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

Standardize post-quantum cryptography   **Migrate federal systems**   **Encourage all sectors to prepare**
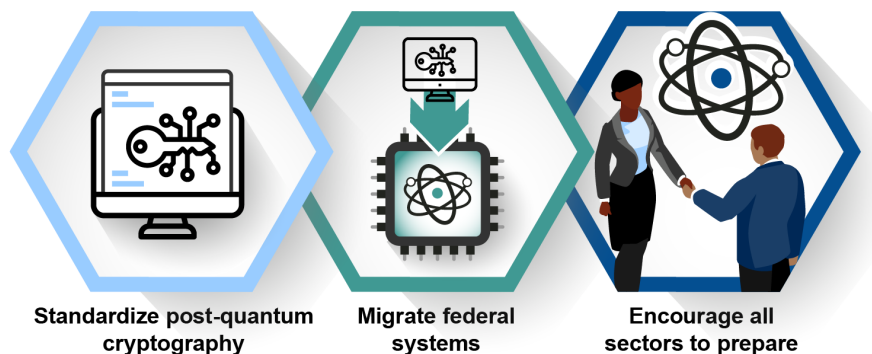
Sources: GAO analysis; narathip/stock.adobe.com (computer/key illustration); GAO (all other icons/illustrations). | GAO-25-108590

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.