinating the strategy and ensuring that it fully addresses the desired characteristics of a national strategy. ONCD did not agree or disagree with our recommendation and, as of March 2025, has not yet addressed it.

[42]Office of Management and Budget, *Migrating to Post Quantum Cryptography*, M-23-02.

[43]We also supplemented OMB's guidance with several components from our prior work on transition planning. See GAO-20-155.

Table 3: GAO Evaluation Framework of Post-Quantum Cryptography (PQC) Transition Preparatory Practices and Associated Activities

Transition preparatory practice	Transition preparation activity
1. Develop and annually update a prioritized inventory of agency systems with vulnerable cryptography.	a. Identify a complete inventory of priority non-national security systems[a] that reflects high-value assets,[b] high impact systems,[c] systems that contain data expected to remain mission-sensitive in 2035,[d] and any systems that are logical access control systems based on public-key cryptography.[e]
	b. Ensure that the inventory completely describes vulnerable cryptographic algorithms for priority systems.
	c. Ensure that the inventory completely describes other system characteristics, including the type of software package (e.g., commercial-off-the-shelf, government-off-the-shelf, custom developed software), operating system, and type of organization that hosts the system (e.g., agency or cloud hosting) for priority systems.
	d. Ensure that the inventory accurately describes vulnerable cryptographic algorithms for priority systems.
	e. Ensure that the inventory accurately describes other system characteristics, including the type of software package, system provider (e.g., the agency, cloud provider), operating system, and how long system data needs protection for priority systems.
2. Identify and annually update the funding needed to transition vulnerable cryptography on priority systems to PQC.	a. Include the funding needed for all vulnerable systems identified in the inventory and ensure its accuracy.
3. Test PQC in agency environments to help ensure that the algorithms will work in practice.	a. Work with software vendors to identify candidate environments, hardware, and software (e.g., web browsers, cloud service providers, endpoints) for the testing of PQC.
	b. Test PQC in agency environments.

Source: GAO analysis of Office of Management and Budget (OMB) guidance and GAO-20-155. I GAO 27-108740

[a]As defined in the Federal Information Security Modernization Act of 2014, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3542(b)(2). For the purposes of this report, systems that do not meet the criteria for national security systems are referred to as non-national security systems.

[b]A high-value asset is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission, or is considered essential to an agency's security and resilience.

[c]High-impact systems are those in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of "high." According to National Institute of Standards and Technology standards, agencies are to identify a security objective as "high" when the loss of that objective would be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals (e.g., unable to perform one or more of its primary functions).

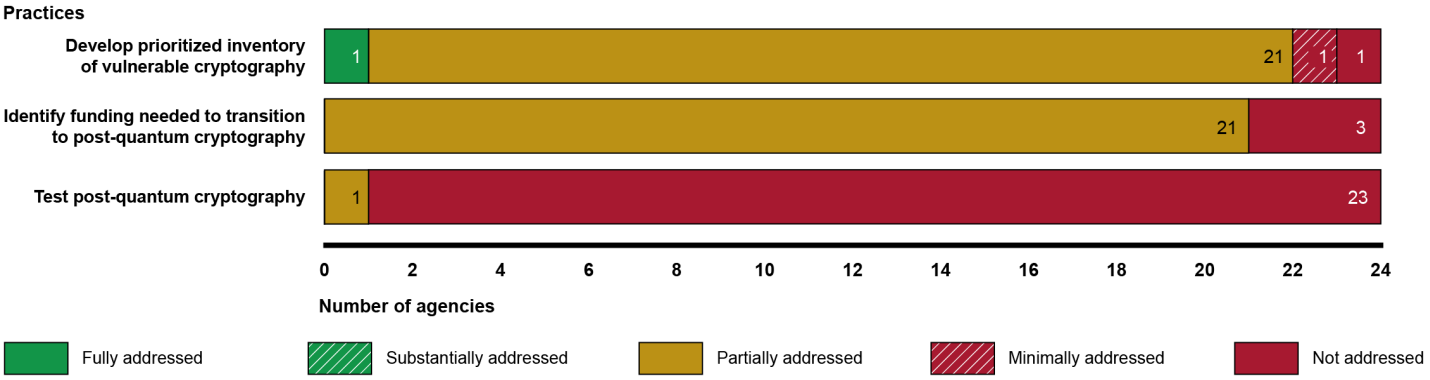
[d]According to OMB guidance M-23-02, this criterion refers to data that would still be considered mission-sensitive if decrypted by a cryptographically relevant quantum computer in 2035.

[e]A logical access control system controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database. These systems require validation of an individual's identity through some mechanism, such as a personal identification number, card, biometrics, or other token. In addition, these access control systems have the

capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

None of the 24 selected agencies fully addressed these three key practices (see figure 4). A more detailed evaluation of each practice follows the figure.

Figure 4: Extent to Which the 24 Chief Financial Officers Act Agencies Addressed Preparatory Practices for Migrating to Quantum Computing



Source: GAO analysis of agency information. | GAO-27-108740

Agencies Have Not Fully Developed Prioritized Inventories of Systems with Vulnerable Cryptography

Only one of the 24 agencies fully addressed all applicable activities for developing prioritized inventories of systems with vulnerable cryptography. Most of the 24 agencies partially addressed the first three applicable activities, and six agencies that were selected for further analysis either partially addressed or did not address the remaining two activities.

- **Complete inventory of priority systems.** One of the 24 agencies fully addressed the preparatory activity. In contrast, one agency did not develop an inventory and the remaining 22 agencies partially addressed the activity because they did not fully account for all priority systems in their inventories. Specifically:
  - A majority of the agencies' inventories did not identify all high-impact systems.
  - Most of the agencies' inventories did not identify all high-value assets.
  - A majority of the agencies' inventories did not include or consider additional vulnerable cryptographic systems that (1) contain data

expected to remain mission-sensitive in 2035 or (2) provide access control based on public-key infrastructure.

- **Complete inventory of vulnerable cryptographic algorithms.** One agency fully addressed this activity by identifying one or more vulnerable cryptographic algorithms for the systems identified in its inventory. However, one agency did not complete an inventory of priority systems and their vulnerable cryptographic algorithms and the 22 remaining agencies partially completed such inventories. In particular:
  - Several of the agencies' inventories did not include vulnerable algorithms for one or more priority systems.
  - Several of the agencies' inventories incorrectly included "symmetric key" cryptographic algorithms as being vulnerable to a CRQC for one or more priority systems. [44]
  - Several of the 22 agencies included information on the vulnerable cryptographic algorithms, but their inventories did not include all priority systems, as previously discussed. As such, they did not have a complete inventory of all vulnerable cryptographic algorithms.
- **Complete descriptions of key system characteristics.** One agency fully addressed this activity by identifying key system characteristics for each of the systems identified in its inventory. By contrast, one agency did not complete an inventory and 22 agencies' inventories partially addressed this activity because their inventories included system characteristic descriptions for some, but not all, systems. In particular:
  - Several of the 22 agencies' inventories had missing data for the type of software package (e.g., commercial-off-the-shelf, government-off-the-shelf, custom developed software).
  - Several agencies included information on key system characteristics; however, their inventories did not include all priority systems, as previously discussed. As such, they did not have a complete inventory of all key system characteristics.

[44]As previously mentioned, symmetric key cryptography uses the same key to encrypt and decrypt data and is used to ensure that communications and data at rest stay private. In addition, this cryptography is not currently projected to be vulnerable to quantum computers.

- Several agencies' inventories had missing data for the type of operating system used (i.e., software that supports a computer's basic functions).
- Several agencies' inventories had missing data for the type of organization that hosts the system (e.g., the agency's cloud provider).

- **Accurate inventory of vulnerable cryptographic algorithms.** None of the six agencies we selected for further review fully addressed this activity. Two agencies partially addressed it by providing documentation that supported the source of the algorithms for some, but not all, of the selected systems. The remaining four agencies did not address this activity. Three of those four agencies did not provide documentation that supported the vulnerable cryptographic algorithms used for the selected systems. The other agency did not provide an inventory or supporting documentation.
- **Accurate descriptions of key system characteristics.** None of the six selected agencies fully addressed this activity. Four agencies partially addressed it by providing documentation supporting their respective inventories' descriptions of key system characteristics for some, but not all, selected systems. Specifically:
  - One of the four agencies provided documentation that supported the names of the software packages used for all selected systems. Two agencies provided documentation that supported the names of the software packages used for some, but not all, selected systems. The remaining agency provided documentation that did not support the software packages used for any of the selected systems.
  - Three of the four agencies provided documentation that supported the type of operating system used by some, but not all, of the selected systems.[45] The remaining agency provided documentation that did not support the operating systems used for any of the selected systems.
  - Two of the four agencies provided documentation that supported the type of organization that hosts the system (e.g., the agency's cloud provider) for all selected systems. The remaining two agencies provided documentation that supported the type of hosting organization for some, but not all selected systems.

[45]As previously mentioned, an operating system is software that supports a computer's basic functions.

- The remaining two agencies did not address this activity. One agency did not provide any supporting documentation and the other did not provide an inventory or supporting documentation.

Several Factors Contributed to Incomplete Implementation of Inventory Activities

The incomplete implementation of the inventory activities was due, in part, to a lack of (1) cryptography expertise, (2) documented inventory maintenance processes, (3) automated tools, and (4) a plan for addressing the challenge of developing an inventory for one agency's complex environment. Specifically:

- **Lack of cryptography expertise.** We have previously reported on the importance of ensuring that personnel with the right skills are in place to support technology transition efforts.[46] Having staff with these skills positions agencies to effectively prepare for technology transitions and avoid adverse effects—such as lengthy delays. Where agencies have identified gaps, our prior reports have highlighted the importance of developing and implementing plans to fill them.[47]

  Six agencies took steps to educate and train their workforce on cryptography. For example, two of those six agencies conducted internal training to provide an overview of PQC transition requirements to relevant employees. However, the remaining 18 agencies reported a lack of expertise in cryptography and developing related inventories.[48] In addition, those agencies have not developed plans to fill those gaps.[49]

- **Lack of documented inventory maintenance processes.** We have previously highlighted the importance of having a documented process for developing and maintaining an inventory of technology assets in our prior work on major transitions.[50] Such processes can position agencies to consistently and accurately incorporate

[46]GAO-20-155.

[47]See, e.g., GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129 (Washington, D.C.: Oct. 30, 2019) and *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[48]ONCD officials emphasized that agencies face shortfalls and difficulties in hiring skilled cybersecurity professionals, including those with cryptography expertise.

[49]These agencies cited several reasons for not developing plans to address the lack of workforce cryptography expertise, including the high cost of training and resource limitations.

[50]GAO-20-155.

information relating to technology used across the organizations and any changes made during and after the transition into their inventories. One agency established an inventory maintenance process that included a detailed process for collecting inventory information and various roles and responsibilities for maintaining that information. However, the other 23 agencies did not document an inventory maintenance process.[51]

- **Lack of automated tools.** CISA, NIST, and the National Security Agency recommend that organizations use automated tools to help develop inventories of systems with vulnerable cryptography.[52] These tools can be used to find vulnerable cryptographic methods across the organization's technology assets—including network protocols, end user systems, servers, and applications and their associated libraries.[53] Five agencies used automated tools to identify and verify data in their inventories. However, the other 19 agencies did not use any such tools.[54]

  Officials from 15 agencies stated that it was too early in the migration process to use automated tools or that they were waiting for CISA to identify appropriate tools.[55] According to CISA officials, the agency started working with NIST's National Cybersecurity Center of Excellence in 2024 to develop use cases that aided in identifying

[51]These agencies cited several reasons for not documenting an inventory maintenance process, including the need to first establish accurate inventories prior to developing maintenance processes and various cost and resource constraints. For example, officials from one agency stated that they had to prioritize the department's limited resources and developed an ad-hoc inventory maintenance process in lieu of dedicated inventory and planning processes for PQC.

[52]CISA, NIST, and the National Security Agency. *Quantum-Readiness: Migration to Post-Quantum Cryptography* (Aug. 21, 2023).

[53]ONCD officials noted that automated tools can assist with creating a cryptography inventory but cannot be relied on to fully complete one.

[54]ONCD officials added that automated tools were never a requirement in policy for agencies to utilize, but rather an option to assist agencies in conducting an inventory.

[55]For example, officials at one agency stated that the agency was anticipating using a CISA-provided tool and therefore has not acted on establishing automated tools. However, according to CISA officials, the agency has not communicated to departments and agencies that they should wait for CISA to provide tools. Those officials added that they have communicated that the agency was exploring automation and the feasibility of integrating tools into the Continuous Diagnostics and Mitigation program as part of its automated inventory strategy.

capabilities of vendor-automated cryptographic discovery tools.[56] CISA officials added that the intent of their work is to identify tools that can be used to allow agencies to move from manual to automated processes for developing and maintaining their cryptographic inventories.

According to CISA, the agency anticipates releasing its assessment of tools for agencies to consider by December 2025. If CISA follows through on its plans to test vendor-automated cryptography discovery tools and release a report with its results, agencies will be better positioned to select tools that meet their needs for automating their cryptographic inventory development processes.

- **Lack of a plan for addressing the challenge of developing an inventory for one agency's complex environment.** According to agency officials, this department did not address activities related to developing an inventory due to the complexities of compiling one across such a large organization. For example, those officials explained that the department's unclassified systems support more than 4 million endpoints (i.e., physical or virtual devices that connect to a network), and it is very challenging to identify the cryptography embedded in the applications used by these devices.

  Our prior work has shown that plans—such as operational plans—can provide a roadmap for addressing identified challenges—including those with significant scope and complexity.[57] In addition, we have reported that such plans can better position an agency to work collaboratively and strategically with external partners—such as technology vendors that support the department's millions of devices.[58] However, one agency has not developed a plan to address

[56]Established in 2012, the National Cybersecurity Center of Excellence works with technology industry partners to develop cybersecurity solutions that demonstrate how to apply standards and best practices using commercially available technology.

[57]See, e.g., GAO, *Chemical Terrorism: A Strategy and Implementation Plan Would Help DHS Better Manage Fragmented Chemical Defense Programs and Activities*, GAO-18-562 (Washington, D.C.: Aug. 22, 2018); *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*, GAO-17-300 (Washington, D.C.: Apr. 6, 2017); *Managing for Results: Practices for Effective Agency Strategic Reviews*, GAO-15-602 (Washington, D.C.: July 29, 2015); *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation*, GAO-05-372 (Washington, D.C.: Sept. 8, 2005); and *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[58]See, e.g., GAO-18-562, GAO-17-300, GAO-15-602, GAO-05-372, and GAO-04-408T.

the challenge of developing an inventory of agency systems with vulnerable cryptography across its large and complex environment.[59]

Representatives from OMB and ONCD acknowledged the weaknesses in agencies' inventories and described efforts planned and underway to help address them. For example:

- OMB officials stated they held technical assistance meetings with some agencies to help address missing items and data errors. In addition, they told us that they intend to develop future guidance to help address the weaknesses we identified.
- ONCD officials explained that they assisted agencies with guidance on establishing such a baseline inventory, including through working groups, office hours sessions, and responses to questions. Those officials noted that the inventory effort was designed to be an iterative, annual process, building on the previous year's submissions to provide better, increasing granularity as this process matures over several years.

Nevertheless, there is an urgent need for agencies to address the inventory weaknesses in light of the risk to systems that may be targeted for "harvest now, decrypt later." As previously mentioned, threat actors could harvest critical information now that is not yet protected by PQC and decrypt it once a CRQC is built. Accordingly, it is important for agencies to expeditiously identify priority systems for transitioning to PQC, including those that contain data expected to remain mission-sensitive in 2035.

As such, agencies cannot wait to mature their inventory development processes and for OMB to develop and finalize guidance related to the inventory weaknesses we identified. Until CISA completes its test of vendor-automated cryptography discovery tools and agencies take steps to address the lack of expertise and processes, agencies will likely

[59]According to agency officials, the agency is taking a measured and thoughtful approach to inventorying given the breadth of the agency's systems. Those officials added that they expect to describe their plans for developing an inventory in a soon to be released PQC strategy document.

continue to struggle to develop complete and accurate inventories.[60] In turn, they will not be well-positioned to establish and implement plans for migrating existing systems to PQC and replacing legacy systems that cannot support PQC. Further, without a plan for addressing the challenge of developing an inventory for one agency's environment, that agency will not be optimally positioned to prioritize its numerous and complex systems for migration to PQC.

Agencies Have Not Fully Identified Funding Needed to Transition to Post-Quantum Cryptography

None of the 24 agencies fully addressed the one activity under the preparatory practice to identify the funding needed to transition vulnerable cryptography on priority systems to PQC. Specifically, 21 agencies partially included the funding needed for all vulnerable systems and ensured that the assessment was accurate. Although these agencies developed funding assessments, only one agency developed an assessment that was based on a complete inventory of priority systems, as previously discussed.

In addition, each of these 21 agencies acknowledged that the data were not fully accurate. For example:

- Officials from one agency explained that the funding assessment was not reliable as technology products with PQC do not currently exist.
- Officials from another agency stated that funding assessment reliability cannot be determined without vendor-provided price quotes, standard measures, reliable tools, and a trained workforce.

The other three agencies did not develop funding assessments.

Several Factors Contributed to Incomplete Adoption of Funding Assessments

The incomplete adoption of this activity is due in part to (1) incomplete and inaccurate inventories, (2) a lack of documented funding assessment processes, and (3) a lack of vendor cost data. Specifically:

- **Incomplete and inaccurate inventories.** As previously stated, most agencies are challenged in developing complete and accurate system inventories. This hinders their ability to determine which vulnerable

[60]As previously discussed, CISA officials highlighted that the agency has been clear in its communication to departments and agencies that conducting manual inventories is a necessary part of the migration process. Officials added that automated tools will help provide visibility into the things missed during the manual process and help move agencies toward crypto agility and continuous monitoring in the future. As a result, CISA officials emphasized that agencies should continue to focus on identifying sensitive data and systems, understanding their environments and architectures, and improving the process for collecting and reporting inventories.

systems and algorithms need to be replaced, and the cost (including hardware and software costs) associated with the replacement.

- **Lack of documented funding assessment processes.** Only one of the 24 agencies documented processes for assessing the funding needed to migrate to PQC. Fourteen agencies stated that it was too early to document funding assessments—particularly given that NIST recently finalized standards for PQC. However, we have previously highlighted the importance of having a documented process in our prior work on major transitions before they occur.[61] Specifically, early documented processes related to funding assessments can help reduce the risk of unexpected costs that can occur during major transitions, including the migration to PQC.
- **Lack of vendor cost data.** Eleven agencies reported that it was difficult to develop a funding assessment when no vendors had technology products with PQC and therefore did not have estimated costs as the basis of a funding assessment. ONCD representatives added that the lack of vendor cost data is the biggest factor preventing agencies from completing a reliable funding assessment. Those same representatives stated that accurate cost data is still not available due to the lack of commercially available products.[62]

  Nevertheless, agencies were directed to complete their funding assessments in June 2024. NIST finalized the core set of PQC standards in August 2024 and encouraged cybersecurity experts (including technology vendors) to start incorporating these standards into their systems and products. As more commercially available products with PQC become available, vendors will be positioned to provide agencies with more accurate cost data.

  ONCD officials added that OMB is expected to issue a policy memorandum around Summer 2025 instructing federal agencies to develop a plan to upgrade their non-national security systems to PQC. OMB and ONCD will then begin working with each federal agency on cost estimates. With the release of the NIST PQC standards, forthcoming OMB policy memorandum, and better vendor cost estimates, agencies should be better situated to develop complete and accurate funding assessments.

[61]GAO-20-155. According to ONCD officials, OMB will publish PQC migration guidance later this year. Those officials added that departments and agencies will be able to use this guidance to begin developing PQC migration strategies.

[62]Those representatives also noted that agency cost estimates are a multi-year exercise.

OMB and ONCD representatives acknowledged the weaknesses in agency funding assessments but said that they were reliable for the purposes for which they have been used. More specifically:

- OMB representatives explained that the funding assessments were used to provide congressional committees with a rough order of magnitude estimate of the governmentwide cost to migrate prioritized systems to PQC.[63]
- ONCD officials stated that agency funding assessments were not intended to provide funding or budget information; rather, they were to provide senior decision-makers with rough cost estimates for the migration to PQC. Further, the officials added that accurate cost information was not yet expected because vendors were in the early stages of incorporating the recently finalized algorithms into their products.[64] In addition, commercially available products utilizing the new PQC NIST encryption standards were not available in the marketplace. As such, agencies were instructed to look at historical program baseline costs and project those costs forward, as best they could, to establish a rough-order cost baseline. However, officials added that estimates will be further refined once PQC products are publicly available on the marketplace and accurate cost estimates can be established.

Nevertheless, agencies are not well-positioned to rectify these weaknesses for future cost estimates. Without establishing and implementing documented processes for assessing the funding needed to migrate to PQC, agencies will be unable to prepare complete and accurate assessments and risk experiencing unexpected migration costs.

Agencies Have Not Tested Post-Quantum Cryptography

As previously stated, OMB guidance recommends that agencies (1) work with software vendors to identify candidate environments, hardware, and software (e.g., web browsers, cloud service providers, and endpoints) for the testing of PQC, and (2) test PQC in agency environments. Such testing can position organizations to identify certain systems (e.g., legacy

[63]OMB used these funding assessments to provide congressional committees with an ONCD-developed estimate that the total governmentwide cost required to migrate priority systems to PQC or replace legacy systems that cannot support PQC was approximately $7.1 billion. See Office of Management and Budget, *Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act*. OMB's report noted that a significant portion of the overall estimate reflects legacy systems that cannot support PQC.

[64]ONCD officials added that historical program data was intended to help form the basis of the assessments.

systems and custom software) that may not support PQC to inform plans for replacing them.

However, only one out of 24 agencies fully addressed one of the two activities. Specifically, the one agency conducted market research to identify candidate vendor implementations of PQC in software to be tested in the department's environment. However, the one agency did not test PQC in its environment. In addition, the remaining 23 agencies did not address either of the activities.

Agency officials and ONCD officials acknowledged that agencies had not yet worked with software vendors to identify candidate environments for PQC testing or tested PQC in their environments. These officials gave various reasons for why these activities had not occurred. Specifically:

- 16 agencies stated that it was too early to identify testing candidates and test PQC in their environments because technology vendors were still in the early stages of incorporating the algorithms into their products.
- ONCD officials stated that evaluating and testing PQC standards were not requirements for individual agencies, since most are not resourced for this. According to ONCD officials, testing is a voluntary activity, as mission and resources allow, to further assist NIST with the evaluation of these standards.[65] In addition, ONCD officials added that, at the time GAO conducted its interviews in 2024, NIST had not yet published its PQC standards.[66]

However, OMB guidance encouraging agencies to test PQC was released in November 2022, before NIST finalized the PQC standards. In addition, the guidance highlights the importance of testing the technology in agency environments before commercial implementations are finalized, even though this testing would not be validated to the same extent as a full commercial solution. Such testing in agency environments has been practical for several years without the use of any commercial applications.

[65]Specifically, according to ONCD officials, OMB-M-23-02 encouraged but did not require federal agencies to test PQC because of a lack of agency cryptographic expertise or resources to conduct such testing. However, according to ONCD officials, the office and OMB have encouraged agencies that have expressed an interest in testing to work with NIST's National Cybersecurity Center of Excellence, and several have done so. This has helped to ensure testing is controlled, centralized, and standardized, and has helped NIST with the publication of its PQC standards in August 2024.

[66]ONCD officials also noted that published tools and resources were not released in time for agencies to consider in planning for PQC migration to NIST-approved standards.

For example, open-source tools have been available for at least 4 years to help organizations begin researching and prototyping PQC.[67] Thus, open-source tools would be sufficient to begin testing before a fully validated implementation is available. [68]

Further, OMB's guidance does not indicate that PQC testing is to be a voluntary activity.[69] As previously mentioned, our prior work has shown that plans—such as operational plans—can better position an agency to work collaboratively and strategically with external partners, such as technology vendors that support federal agencies.[70] However, agencies have not developed plans for testing PQC, including identifying where in agency networks such testing should occur. Until agencies develop and implement such plans, they will not be well-positioned to identify and quickly replace certain systems (e.g., legacy systems and custom software) that may not support PQC.

Conclusions

Although experts say that the probability that a CRQC will be built in the next 10 years is low, the impact of such a computer on unprepared federal systems could be catastrophic to the nation's economy and security. There is also a risk that threat actors could harvest large amounts of data now and decrypt it later once a CRQC becomes available. The loss of even a small amount of important sensitive information could have a severe effect on federal operations.

[67]For example, the Open Quantum Safe project offers an open-source library of quantum-resistant cryptographic algorithms and prototype integrations of PQC into widely used protocols and applications. https://openquantumsafe.org/.

[68]ONCD officials noted that, while the office recognizes the value of open-source libraries and their contribution to the digital ecosystem, these libraries alone are insufficient for advancing the transition to PQC in government systems due to critical limitations (e.g., they do not provide compliance tracking, are often research-grade, and are without external audits). Officials added that federal agency use of code libraries requires controlled implementation, rigorous validation, lifecycle governance, and security oversight that open-source projects alone cannot fulfill.

[69]OMB did not respond to our requests for comments on our preliminary results. ONCD stated that, although agencies are encouraged to test PQC algorithms, testing is not an explicit policy requirement for agencies. Those officials added that the OMB guidance recognizes that most agencies do not have the cryptographic expertise or resources to conduct such testing. The officials noted that this is why only CISA was specifically tasked in the guidance to work with vendors to identify candidate hardware and software for testing PQC algorithms. ONCD officials also noted that their office and OMB have encouraged agencies that have expressed an interest in testing to work with NIST, and that several agencies have done so.

[70]See, e.g., GAO-18-562, GAO-17-300, GAO-15-602, GAO-05-372, and GAO-04-408T.

Federal agencies recognize the quantum computing threat and have taken some actions to partially address it. However, agencies have not fully carried out initial steps to prepare for this threat. Agencies' lack of (1) plans for obtaining needed cryptography expertise, (2) processes for developing inventories and funding assessments, and (3) plans to guide PQC testing increase the risk that their transitions to quantum-resistant cryptography will occur too late. Until agencies develop and implement plans and processes to ensure that the federal government expeditiously transitions priority systems to PQC, data currently protected by cryptography will be at risk of exposure.

Recommendations for Executive Action

In the sensitive report that we issued in September 2025, we made 89 recommendations to CISA and 23 of the 24 CFO Act agencies to, among other things, establish and implement processes to develop inventories of vulnerable cryptography and identify funding for post-quantum cryptography.[71]

Agency Comments and Our Evaluation

We provided a draft of (1) the sensitive report and (2) this report to 29 agencies—the National Security Agency, the Office of the Director of National Intelligence, OMB, ONCD, the Office of Science and Technology Policy, and the 24 CFO Act agencies—for review and comment.

Sensitive report. All agencies, with the exception of OMB and the Department of Interior, provided responses to our sensitive report. Further, of the 23 agencies we made recommendations to in our sensitive report,

- 12 agencies agreed with our recommendations;
- two agencies partially agreed with our recommendations;
- one agency disagreed with three of the four recommendations and agreed with the remaining one;
- seven agencies neither agreed nor disagreed with our recommendations; and
- one agency—the Department of the Interior—did not provide a response.

We continue to believe that all of the recommendations made in the sensitive report are warranted. We have omitted the original agency comment letters reprinted in the sensitive report due to sensitivity

[71]GAO-25-107392SU.

concerns. We also received technical comments from multiple agencies, which we incorporated into the report, as appropriate.

This report. All agencies, with the exception of the U.S. Agency for International Development, provided a response on this public version of our report. The bullets below describe the comments we received from the 28 agencies.

- Two agencies—the Department of Homeland Security and the Social Security Administration—provided comments on steps planned or underway to prepare for the threat of a CRQC.
  - In written comments, reprinted in Appendix IV, the Department of Homeland Security reiterated its response to the recommendations we made in our sensitive report and noted that it remained committed to ensuring that its systems and networks implement and maintain quantum readiness.
  - In written comments, reprinted in Appendix V, the Social Security Administration agreed with the recommendations and noted that it had updated its process to collect cryptographic information. It also noted that it would develop transition plans once PQC-resistant algorithms become available.
- Five agencies—the Environmental Protection Agency, the Department of Energy, the Office of the Director on National Intelligence, the Office of the National Cyber Director, and the Office of Science and Technology Policy—provided technical comments on this public version of the report, which we have incorporated as appropriate.
- The remaining 21 agencies stated that they did not have comments on this public version of the report.

We are sending copies of this report to the appropriate congressional committees, the heads of the 24 CFO Act agencies, the Director of CISA, the Director of National Intelligence, the Director of OMB, the Director of the Office of Science and Technology Policy, the National Cyber Director, the National Security Agency and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Marisol Cruz Cain or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

Sincerely,

//SIGNED//

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the threats cryptanalytically relevant quantum computers (CRQC) pose to cryptography on federal agencies systems; and (2) evaluate the extent to which federal agencies have begun planning for post-quantum cryptography (PQC) migration consistent with federal guidance.

This report presents a public version of a sensitive report that we issued in September 2025.[1] Ten agencies in our review determined certain information in our September report to be sensitive, which must be protected from public disclosure. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To address the first objective, we conducted a literature search for information on both quantum computing and the development of CRQCs in the U.S. and internationally, including publicly available information on when a CRQC may be built and the impacts of such a computer. We reviewed the literature to assess the quality of information, then summarized the relevant public reports, threat assessments, and other related documentation.

Additionally, we interviewed knowledgeable officials and summarized documentation from federal agencies with responsibilities for (1) identifying and assessing cyber threats to federal agency systems—including threats posed by a CRQC, and/or (2) promoting quantum computing research and development. Those federal agencies are the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), the National Security Agency, the Office of the Director of National Intelligence, and the Office of Science and Technology Policy.

To address the second objective, we assessed 24 Chief Financial Officers Act (CFO Act) agencies' preparation efforts against an evaluation

[1]GAO, *Future of Cybersecurity: Federal Actions Needed to Prepare for Quantum Computing Threat*, GAO-25-107392SU (Washington, D.C.: Sept. 11, 2025).

framework.[2] To compile the framework, we primarily reviewed relevant Office of Management and Budget (OMB) guidance.[3] We also reviewed our prior work on IT system transition planning.[4] We then summarized this guidance and prior work into three practices and eight associated activities. Those practices and associated activities are shown in table 4 below.

[2]The 24 CFO Act agencies are the Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration; the Social Security Administration; and the U.S. Agency for International Development.

[3]Office of Management and Budget, *Migrating to Post-Quantum Cryptography*, M-23-02 (Washington, D.C.: Nov. 18, 2022).

[4]GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays*, GAO-20-155 (Washington, D.C.: Apr. 7, 2020).

Table 4: GAO Evaluation Framework of Post-Quantum Cryptography (PQC) Transition Preparatory Practices and Associated Activities

Transition preparatory practice	Transition preparation activity
1. Develop and annually update a prioritized inventory of agency systems with vulnerable cryptography.	a. Identify a complete inventory of priority non-national security systems[a] that reflects high-value assets,[b] high impact systems,[c] systems that contain data expected to remain mission-sensitive in 2035,[d] and any systems that are logical access control systems based on public-key cryptography.[e]
	b. Ensure that the inventory completely describes vulnerable cryptographic algorithms for priority systems.
	c. Ensure that the inventory completely describes other system characteristics, including the type of software package (e.g., commercial-off-the-shelf, government-off-the-shelf, custom developed software), operating system, and type of organization that hosts the system (e.g., agency or cloud hosting) for priority systems.
	d. Ensure that the inventory accurately describes vulnerable cryptographic algorithms for priority systems.
	e. Ensure that the inventory accurately describes other system characteristics, including the type of software package, system provider (e.g., the agency, cloud provider), operating system, and how long system data needs protection for priority systems.
2. Identify and annually update the funding needed to transition vulnerable cryptography on priority systems to PQC.	a. Include the funding needed for all vulnerable systems identified in the inventory and ensure its accuracy.
3. Test PQC in agency environments to help ensure that the algorithms will work in practice.	a. Work with software vendors to identify candidate environments, hardware, and software (e.g., web browsers, cloud service providers, endpoints) for the testing of PQC.
	b. Test PQC in agency environments.

Source: GAO analysis of Office of Management and Budget (OMB) guidance and GAO-20-155. I GAO 27-108740

[a]As defined in the Federal Information Security Modernization Act of 2014, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3542(b)(2). For the purposes of this report, systems that do not meet the criteria for national security systems are referred to as non-national security systems.

[b]A high-value asset is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission or is considered essential to an agency's security and resilience.

[c]High-impact systems are those in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of "high". According to National Institute of Standards and Technology standards, agencies are to identify a security objective as "high" when the loss of that objective would be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals (e.g., unable to perform one or more of its primary functions).

[d]According to OMB guidance M-23-02, this criterion refers to data that would still be considered mission-sensitive if decrypted by a cryptanalytically relevant quantum computer in 2035.

[e]A logical access control system controls an individual's ability to access one or more computer system resources, such as a workstation, network, application, or database. These systems require validation of an individual's identity through some mechanism, such as a personal identification number, card, biometrics, or other token. In addition, these access control systems have the

capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

We then evaluated the 24 CFO Act agencies' efforts to address these three preparatory practices and the associated activities:

- **Develop and annually update a prioritized inventory of agency systems with vulnerable cryptography.** To assess this practice, we collected and analyzed agency inventories and interviewed or collected written responses from knowledgeable officials regarding missing data and controls used to develop and maintain the inventories. We describe the steps we took to assess each activity in more detail below.
  - To assess the activity of *identifying a complete inventory of non-national security systems*, we reviewed agency reports on metrics associated with their cybersecurity programs, including the number of high impact systems and high-value assets. We then compared the high impact systems and high-value assets in these metrics reports to the systems and assets identified in agencies' inventories of vulnerable cryptography.
  - To assess the activity of *ensuring that the inventory completely describes vulnerable cryptographic algorithms for priority systems*, we electronically tested the inventories for missing data in the data element associated with vulnerable cryptographic algorithms. In addition, we manually reviewed the data for obvious errors—namely, the inclusion of symmetric algorithms.[5]
  - To assess the activity of *ensuring that the inventory completely describes other system characteristics*, we electronically tested the agency inventories to identify missing values in key data elements, including vulnerable cryptographic algorithms used, operating systems, and system hosting information for each priority system identified in the inventories.
  - To assess the activity of ensuring *that the inventory accurately describes vulnerable cryptographic algorithms*, we selected 15 systems for further review at six agencies. To select the agencies, we divided the fiscal year 2023 IT budgets of the 24 CFO Act

[5]As previously mentioned, although an algorithm has been developed that can speed up the process for identifying the key used in symmetric key cryptography (Grover's algorithm), current projection suggestions are that large quantum computers will not be able to complete the algorithm in a similar time frame. As such, OMB's guidance for developing the inventories called for agencies to only highlight public-key algorithms as being vulnerable to a CRQC.

agencies into three strata: (1) the eight agencies with the largest budgets, (2) the next eight agencies with moderate sized budgets, and (3) the last eight agencies with the smallest budgets.[6] We then randomly selected six agencies for review—two from each stratum.

We then randomly selected three systems[7] from five of the six selected agencies' prioritized inventories.[8] For each system, we asked knowledgeable agency officials to provide us with documentation that identified the vulnerable algorithms used by those systems (e.g., reports from automated tools used to identify cryptography). We then compared that documentation to the algorithms identified in the agencies' inventory submissions to determine whether they accurately aligned.

- To assess the activity of *ensuring that the inventory accurately describes other system characteristics*, we asked agency officials to provide us with documentation that described the characteristics of the selected 15 systems (e.g., system security plans). We then compared that documentation to the characteristics identified in the agencies' inventory submissions to determine whether they accurately aligned.

- **Identify and annually update the funding needed to transition vulnerable cryptography on priority systems to PQC.** To assess the activity in this practice, we collected and reviewed agency funding assessments and interviewed or collected written responses from knowledgeable officials regarding missing data and controls used to develop and maintain the inventories. We describe the steps we took to assess the activity in more detail below.

  - To assess the activity of *including the funding needed for all vulnerable systems identified in the inventory and ensuring its*

[6]We did so using the Fiscal Year 2024 IT Portfolio data available on the Federal IT Dashboard. The Federal IT Dashboard is a public, government website previously operated by the Office of Management and Budget and currently by the General Services Administration at https://itdashboard.gov. It includes streamlined data to enable agencies and Congress to understand and manage federal IT portfolios and make better IT planning decisions.

[7]In selecting these systems, we divided them into three strata: (1) high-value assets, (2) high-impact systems, and (3) other systems that agencies determine are likely to be particularly vulnerable to CRQC-based attacks. We then selected one system from each stratum.

[8]We were not able to select systems from the remaining agency because it did not develop an inventory of prioritized systems.

accuracy, we reviewed the results of our assessment of the activity related to identifying a complete inventory of non-national security systems. Further, we asked agencies to describe the extent to which they determined their assessments to be accurate. Each of the agencies self-identified accuracy issues (or did not develop funding assessments); as such, we did not perform further testing on the accuracy of the assessments.

- **Test PQC in agency environments to help ensure that the algorithms will work in practice.** To assess the two activities in this practice, we asked agencies to provide test plans and results of any PQC testing. We also interviewed or collected written responses from knowledgeable officials regarding factors that prevented them from testing PQC. We describe the steps we took to assess each activity in more detail below.
  - To assess the practice of *working with software vendors to identify candidates for the testing of PQC*, we reviewed market research and other agency plans.
  - To assess the practice of *testing PQC in agency environments*, we asked agencies to provide relevant test results. None of the agencies performed such tests; as such, we did not take steps to further review test results.

We assessed each of the activities as:

- **fully addressed**—the agency provided evidence that it had fully implemented the activity,
- **partially addressed**—the agency provided evidence that it had implemented about half or a large portion of the activity,
- **not addressed**—the agency did not provide evidence it had implemented the activity, or
- **not selected**—the agency was not chosen for the specific activity.

Finally, we assessed each of the three preparatory practices as:

- **fully addressed:** The agency provided evidence that it had fully implemented all activities within a selected practice.
- **substantially addressed:** The agency provided evidence that it had either:
  - fully implemented two activities and did not implement the remaining one activity within the first practice, or

  - fully implemented one activity and partially implemented the remaining activity within the second or third practice.
- **partially addressed:** The agency provided evidence that it had either:
  - partially implemented all activities within a selected practice,
  - partially implemented four activities and did not implement the remaining one activity within the first practice, or
  - fully implemented one activity and did not implement the remaining activity within the second or third practice.
- **minimally addressed:** The agency provided evidence that it had either:
  - partially implemented three activities and did not implement the remaining two activities within the first practice,
  - partially implemented one activity and did not implement the remaining activity within the second or third practice.
- **not addressed:** The agency did not provide evidence that it had implemented any of the activities within a selected practice.

We presented the results of our assessment to the 24 agencies as well as OMB and the Office of the National Cyber Director (ONCD). In particular, we solicited their input and explanations for the results.

The performance audit upon which this report is based was conducted from February 2024 to September 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We subsequently coordinated with executive branch agencies included in this review from September 2025 to September 2026 to obtain agreement that the contents of this public version of the original report, which was marked with controlled unclassified information designations, may be publicly released. This public version was also prepared in accordance with these standards.

Appendix II: Summary of China's Efforts to Prioritize Quantum Information Science Development

One nation-state actor that our intelligence community has consistently highlighted as the top cyber threat to the U.S. Government—China[1]—has prioritized quantum information science development. In particular:

- **China is seeking to become a quantum information science superpower**. According to the intelligence community, China seeks to become a world science and technology superpower—including in the area of quantum information science—and to use this technological superiority for economic, political, and military gain.[2] However, it is unclear how much funding China has devoted to quantum computing. According to a study from the RAND Corporation, Chinese reports of total government funding for quantum technology are wildly conflicting, with publicly reported estimates ranging from $84 million per year to almost $3 billion per year.[3]
- **China is a global leader in quantum patents**. China is one of the global leaders in quantum patents. For example, prior to June 2023 China filed 1,408 patents related to quantum computing, according to research by the European Quantum Industry Consortium.[4] This is a substantial number of patents when compared to the amount filed by non-US countries during that same period, as shown in figure 5.

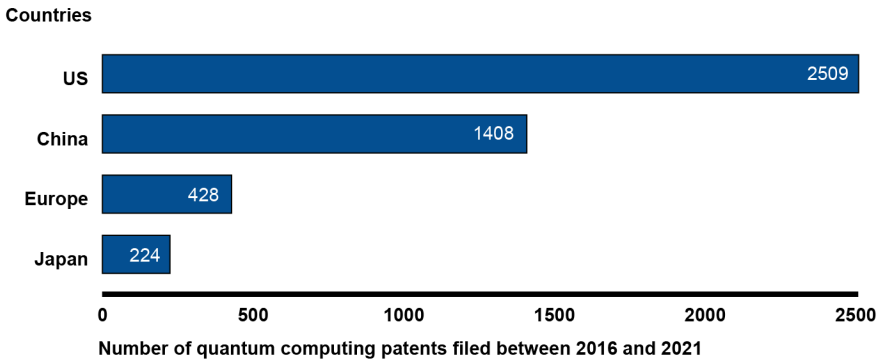
[1]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 25, 2025).

[2]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*. Of note, the Department of Defense recently reported that China is seeking to end its reliance on international components by developing its own specialized support equipment for quantum computers. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2024).

[3]RAND Corporation, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* (Feb. 2, 2022).

[4]European Quantum Industry Consortium, *A Portrait of the Global Patent Landscape in Quantum Technologies* (January 2024).

Figure 5: Ranked Number of Quantum Computing Patents Filed Prior to June 2023



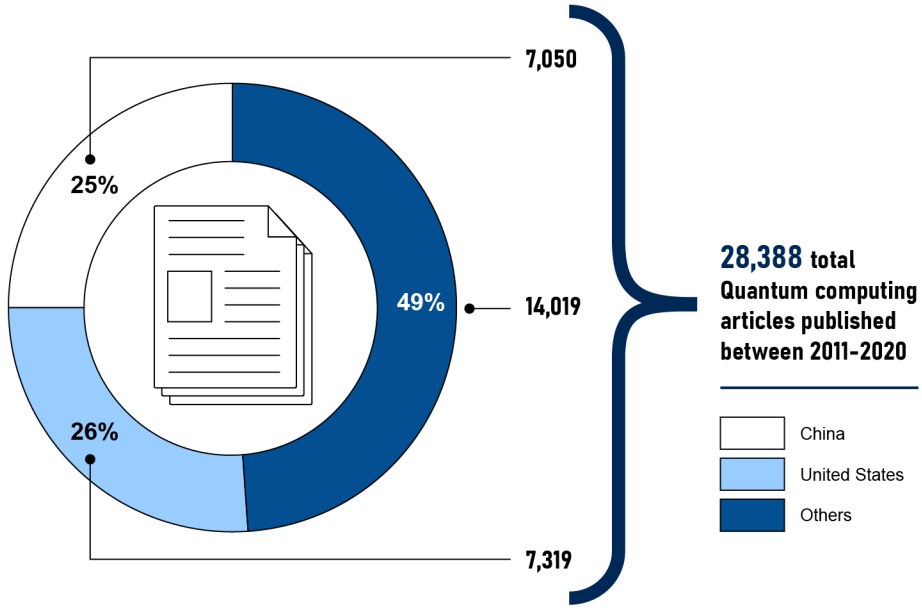
Source: GAO analysis of European Quantum Industry Consortium data. | GAO-27-108740

- **China is a global leader in quantum research**. With respect to research, China has high research output in every application domain of quantum technology, with more than 14,000 publications over the last decade from over 2,000 research institutions, according to a study from the RAND Corporation.[5] In addition, China has a significant share of the global research output in quantum computing, as shown in figure 6.[6]

[5]RAND Corporation, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*.

[6]RAND Corporation, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*.

Figure 6: Share of Global Quantum Computing Articles Published between 2011-2020

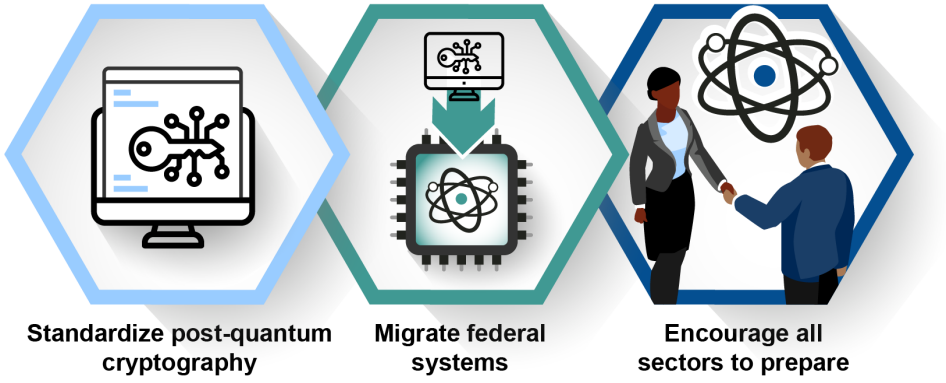


Sources: GAO analysis and icon (paper article). | GAO-27-108740

Appendix III: Summary of National Quantum Computing Cybersecurity Strategy

Various documents developed over the past 9 years have contributed to an emerging U.S. national strategy for addressing the threat of quantum computing to cryptography on unclassified systems. Based on review of these documents, we identified three central goals to the strategy (see figure 7).

Figure 7: The Three Central Goals of the U.S. National Quantum Computing Cybersecurity Strategy



Sources: GAO analysis; narathip/stock.adobe.com (computer/key illustration); GAO (all other icons/illustrations). | GAO-27-108740

See figure 8 below for a description of these goals and the documents in which they are outlined.

Figure 8: Central Goals Outlined in the Documents That Comprise the U.S. National Quantum Computing Cybersecurity Strategy

Goal 1: Standardize post-quantum cryptography (PQC)

Goal 2: Develop and implement plans for migrating federal agency systems to PQC

Goal 3: Encourage all sectors of the U.S. economy—including critical infrastructure sectors—to follow the federal government's model in preparing for a post-quantum future

Document Name	Release Date	Key Points
National Institute of Standards and Technology (NIST) Internal Report 8105, *Report on Post-Quantum Cryptography*	Apr 2016	• NIST outlined that it was taking steps to initiate a standardization effort in PQC. For example, NIST noted that it planned to subject any proposals to 3 to 5 years of scrutiny before standardization.
The White House, *National Cyber Strategy of the United States of America*	Sep 2018	• NIST will continue to evaluate and standardize quantum-resistant cryptographic methods.
The White House, *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, NSM-10	May 2022	• The U.S. must prioritize the timely and equitable transition of cryptographic systems to PQC, with the goal of mitigating as much risk as is feasible by 2035. • Migration to PQC is imperative across all sectors of the economy - including government and critical infrastructure. • The Cybersecurity and Infrastructure Security Agency (CISA) and NIST are to engage with critical infrastructure partners to advance PQC adoption.
Homeland Security Operational Analysis Center (operating under the direction of the Department of Homeland Security), *Preparing for Post-Quantum Critical Infrastructure: Assessments of Quantum Computing Vulnerabilities of National Critical Functions*	Aug 2022	• All national critical functions (i.e., 55 critical roles performed by government and the private sector considered vital to the security, economy, and public health and safety of the nation) will need to prepare for migration to PQC. • Three national critical functions are critical enablers of PQC migration: (1) provide internet-based content, (2) provide identity management and associated trust support services, and (3) provide IT products and services.
Office of Management and Budget, *Migrating to Post-Quantum Cryptography*, M-23-02	Nov 2022	• Agencies are to annually (1) develop prioritized inventories of information systems that contain vulnerable cryptographic methods and (2) assess the funding required to migrate to PQC.
The White House, *National Cybersecurity Strategy*	Mar 2023	• The federal government will prioritize the transition of vulnerable systems to PQC. The private sector should follow the government's model in preparing its systems for our post-quantum future.
The White House, *National Cybersecurity Strategy Implementation Plan*, Version 2	May 2024	• NIST will finalize its process to standardize one or more quantum-resistant methods.
Office of Management and Budget, *Report on Post-Quantum Cryptography*	Jul 2024	• The strategy is based on four principles: (1) a comprehensive cryptographic inventory; (2) migration must start before a cryptographically relevant quantum computer is known to be operational; (3) agencies must prioritize systems for PQC migration; and (4) identify systems that cannot support PQC early.
NIST Collection of Standardized PQC Methods: • Federal Information Processing Standard (FIPS) 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard • FIPS 204, Module-Lattice-Based Digital Signature Standard • FIPS 205, Stateless Hash-Based Digital Signature Standard	Aug 2024	• NIST finalized a set of standardized cryptographic methods believed to be resistant to cryptographically relevant quantum computers. Each PQC standard contains directions for implementing the method and descriptions of its potential uses. These methods are intended for public-key cryptography applications, and more are to be published in the future.

Source: GAO analysis of documents identified in the table. | GAO-27-108740

Note: On June 6, 2025, the White House issued an Executive Order on SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144. The order calls for the Secretary of Homeland

Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in consultation with the Director of the National Security Agency, to release by December 1, 2025, and thereafter regularly update, a list of product categories in which products that support PQC are widely available.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

BY ELECTRONIC SUBMISSION

December 15, 2025

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-108740, "FUTURE OF CYBERSECURITY: Federal Actions Needed to Prepare for Quantum Computing Threat"

Dear Ms. Cain:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (hereafter referred to as "the auditors") work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note the auditors' recognition of the importance of the threat of quantum computing to the cryptography used by federal agency systems, and migrating to post-quantum cryptography—cryptography that is resistant to quantum computers. DHS remains committed to ensuring that the Department's systems and networks, including high value assets and high impact systems, implement and maintain quantum readiness.

DHS responded to five recommendations in the previously issued restricted version of this report; however, the details contain sensitive information and as such are not being published here.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JEFFREY M BOBICH

Digitally signed by JEFFREY M BOBICH
Date: 2025.12.15 17:32:42 -05'00'

JEFFREY M. BOBICH
Director of Financial Management

2

Appendix V: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

December 17, 2025

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Cruz Cain,

Thank you for the opportunity to review the draft report, "FUTURE OF CYBERSECURITY: Federal Actions Needed to Prepare for Quantum Computing Threat" (108740). We agree with the recommendations. We have updated our process to collect cryptographic information through our Governance, Risk, and Compliance tool. A review of our inventory of information systems, as defined by the Federal Information Security Modernization Act, revealed that none currently use vulnerable cryptographic algorithms.

Once Post-Quantum Cryptography resistant algorithms become widely available for our information systems, we will develop transition plans accordingly.

Please contact me at (410) 274-0654 if I can be of further assistance. Your staff may contact Amy Gao, Director of the Audit Liaison Staff, at (410) 966-1711.

Sincerely,

Chad Poist
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Kaelin Kuhn (Assistant Director), Tina Barreto, Ceara Lance, and Sukhjoot Singh (Analysts-in-Charge), Ajay Amit, Evelyn Dube, Jonah Guthrie, Michael Lebowitz, Jess Lionne, Melissa Melvin, Claire McLellan, Carlo Mozo, and Andrew Stavisky.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us

Please Print on Recycled Paper.