

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 cruzcaim@gao.gov

What GAO Found

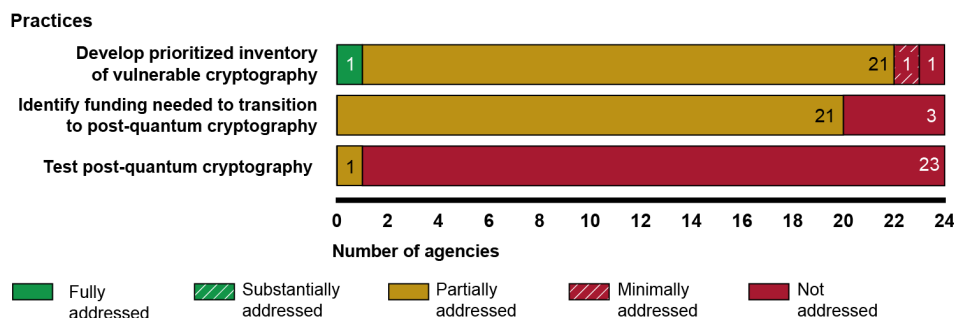
Quantum computers leverage qubits (the quantum equivalent of classical computer bits) to solve specific problems significantly faster than classical computers. However, the emergence of quantum computers could undermine the cryptography (e.g., encryption) that federal agencies use to secure their systems. 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. We worked with the Office of the National Cyber Director from September 2025 through September 2026 to prepare this version.

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.

We are not making any additional recommendations in this public version.