GAO U.S. Government Accountability Office

Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy

GAO-25-107703
Q&A Report to the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

November 21, 2024

Why This Matters

Federal agencies and our nation's critical infrastructure—such as energy, transportation systems, communications, and financial services—are dependent on technology systems and electronic data to provide essential services and to process, maintain, and report vital information. Agencies and critical infrastructure owners and operators rely on cryptography (e.g., encryption) to protect sensitive systems and data.

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

We were asked to examine the federal government’s strategy to address the threat that quantum computers pose to cryptography on unclassified systems. This report provides information on how cryptographic methods protect systems and data, the threat quantum computers pose, strategies that international organizations have established to address this threat, and the U.S. national quantum computing cybersecurity strategy and the extent to which it addresses the desirable characteristics of a national strategy.

Key Takeaways

- Various documents developed over the past eight years have contributed to an emerging U.S. national quantum computing cybersecurity strategy. Based on our review of these documents, we identified three central goals: (1) standardize post-quantum cryptography, (2) migrate federal systems to that cryptography, and (3) encourage all sectors of the economy to prepare for the threat.
- The U.S. strategy documents partially address the desirable characteristics of a national strategy, as identified in prior GAO work. For example, with respect to the objectives, activities, milestones, and performance measures characteristic, the strategy documents identified objectives and activities for the first two goals but not for the third. In addition, the strategy documents did not fully identify milestones for the second and third goals and did not identify performance measures for any of the three goals.

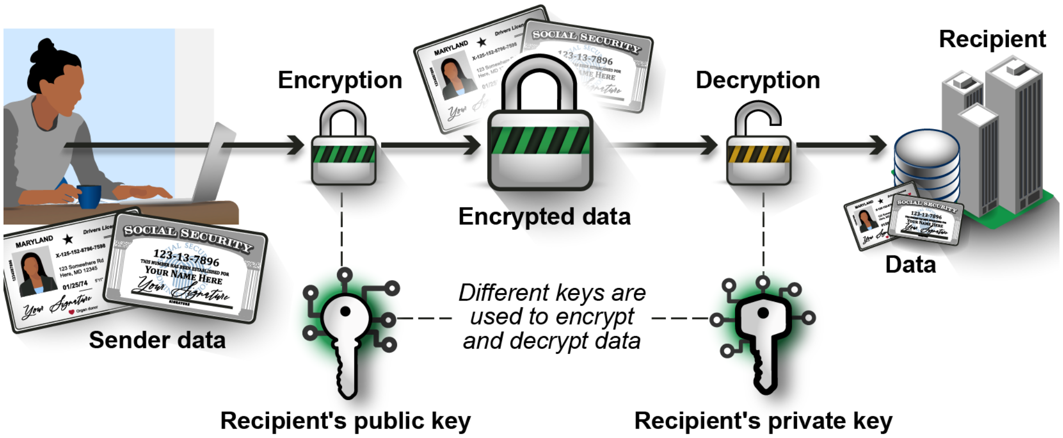
- No single federal organization is responsible for the U.S. strategy's coordination. In January 2021, Congress established an organization that is well-positioned to lead such efforts—the Office of the National Cyber Director.
- We recommend that the National Cyber Director (1) lead the coordination of the U.S. national quantum computing cybersecurity strategy and (2) ensure that the strategy's various documents address all the desirable characteristics of a national strategy.

What is cryptography and why is it important?

Cryptography is the practice of protecting information by transforming it using mathematical functions. These mathematical functions 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.[1]

Public-key cryptography is a common method of protecting information using two different keys, one private and one public.[2] Information can be transmitted freely with one of these keys applied. However, it only becomes accessible when received by an individual or organization that has the other key 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; Manoel/stock.adobe.com (keys); GAO (person and all other illustrations). | GAO-25-107703

Classical cryptographic methods, such as those used in public-key cryptography, are nearly impossible for conventional computers to break in reasonable time frames. Accordingly, federal agencies and critical infrastructure owners and operators rely on these methods to keep sensitive data and personally identifiable information secure within their technology systems.[3]

What are quantum computers and what threat do they pose to cryptography?

Quantum computers leverage the properties of a qubit (the quantum equivalent of classical computer bits) to solve selected problems significantly faster than classical computers. Current public-key cryptographic methods rely on the difficulty conventional computers have in performing certain calculations (i.e., factoring large numbers). However, sufficiently powerful quantum computers will not have this difficulty, potentially shortening the time to break current public-key methods to only hours or days compared to the billions of years a conventional computer would take.

Some experts estimate that a CRQC capable of breaking public-key cryptographic methods may be developed in the next 10 to 20 years.

Furthermore, adversaries could copy data protected by cryptography today and store it with the intention of accessing it later once a CRQC is developed.

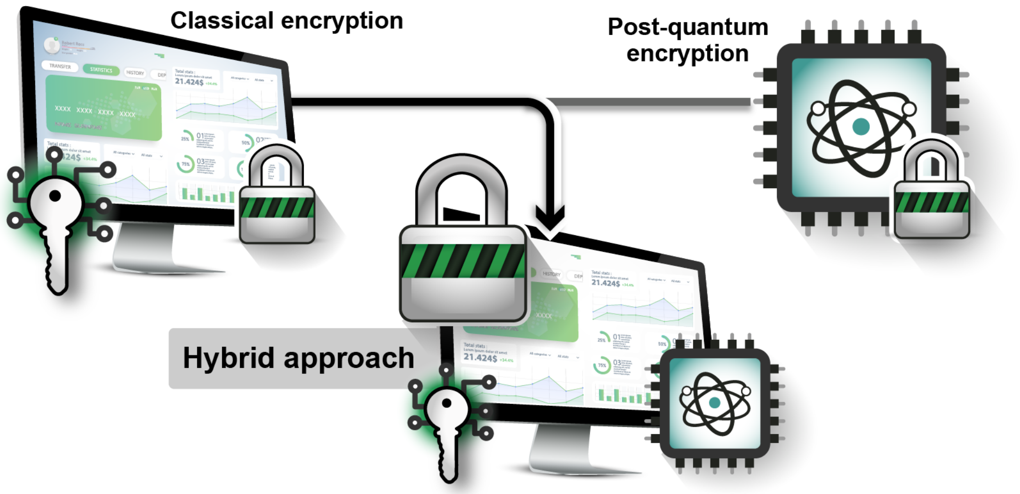
The capabilities of a quantum computer pose a significant threat to our nation's cryptography. Specifically, they pose a threat to the confidentiality, integrity, and availability of systems and data that rely on cryptography for protection. For example:

- *Confidentiality.* An adversary could use a quantum computer to break cryptographic methods and gain access to sensitive government information stored or communicated on a federal agency system (e.g., tax records, e-mails of senior department and agency leadership).
- *Integrity.* An adversary could target cryptographic methods that authenticate the source of information or data, allowing them to create and distribute fake communications that appear legitimate (e.g., a fake email from the head of a department or agency with a legitimate digital signature).
- *Availability.* An adversary could use a quantum computer to target critical infrastructure and disrupt the availability of important systems that provide essential services (e.g., electricity, water and wastewater, healthcare).

What strategies have international entities developed to address the threat of quantum computing?

Several major international organizations whose activities significantly influence the security of cyberspace—such as the Group of Seven and the North Atlantic Treaty Organization—have encouraged the use of post-quantum cryptography (PQC) that is resistant to quantum computers.[4] However, several other international organizations—such as the European Union and the Internet Engineering Task Force—have encouraged or published guidance on the use of a "hybrid" approach to PQC for certain applications. As shown in figure 2, such an approach involves the simultaneous use of both a new PQC method and a classical method.

Figure 2: A Simple Application of Hybrid Cryptography on an Information System



Sources: GAO analysis; ZinetroN/stock.adobe.com (bank screen shot); Manoel/stock.adobe.com (keys); GAO (all other illustrations/icons). | GAO-25-107703

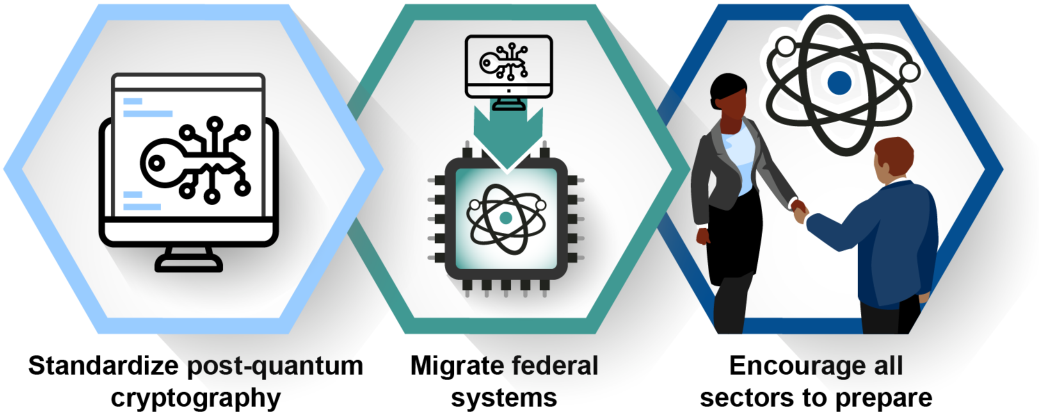
The "hybrid" approach could help provide enhanced protection before a CRQC is operational, but it could also introduce several challenges. According to industry experts, the benefit of this hybrid approach is that, if a vulnerability is identified in the near term that allows for a classical computer to break a new PQC method, the classical cryptographic method would still be in place to keep the information secure. The challenges with the hybrid approach are increased computing resources needed to run both methods and the added complexity of two migrations—an initial one to hybrid PQC and a later one to just PQC.

The Internet Engineering Task Force has begun the process of incorporating the "hybrid" approach described above to internet protocols.[5] For example, the organization has developed a draft standard for using a "hybrid" approach in Transport Layer Security 1.3—a widely used protocol for providing secure communications over computer networks. Several major international technology companies—such as Amazon, Apple, Google, and Meta—have also already begun adopting hybrid mechanisms in some of their products.

What is the national quantum computing cybersecurity strategy?

Various documents developed over the past eight 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 3):

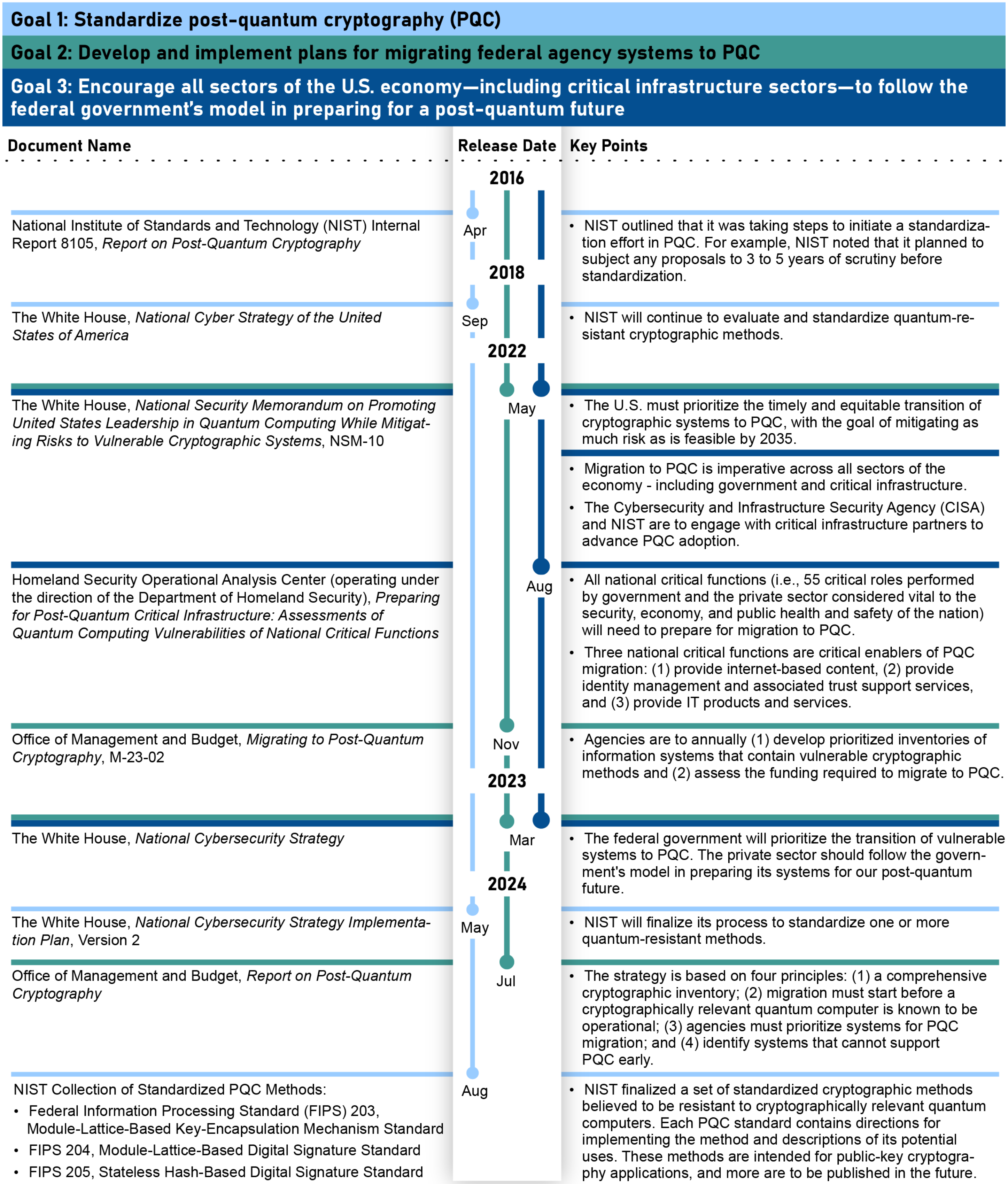
Figure 3: The Three Central Goals of the U.S. National Quantum Computing Cybersecurity Strategy


Standardize post-quantum cryptography
Migrate federal systems
Encourage all sectors to prepare

Sources: GAO analysis; narathip/stock.adobe.com (computer/key illustration); GAO (all other icons/illustrations). | GAO-25-107703

See figure 4 below for a description of these goals and the documents in which they are outlined.

Figure 4: 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*	2016 Apr	• 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*	2018 Sep	• 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	2022 May	• 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	• 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	• 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*	2023 Mar	• 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	2024 May	• NIST will finalize its process to standardize one or more quantum-resistant methods.
Office of Management and Budget, *Report on Post-Quantum Cryptography*	Jul	• 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	• 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-25-107703

What are the characteristics of a desirable national strategy?

We previously identified a set of desirable characteristics to aid parties in developing and implementing national strategies to help enhance their usefulness in policy and resource decisions, as well as ensure accountability.[6] National strategies should ideally contain these six characteristics:

- **Purpose, scope, and methodology.** Describes why the strategy was produced, the scope of its coverage, and the process by which it was developed.
- **Problem definition and risk assessment.** Identifies the national problems and threats the strategy is directed toward and analyzes threats to, and vulnerabilities of, critical assets and operations.
- **Objectives, activities, milestones, and performance measures.** Defines the objectives identifying what the strategy is trying to achieve, and activities to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.
- **Resources, investments, and risk management.** Summarizes what the strategy's implementation will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.
- **Organizational roles, responsibilities, and coordination.** Describes who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.
- **Implementation and integration.** Addresses how a national strategy is to be implemented and how the document relates to other strategies' goals, objectives, and activities—including international strategies.

What desirable characteristics does the national quantum computing cybersecurity strategy address?

The government's quantum computing cybersecurity strategy documents partially addressed all six desirable characteristics of a national strategy.

- **Purpose, scope, and methodology.** Several documents identified their purpose and scope. With regard to methodology, the National Institute of Standards and Technology's (NIST) PQC standards documents provide information on how they were developed through a selection and evaluation process. However, the remaining documents did not describe the methodology or the process agencies used to develop them for the other two goals.

- **Problem definition and risk assessment.** Although several documents defined the problem as the threat of a CRQC to vulnerable cryptographic methods, they did not fully define a CRQC. Specifically, the documents did not define the point at which a quantum computer would become cryptographically relevant, such as when it can defeat particular cryptographic methods and key sizes within a certain period of time (e.g., a week).

  Regarding risk assessments, one of the documents identified and assessed the risk of a CRQC to each of the 55 national critical functions associated with critical infrastructure. This risk assessment addressed several factors, including urgency, breadth of systems requiring updates, and priority for assistance. For example, the assessment highlighted the risk of a CRQC to operational technology (i.e., systems and devices that interact with the physical environment) used by several critical functions (e.g., distributing electricity). In particular, the assessment explained that it may be costly and challenging to migrate these systems to PQC—particularly for legacy systems that lack any cryptography, or the computing resources needed for PQC.

However, the strategy documents did not include a similar risk assessment for federal agencies and their systems (e.g., assess the urgency relative to certain agencies or critical functions that the agencies and their systems perform).

- **Objectives, activities, milestones, and performance measures.** The government's quantum computing cybersecurity strategy documents identified objectives and activities for the first two goals related to standardizing PQC and transitioning federal agency systems to PQC. However, the documents did not fully define objectives or activities for the other goal of encouraging all sectors—including critical infrastructure—to migrate to PQC. Although the strategy documents directed the Cybersecurity and Infrastructure Security Agency (CISA) and NIST to collaborate with critical infrastructure owners and operators, they did not specify how federal organizations are to encourage the adoption of PQC.

  Regarding milestones and performance measures, one of the documents included milestones for the activities associated with the goal of standardizing PQC. The strategy documents also identified several milestones for the second goal of transitioning federal agency systems to PQC. Specifically, the identified milestones related to preparing agencies to transition to PQC and the end date for the transition. However, the strategy documents did not identify any interim milestones to guide agencies' actual migration to PQC.[7] Regarding the third goal of encouraging sectors (including critical infrastructure) to migrate to PQC, the documents did not provide any milestones. Moreover, the strategy documents did not identify performance measures for the three goals.

- **Resources, investments, and risk management.** The strategy and its associated documentation identified the cost of addressing the second goal of migrating federal agency systems and where resources and investments should be targeted. Specifically, the Office of Management and Budget's (OMB) *Report on Post-Quantum Cryptography* provided a cost estimate of $7.1 billion to migrate priority federal agency systems to PQC between 2025 and 2035.[8] However, OMB's report identified concerns with the accuracy of the $7.1 billion cost estimate. According to the report, this figure represents an initial rough order of magnitude projection with a high level of uncertainty. OMB's report added that agencies are required to update their cost estimates annually to allow for adjustments as they gain familiarity with their inventories of existing cryptography and costing methodologies, as well as the transition process.

  In addition, the strategy documents did not identify specific investment sources or types of resources needed for addressing the second goal (e.g., staffing levels and expertise needed throughout the migration effort). Regarding risk management for this goal, the report did address how agencies are to manage risk by identifying priority systems that need to be migrated first.

  Further, when it comes to the other two goals of standardizing PQC and transitioning all sectors—including critical infrastructure—to PQC, the documents did not describe the cost, resources, or investments needed. The documents also did not describe risk management processes related to these two goals.

- **Organizational roles, responsibilities, and coordination.** Regarding roles and responsibilities, the various quantum computing cybersecurity strategy documents addressed which organizations will be implementing the strategy for the two goals of standardizing PQC and migrating federal systems to that cryptography and what their roles and responsibilities will be. However, the documents did not fully address organizational roles or responsibilities for CISA or NIST in the final goal of encouraging all sectors—including critical infrastructure—to migrate to PQC. In particular, given the previously discussed gaps in fully defining objectives and activities for this goal, which organizations will be needed for implementing the goal's interim milestones and what their roles and responsibilities will be is unclear.

With respect to coordination, the documents had mechanisms for participating parties to coordinate efforts for each of the three goals. For example, the documents highlighted the use of an interagency working group to coordinate migration across federal agencies.

- **Integration and implementation.** Several of the documents that comprise the strategy are integrated with other strategy documents by including references to them. However, the documents did not describe how, if at all, the strategy will integrate with international strategies—particularly those that have emphasized the use of a "hybrid" approach to PQC.

  Regarding implementation, the strategy documents discussed plans for implementation of the first two goals. However, the strategy did not describe plans for implementing the third goal of transitioning all sectors to PQC—including critical infrastructure.

Why have the desirable characteristics for the national quantum computing cybersecurity strategy not been fully addressed?

The desirable characteristics have not been fully addressed, in part, because no single federal organization is responsible for coordination and oversight of a comprehensive national strategy for quantum computing cybersecurity. For example, the *2022 Quantum Computing Cybersecurity Preparedness Act* called for OMB to develop a strategy for addressing the quantum computing threat to federal systems.[9] Pursuant to that mandate, OMB's July 2024 *Report on Post-Quantum Cryptography* contains a section that is focused on the strategy for addressing the second goal of developing and implementing plans for migrating federal agency systems to PQC.[10] However, consistent with the act, the strategy in the document did not cover the third goal of encouraging all sectors to prepare for PQC.

Although no single organization is responsible for the coordination and oversight of the national quantum computing cybersecurity strategy, Congress established an organization well-positioned to lead such efforts. In January 2021, Congress established the Office of the National Cyber Director (ONCD) to provide cybersecurity leadership for the United States.[11] The National Cyber Director heads the office and leads the coordination and implementation of national cyber policy and strategy.[12] In addition, federal law requires the Director to annually report to Congress on cybersecurity threats, including any new or emerging technologies that may affect national security—such as the threat posed by quantum computing to cryptography.[13]

After we shared our preliminary findings with ONCD, officials agreed that the Executive Office of the President and certain organizations that comprise it, including ONCD, are well-positioned to lead the coordination of the national quantum computing cybersecurity strategy.[14] If ONCD embraces this coordination role, agencies will have more clarity on their responsibilities and the common outcomes they are aiming to achieve. In addition, it is important that the various strategy documents fully address the desirable characteristics for national strategies. A fully comprehensive strategy will provide the nation a better-defined roadmap for allocating and managing resources and holding participants accountable for achieving results.

Conclusions

Federal agencies and critical infrastructure owners and operators face an urgent need to transition to PQC to address the threat to the cryptography that our nation relies on to protect sensitive information. This transition is particularly critical given the potential for adversaries to copy sensitive data today and access it once a CRQC becomes available.

Federal agencies recognize the quantum computing threat and have taken some actions to partially address it. Designating leadership committed to fully implementing desirable characteristics of a national strategy is essential to ensure success. ONCD is well-positioned to fill this gap and provide a comprehensive roadmap for the transition to PQC.

Recommendation for Executive Action

The National Cyber Director should (1) lead the coordination of the national quantum computing cybersecurity strategy and (2) ensure that the strategy's various documents address all the desirable characteristics of a national strategy. (Recommendation 1)

Agency Comments

We provided a draft of this report to the Departments of Commerce and Homeland Security, as well as the Office of Management and Budget, the Office of Science and Technology Policy, and ONCD for review and comment.

ONCD did not agree or disagree with the recommendation in the report. The Office of Management and Budget and Office of Science and Technology Policy did not have any comments on the report. The Departments of Commerce and Homeland Security, as well as ONCD, provided technical comments, which we incorporated as appropriate.

How GAO Did This Study

We summarized information on cryptography and the threat quantum computers pose to it. To do so, we reviewed relevant prior GAO work.[15]

In addition, we summarized the strategies international organizations had developed to address the threat of quantum computers to their cryptography. To do so, we selected 16 organizations whose international activities significantly influence the security and governance of cyberspace, as identified in prior GAO work (see table 1 below for the 16 organizations).[16] We also confirmed these organizations' continued influence on cyberspace by comparing them with

- those organizations with whom the Department of State's Cyberspace and Digital Policy Bureau engages, according to the department's relevant strategy;[17] and
- those organizations identified in more recent GAO reports involving international technology issues.[18]

Table 1: Selected Organizations with Significant Influence on International Cyberspace Security and Governance

Asia-Pacific Economic Cooperation	International Organization for Standardization	North Atlantic Treaty Organization
Association of Southeast Asian Nations	International Telecommunication Union	Organization of American States
Council of Europe	Internet Corporation for Assigned Names and Numbers	Organisation for Economic Cooperation and Development
European Union	Internet Engineering Task Force	United Nations
Group of Seven	Internet Governance Forum	
Institute of Electrical and Electronic Engineers	INTERPOL	

Source: Summary of GAO information. | GAO-25-107703

We reviewed each organization's website to identify and summarize strategies and other information the organizations developed on addressing the threat of quantum computing to cryptography.

Further, we summarized the U.S. national quantum computing cybersecurity strategy and determined the extent to which it addressed desirable characteristics of a national strategy. To do so, we selected five federal agencies with leadership roles defined in legislation in quantum computing or the cybersecurity of unclassified federal agency and critical infrastructure systems. Those five federal agencies were the Department of Commerce's National Institute of Standards and Technology and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency; as well as the Office of Management and Budget, the Office of Science and Technology Policy, and the Office of the National Cyber Director.

We asked these agencies to identify key documents that comprised the U.S. strategy for addressing the threat of quantum computing to cryptography used to protect unclassified federal agency and critical infrastructure systems. We then reviewed and summarized the documents' collective central goals and the main points in each document. We presented our summary to the five selected agencies and solicited their input on the completeness and accuracy of the information.

We then compared these documents to the desirable characteristics of a national strategy, as identified in prior GAO work.[19] Table 2 identifies the six characteristics included in our review.

Table 2: Desirable Characteristics of a National Strategy

Characteristic	Definition	Examples
Purpose, scope, and methodology	Describes why the strategy was produced, the scope of its coverage, and the process by which it was developed.	• Statement of broad or narrow purpose • Major functions, mission areas, or activities it covers
Problem definition and risk assessment	Identifies the national problems and threats the strategy is directed toward and analyzes threats to, and vulnerabilities of, critical assets and operations.	• Discussion/definition of problems, their causes, and operating environment • Risk assessment (analysis of threats/vulnerabilities)
Objectives, activities, milestones, and performance measures	Defines the objectives identifying what the strategy is trying to achieve, and activities to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	• Overall results desired • Specific activities to achieve results • Priorities, milestones, and performance measures
Resources, investments, and risk management	Summarizes what the strategy's implementation will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs.	• Resources and investments associated with the strategy • Types of resources needed (budgetary, human capital, contracts) • Sources of resources (e.g., federal, state, local, and private)
Organizational roles, responsibilities, and coordination	Describes who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	• Roles and responsibilities of specific federal agencies or offices • Lead, support, and partner roles and responsibilities
Implementation and integration	Addresses how a national strategy is to be implemented and how it relates to other strategies' goals, objectives, and activities—including international strategies.	• Integration with international and national strategies and with relevant documents from implementing organizations • Implementation guidance

Source: GAO. | GAO-25-107703

We assessed whether the strategy documents had addressed the desirable characteristics of a national strategy as

- fully addressed, if available evidence demonstrated all aspects of the selected characteristic;
- partially addressed, if available evidence demonstrated some, but not all, aspects of the selected characteristic; and
- not addressed, if available evidence did not demonstrate any aspects of the selected characteristic.

As part of our analysis, we also reviewed prior legislation, key documentation, and interviewed agency officials to determine federal roles and responsibilities tied to cybersecurity and the quantum computing cybersecurity strategy.

We conducted this performance audit from July 2024 to November 2024 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.

List of Addressees

The Honorable Margaret Wood Hassan
Chair
The Honorable Mitt Romney
Ranking Member
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

We are sending copies of this report to the appropriate congressional committees, the Departments of Commerce and Homeland Security, as well as the Office of the National Cyber Director, Office of Management and Budget, and Office of Science and Technology Policy. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Marisol Cruz Cain, Director, Information Technology and Cybersecurity, cruzcainm@gao.gov, (202) 512-5017

Sarah Kaczmarek, Managing Director, Public Affairs, KaczmarekS@gao.gov, (202) 512-8590

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400

Staff Acknowledgments: Kaelin Kuhn (Assistant Director), Ceara Lance (Analyst-in-Charge), Evelyn Dube, Jess Lionne, Adam Vodraska, Michael Lebowitz, Scott Fletcher, Claire McLellan, Nicole Catanzarite, Christopher Businsky, and Scott Pettis

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.

Visit GAO on the web at https://www.gao.gov.

Endnotes

[1] One type of cryptography, digital signatures, includes the virtual signing and authentication of documents. This cryptographic method involves the sender signing a message and applying their own private key to the signature, followed by the signature being verified by the same sender's public key. This results in a message with a verified signature that can be sent to others.

[2] Another type of cryptographic method is private-key, or symmetric, cryptography. This cryptographic method uses the same private key for both encryption and decryption.

[3] In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

[4] PQC refers to new cryptographic methods intended to withstand attacks from both quantum and conventional computers.

[5] Internet protocols are sets of rules for data transmission that allow different devices to "communicate", or transfer data to one another. The Internet Engineering Task Force is a technical standards-setting body responsible for developing and maintaining the Internet's core standards. It is a voluntary, consensus-based standards body, whose participants include network operators, academics, and representatives of government and industry.

[6] GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[7] Office of Management and Budget representatives noted that, in accordance with NSM-10, the office plans to issue interim milestones to guide agency migration to PQC.

[8] Office of Management and Budget, *Report on Post-Quantum Cryptography as required by the Quantum Computing Cybersecurity Preparedness Act,* Pub. L. No: 117-260 (July 2024).

[9] Pub. L. No. 117-260 (Dec. 21, 2022). The Quantum Computing Cybersecurity Preparedness Act conveyed the sense of Congress that a strategy for the migration of IT of the federal government to PQC is needed.

[10] Office of Management and Budget, *Report on Post-Quantum Cryptography*.

[11] 6 U.S.C. § 1500(a) - (c)(C).

[12] 6 U.S.C. § 1500(b) - (c).

[13] 6 U.S.C. § 1500(c)(1)(G).

[14] ONCD officials also highlighted the following organizations within the Executive Office of the President: the National Security Council, Office of Management and Budget, and Office of Science and Technology Policy.

[15] See, e.g., GAO, *Science & Tech Spotlight: Securing Data for a Post-Quantum World*, GAO-23-106559 (Washington, D.C.: Mar. 8, 2023) and *Quantum Computing and Communications: Status and Prospects*, GAO-22-104422 (Washington, D.C.: Oct. 19, 2021).

[16] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

[17] Department of State, *United States International Cyberspace & Digital Policy Strategy* (May 6, 2024).

[18] GAO, *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, GAO-24-105563 (Washington, D.C.: Jan. 11, 2024); *Cybersecurity: Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks*, GAO-22-104560 (Washington, D.C.: March 3, 2022); and *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C. Nov. 24, 2020).

[19] GAO-04-408T