



QUANTUM COMPUTING

Leadership Needed to Coordinate Cyber Threat Mitigation Strategy

Statement of Marisol Cruz Cain, Director, Information Technology and Cybersecurity

Testimony

Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery Expected at 2:00 p.m. ET
Tuesday, June 24, 2025

GAO-25-108590

United States Government Accountability Office

Accessible Version

GAO Highlights

QUANTUM COMPUTING

Leadership Needed to Coordinate Cyber Threat Mitigation Strategy

GAO-25-108590

June 2025

A testimony before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Government Reform, House of Representatives.

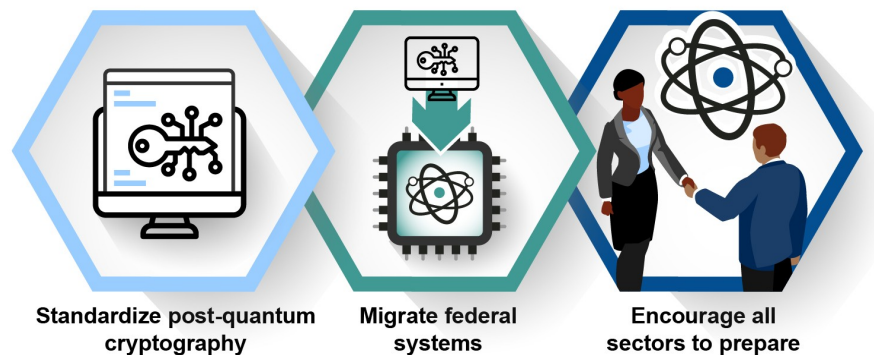
For more information, contact: Marisol Cain Cruz at CruzCainM@gao.gov.

What GAO Found

Quantum computers and their capabilities have the potential to revolutionize modern computing but could also introduce new risks. In October 2021, GAO identified options that policymakers (e.g., legislative bodies, government agencies, and industry) could consider to help address key factors affecting the development of quantum computers. Specifically, the report noted that policymakers could encourage further collaboration; consider ways to expand the workforce; incentivize or support continued investment in development; and encourage the development of a robust, secure supply chain.

In November 2024, GAO reported that various documents developed over the past 8 years had contributed to an emerging U.S. national strategy for addressing the threat of quantum computing to cryptography. Based on review of these documents, GAO identified three central goals in the strategy: (1) standardize post-quantum cryptography that is resistant to attacks from conventional and quantum computers, (2) migrate federal systems to this cryptography, and (3) encourage all sectors of the economy to prepare for the threat of quantum computers to their cryptography (see figure).

Figure: 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-25-108590

However, GAO reported the strategy documents had not fully defined a strategy to counter the threat of quantum computers to the nation's cryptography. Specifically, the documents did not fully address the key characteristics of a national strategy that GAO had identified in prior work. For example, the documents did not identify objectives for the third goal to encourage all sectors to prepare and did not identify performance measures for any of the three goals. GAO noted that these shortcomings occurred, in part, because no single federal organization was responsible for coordination and oversight of a comprehensive national strategy. However, in January 2021 Congress established an organization that is well-positioned to lead these efforts: the Office of the National Cyber Director. If the office embraces this role and ensures

that the strategy fully addresses key characteristics, the nation will have a better-defined roadmap for allocating resources and holding participants accountable.

Why GAO Did This Study

Quantum computers could address some critical problems that are not possible to solve with conventional computers within the span of a human lifetime. However, GAO has reported that the emergence of quantum computers could undermine the security of widely used cryptographic methods (e.g., encryption) that federal agencies and critical infrastructure owners and operators rely on to protect sensitive systems and data. Some experts predict that a quantum computer capable of breaking certain cryptography may be developed in the next 10 to 20 years, putting agency and critical infrastructure systems that rely on cryptography at risk.

GAO was asked to testify on its 2021 and 2024 quantum computing reports. GAO summarized these prior reports that discuss (1) factors that affect the development of quantum computers and (2) the federal government's strategy to address the threat that quantum computers pose to cryptography on unclassified systems.

What GAO Recommends

In its 2024 report, GAO made one recommendation to the Office of the National Cyber Director to (1) lead the coordination of the national quantum computing cybersecurity strategy and (2) ensure that the strategy's various documents address all the key characteristics of a national strategy. The office did not agree or disagree with the recommendation and it has not yet been implemented.

Chairwoman Mace, Ranking Member Brown, and Members of the Subcommittee:

Thank you for the opportunity to discuss our reports on the development of quantum computers and the status of a threat mitigation strategy for such technologies. As you know, quantum computers could solve some critical problems that are not possible with conventional computers within the span of a human lifetime. For example, they may be able to simulate critical chemical reactions for developing fertilizers and medicines.

However, we recently reported that the emergence of quantum computers could undermine the security of widely used cryptographic methods (e.g., encryption) that federal agencies and critical infrastructure owners and operators rely on to protect sensitive systems and data.¹ 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 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.

In this statement, we will summarize our prior reports that discuss (1) factors that affect the development of quantum computers and (2) the federal government’s strategy to address the threat that quantum computers pose to cryptography on unclassified systems. In developing this testimony, we reviewed our recently issued reports on quantum computing.²

More detailed information on the objectives, scope, and methodology for that work can be found in the issued reports listed in Related GAO Products at the conclusion of this statement. We conducted the work on which this statement is based in accordance with all sections of GAO’s Quality Assurance Framework. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

Background

Quantum computers leverage the properties of quantum physics to solve selected problems significantly faster than today’s conventional computers. Conventional computers use binary digits, or “bits,” to represent information through 0s or 1s. By contrast, quantum computers use quantum bits, or “qubits,” to represent information through any combination of 0s and 1s simultaneously.

¹GAO, *Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy*, [GAO-25-107703](#) (Washington, D.C.: Nov. 21, 2024). We also have ongoing work related to the (1) development of quantum computers and the associated workforce and (2) agency preparedness for addressing the threat of quantum computers to their cryptography. This work is being conducted at the request of the Ranking Member of the Joint Economic Committee. We plan to report later this year on the results of our work.








²[GAO-25-107703](#), GAO, *Quantum Technologies: Defense Laboratories Should Take Steps to Improve Workforce Planning*, [GAO-24-106284](#) (Washington, D.C.: Dec. 5, 2023); *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).

Scientists are actively researching a variety of technologies to create physical qubits. An outstanding challenge is that the information that physical qubits represent is 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.

Quantum computers have the potential to be transformative but are in the early stages of development. Experimental quantum computing systems available today are much smaller than the quantum computers needed for chemistry or cryptography applications.

Large quantum computers could solve some critical problems that are not practically possible with computers available today. For example, they may be able to simulate critical chemical reactions for developing fertilizers and medicines (see figure 1). However, potential drawbacks of implementation and use include malicious use by our adversaries (as discussed in more detail in the next section).

Figure 1: Size of Quantum Computer Needed for Different Applications

Physical qubits ^a	Potential applications	Sectors with potential interest	Limitations
<p><1,000 qubits</p> 	<ul style="list-style-type: none"> Calculations for small chemicals (H₂, LiH, BeH₂) require less than 100 qubits Test quality of quantum hardware requires less than 100 qubits Test theories about black holes Quantum assisted optimization 	 Quantum computing companies  Academia  Research institutions	<ul style="list-style-type: none"> May not be useful for end users Unclear how much advantage is obtained for optimization
<p>1,000 – 100,000</p>	<ul style="list-style-type: none"> Enhance machine learning Enhance optimization problems Test quality of quantum hardware Finance simulations 	 Finance	<ul style="list-style-type: none"> Unclear advantage for machine learning Unclear how much advantage is obtained for optimization
<p>100,000+</p> 	<ul style="list-style-type: none"> Simulate critical fertilizer components Chemistry for energy applications Chemistry for pharmaceutical applications Break some forms of encryption Simulate crystals and metals Simulate superconductivity Grover's search algorithm 	 Pharmaceutical  Energy  Agriculture  Security	<ul style="list-style-type: none"> Limits to calculations Unclear advantage for search algorithms Post quantum cryptography prevents quantum attacks

Sources: GAO analysis of government documents, journal articles, National Academies of Sciences, Engineering, and Medicine report, and interviews with agency officials and potential end users, GAO (all illustrations). | GAO-25-108590

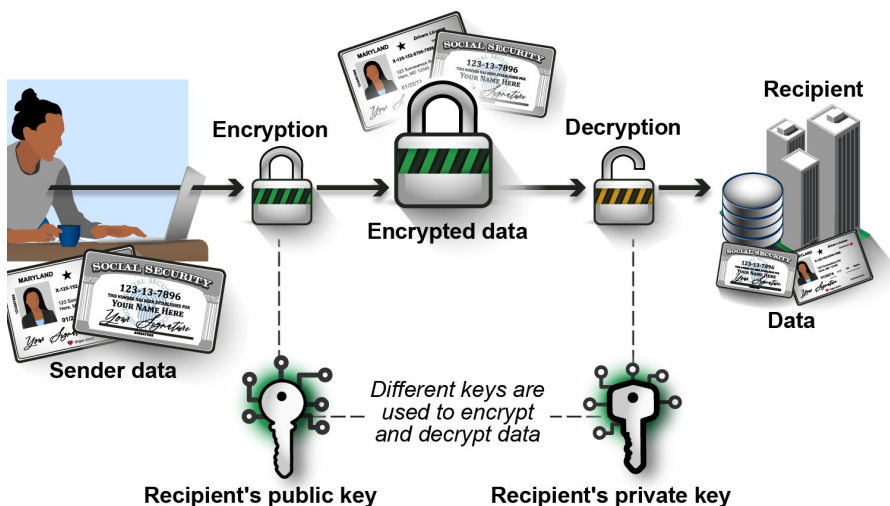
^aSome documents reported the number of logical qubits, a group of physical qubits that mimics a robust single stable qubit. If the number of physical qubits was not provided, we multiplied the number by 1,000 to obtain an estimated number of physical qubits. Estimates of the ratio of logical qubits to physical qubits include 1 to 300, 1,000, 10,000, and higher. As qubits improve, the number of physical qubits needed for some applications may decrease.

Quantum Computers Pose a Threat to Cryptography

One potential drawback to quantum computers is that adversaries may use them to compromise cryptography used to protect sensitive information. Cryptography is the practice of protecting information by using mathematical functions to 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.³

Public-key cryptography is a common method of protecting information using two different keys, one private and one public.⁴ 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 of these keys are combined, the information or data is successfully “unlocked” and can be used accordingly (see figure 2).

Figure 2: 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-25-108590

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.⁵

³One 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.

⁴Another type of cryptographic method is private-key, or symmetric, cryptography. This cryptographic method uses the same private key for both encryption and decryption.

⁵In 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.

However, sufficiently powerful quantum computers would 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—that is, a full-scale quantum computer capable of breaking public-key cryptographic methods—may be developed in the next 10 to 20 years.⁶ 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, emails of senior department and agency leadership).
- **Integrity.** An adversary could target cryptographic methods that authenticate the source of information or data, allowing the creation and distribution of 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).

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.⁷ 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.

Congress has acknowledged the importance of the threat posed by quantum computers to cryptography. In December 2022, Congress passed the *Quantum Computing Cybersecurity Preparedness Act*.⁸ The act called for the Office of Management and Budget to, among other things,

- develop a strategy for addressing the quantum computing threat to federal systems and
- issue guidance to federal agencies on how to address the threat.

⁶A quantum computer capable of breaking encryption would need to hold thousands of logical qubits and would likely require millions of physical qubits.

⁷Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 25, 2025).

⁸Pub. L. No. 117-260 (Dec. 21, 2022).

Key Characteristics of a National Strategy

We previously identified a set of key 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.⁹ 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.

GAO Identified Options to Address Factors That Affect the Development of Quantum Computers

In October 2021, we reported on four factors that affect the development and use of quantum computers and other quantum technologies: (1) collaboration, (2) workforce size and skill, (3) investment, and (4) the supply chain.¹⁰ The table below describes options that policymakers—legislative bodies, government agencies, standards-setting organizations, industry, and other groups—could consider to help address these factors, enhance benefits, or mitigate drawbacks of quantum technology development and use.¹¹

⁹GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

¹⁰[GAO-22-104422](#).

¹¹The options are neither recommendations to federal agencies nor matters for congressional consideration. We intend for these options to provide policymakers with a broader base of information for decision-making.

Table 1: Policy Options to Help Address Factors That Affect Quantum Computer and Other Quantum Technology Development and Use, or to Enhance Benefits or Mitigate Drawbacks

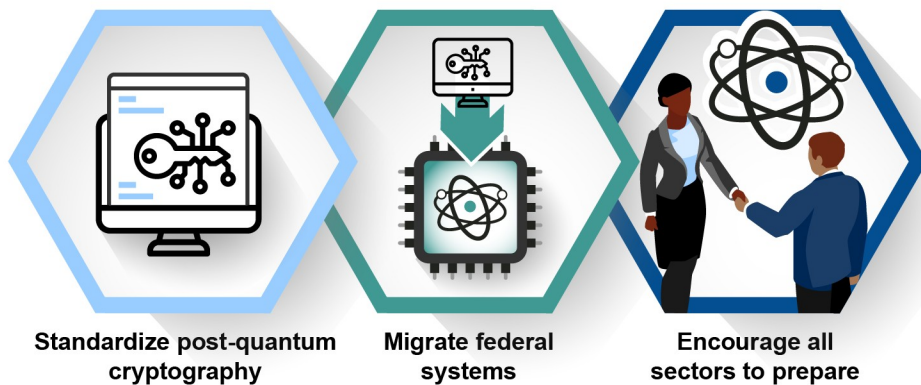
Policy options and potential implementation approaches	Opportunities	Considerations
<p>Collaboration. Policymakers could encourage further collaboration in developing quantum technologies, such as collaboration among:</p> <ul style="list-style-type: none"> Scientific disciplines Sectors Countries 	<p>Collaboration among disciplines could enable technology breakthroughs.</p> <p>Collaboration could help accelerate research and development, as well as facilitate technology transfer from laboratories to the private sector, federal agencies, and others.</p> <p>International collaboration could bring mutual benefits to the U.S. and other countries by accelerating scientific discovery and promoting economic growth.</p>	<p>Intellectual property concerns could make quantum technology leaders reluctant to collaborate.</p> <p>Institutional differences could make collaboration difficult.</p> <p>Export controls may complicate international collaboration but are also needed to manage national security risks.</p>
<p>Workforce. Policymakers could consider ways to expand the quantum technology workforce by, for example:</p> <ul style="list-style-type: none"> Leveraging existing programs and creating new ones Promoting job training Facilitating appropriate hiring of an international workforce who are deemed not to pose a national security risk 	<p>Educational programs could provide students and personnel with the qualifications and skills needed to work in quantum technologies across the private sector, public sector, and academia.</p> <p>Training personnel from different disciplines in quantum technologies could enhance the supply of quantum talent.</p> <p>International hiring could allow U.S. quantum employers to attract and retain top talent from other countries.</p>	<p>Efforts to increase the quantum technology labor force may affect the supply of expertise in other technology fields with high demand.</p> <p>It may be difficult to adequately develop workforce plans to accommodate quantum technology needs.</p> <p>International hiring could be challenging because of visa requirements and export controls, both in place for national security reasons.</p>
<p>Investment. Policymakers could consider ways to incentivize or support investment in quantum technology development, such as:</p> <ul style="list-style-type: none"> Investments targeted toward specific results Continued investment in quantum technology research centers. Grand challenges to spur solutions from the public 	<p>More targeted investments could help advance quantum technologies. These may include investments in improving access to quantum computers and focusing on real-world applications.</p> <p>Quantum technologies testbed facility investments could support technology adoption.</p> <p>Grand challenges have shown success in providing new capabilities and could be leveraged for quantum technologies.</p>	<p>It may be difficult to fund projects with longer-term project timeframes.</p> <p>A lack of standards or, conversely, developing standards too early, could affect quantum technology investments. Without standards, businesses and consumers may not be confident that products will work as expected.</p> <p>Developing standards too early may deter the growth of alternative technology pathways.</p>
<p>Supply chain. Policymakers could encourage the development of a robust, secure supply chain for quantum technologies by, for example:</p> <ul style="list-style-type: none"> Enhancing efforts to identify gaps in the global supply chain Expanding fabrication capabilities for items with an at-risk supply chain 	<p>A robust supply chain could help accelerate progress and mitigate quantum technology development risks by expanding access to necessary components and materials or providing improved economies of scale.</p> <p>Quantum material fabrication capabilities improvements could ensure a reliable supply of materials to support quantum technology development.</p> <p>Facilities dedicated to producing quantum materials could help support scalable manufacturing of component parts needed for quantum technology development.</p>	<p>The current quantum supply chain is global, which poses risks. For example, it is difficult to obtain a complete understanding of a component's potential vulnerabilities.</p> <p>Some critical components, such as rare earths, are mined primarily outside of the U.S., which may pose risks to the supply chain that are difficult to mitigate.</p> <p>Quantum manufacturing facilities take a long time to develop and can be costly.</p>

Source: GAO. | GAO-25-108590

GAO Reported That Federal Agencies Have Not Fully Defined a Strategy for Addressing the Quantum Cyber Threat

In November 2024, we reported that various documents developed over the past 8 years have contributed to an emerging U.S. national strategy for addressing the threat of quantum computing to cryptography on unclassified systems.¹² Based on our review of these documents, we identified three central goals in the strategy: (1) standardize post-quantum cryptography that is resistant to attacks from conventional and quantum computers, (2) migrate federal systems to this cryptography, and (3) encourage all sectors of the economy to prepare for the threat of quantum computers to their cryptography (see figure 3).

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

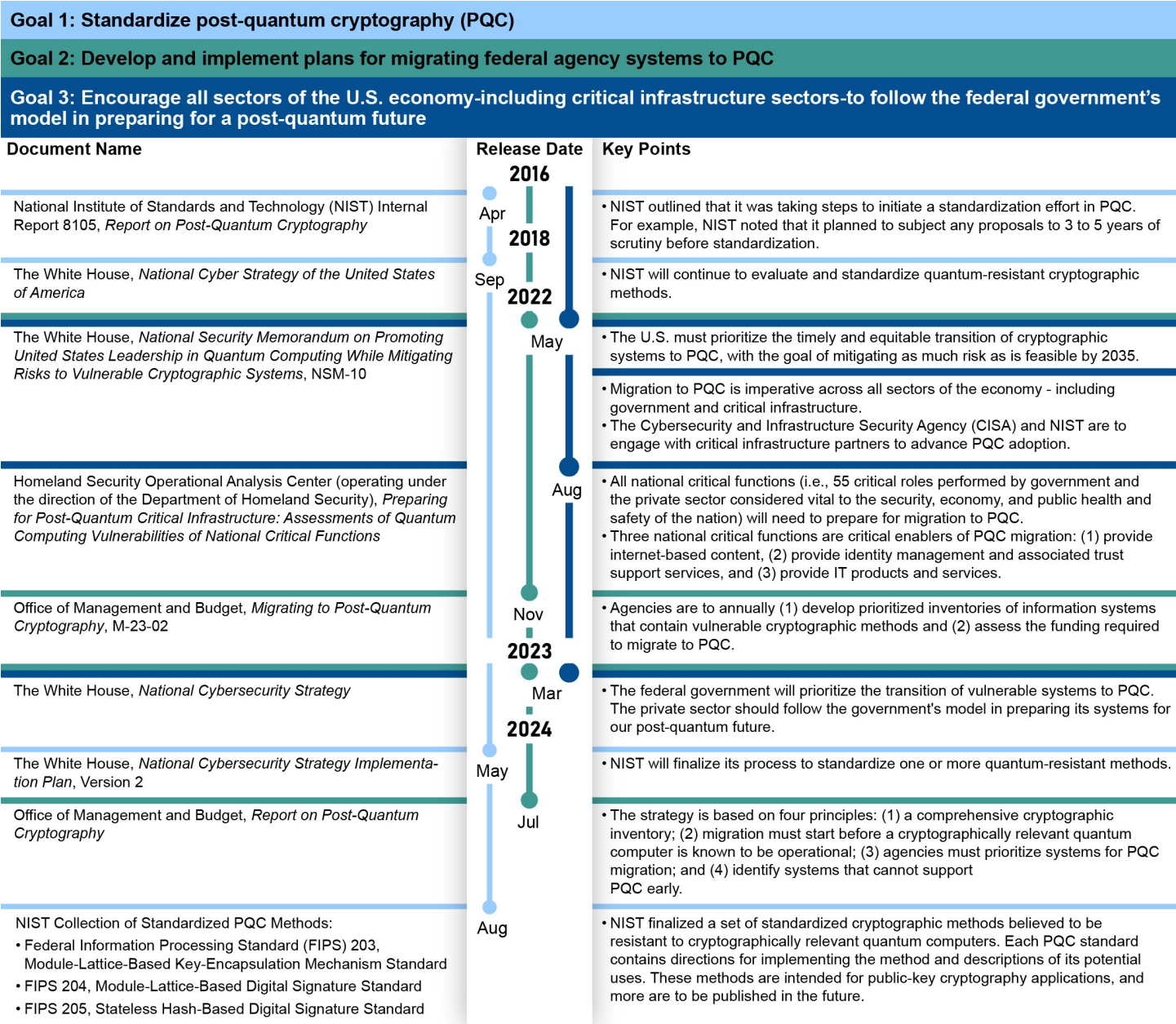


Sources: GAO analysis; narathip/stock.adobe.com (computer/key illustration); GAO (all other icons/illustrations). | GAO-25-108590

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

¹²[GAO-25-107703](#).

Figure 4: Central Goals Outlined in the Documents That Comprise the U.S. National Quantum Computing Cybersecurity Strategy



Source: GAO analysis of documents identified in the table. | GAO-25-108590

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 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 post-quantum cryptography are widely available.

Nevertheless, we reported that federal agencies have not fully defined a strategy for addressing the threat of quantum computers to our nation's cryptography.¹³ Specifically, the government's quantum computing cybersecurity strategy documents partially addressed the six key characteristics of a national strategy identified in our prior work.¹⁴ For example:

- **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 post-quantum cryptography (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.¹⁵ 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*

¹³[GAO-25-107703](#).

¹⁴[GAO-04-408T](#).

¹⁵Office 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.

on *Post-Quantum Cryptography* provided a cost estimate of \$7.1 billion to migrate priority federal agency systems to PQC between 2025 and 2035.¹⁶ 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 are 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.

No Single Federal Organization Is Responsible for the Strategy's Coordination

We reported that the key characteristics have not been fully addressed, in part, because no single federal organization was 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.¹⁷ 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.¹⁸ However, 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

¹⁶Office 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).

¹⁷Pub. 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.

¹⁸Office of Management and Budget, *Report on Post-Quantum Cryptography*.

January 2021, Congress established the Office of the National Cyber Director (ONCD) to provide cybersecurity leadership for the United States.¹⁹ The National Cyber Director heads the office and leads the coordination and implementation of national cyber policy and strategy.²⁰ 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.²¹

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.²² 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 key 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.

As a result, we made one recommendation to ONCD to (1) lead the coordination of the national quantum computing cybersecurity strategy and (2) ensure that the strategy's various documents address all the key characteristics of a national strategy. ONCD did not agree or disagree with the recommendation and it has not yet been implemented.

In conclusion, we have reported on options that policymakers could consider to help enhance benefits or mitigate drawbacks of quantum computing. In addition, federal agencies recognize and have taken some actions to partially address the quantum computing threat. Designating leadership committed to fully implementing key characteristics of a national quantum computing cybersecurity strategy is essential to ensure success. ONCD is well-positioned to fill this gap and provide a comprehensive roadmap for the transition to PQC.

Chairwoman Mace, Ranking Member Brown, and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Marisol Cain Cruz at CruzCainM@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

¹⁹6 U.S.C. § 1500(a) - (c).

²⁰6 U.S.C. § 1500(b) - (c).

²¹6 U.S.C. § 1500(c)(1)(G).

²²ONCD officials also highlighted the following organizations within the Executive Office of the President: the National Security Council, OMB, and Office of Science and Technology Policy.

GAO staff who made key contributions to this testimony include Kaelin Kuhn (Assistant Director), Sukhjoot Singh (Analyst-in-Charge), Chris Businsky, Nicole Catanzarite, Rebecca Eyler, Scott Fletcher, Jonah Guthrie, Karen Howard, Claire McLellan, Melissa Melvin, and Carlo Mozo.

Related GAO Products

Science and Technology Spotlight: Quantum Sensors. [GAO-25-107876](#). Washington, D.C.: January 7, 2025.

Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy. [GAO-25-107703](#). Washington, D.C.: November 21, 2024.

Quantum Technologies: Defense Laboratories Should Take Steps to Improve Workforce Planning. [GAO-24-106284](#). Washington, D.C.: December 5, 2023.

Science & Tech Spotlight: Securing Data for a Post-Quantum World. [GAO-23-106559](#). Washington, D.C.: March 8, 2023.

Information Environment: Opportunities and Threats to DOD's National Security Mission. [GAO-22-104714](#). Washington, D.C.: September 21, 2022.

Quantum Computing and Communications: Status and Prospects. [GAO-22-104422](#). Washington, D.C.: October 19, 2021.

Science & Tech Spotlight: Quantum Technologies. [GAO-20-527SP](#). Washington, D.C.: May 28, 2020.

Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas. [GAO-18-656](#). Washington, D.C.: September 26, 2018.

Letter

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.

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

A. Nicole Clowers, Managing Director, CongRel@gao.gov

Letter

General Inquiries

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