Calendar No. 635

117TH CONGRESS *2d Session*	SENATE	REPORT 117–251

QUANTUM COMPUTER CYBERSECURITY PREPAREDNESS ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 4592

TO ENCOURAGE THE MIGRATION OF FEDERAL GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS TO QUANTUM–RESISTANT CRYPTOGRAPHY, AND FOR OTHER PURPOSES

DECEMBER 13, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 635

117TH CONGRESS *2d Session* | SENATE | REPORT 117–251

QUANTUM COMPUTER CYBERSECURITY PREPAREDNESS ACT

DECEMBER 13, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 4592]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4592) to encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

Scientists and engineers have demonstrated that certain problems that are effectively impossible for conventional, classical computers to solve because of the length of time it would take, can be solved in exponentially less time on quantum computers.[1] As the

[1] In 2019 researchers demonstrated that a quantum computer was able to perform a function in 200 seconds, which would take a state-of-the-art classical supercomputer approximately 10,000 years. F. Arute et al., *Quantum supremacy using a programmable superconducting processor*, Nature (Oct. 23, 2019); California Institute of Technology, *What Is Quantum Computing?*

Continued

technology to develop practical quantum computers continues to advance, experts expect the technology to raise challenges to current cryptography methods, putting existing encryption and data protection methods at risk.[2] S. 4592, the *Quantum Computer Cybersecurity Act*, is based on President Biden's National Security Memorandum addressing "risks posed by quantum computers to America's cybersecurity." The bill requires the Director of the Office of Management and Budget (OMB) and federal agencies to take actions to address these challenges and protect federal data and information systems.

II. BACKGROUND AND NEED FOR THE LEGISLATION

Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers, which rely on classical physics principles.[3] This foundational difference in computing method enables quantum computers to make certain highly complex calculations far more efficiently than classical computers. The continuing advancements of quantum computing technology is anticipated to have wide-ranging applications, including in artificial intelligence, cybersecurity, biological engineering, financial services, including the ability to break current cryptographic systems.[4]

The threat of quantum computing to current encryption schemes today is minimal, but the future risks are not hypothetical—since 1994 scientists have predicted that quantum computers would be able to crack existing encryption schemes.[5] The National Institute of Standards and Technology (NIST) began work in 2016 to identify "quantum-resistant" encryption algorithms, meaning they would be less susceptible to a quantum computer's attack, and announced in July 2022 the first four algorithms that met such a standard.[6]

In May 2022, President Biden signed a quantum computing National Security Memorandum recognizing this threat by identifying "key steps needed to maintain the Nation's competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national

---

(accessed Dec. 6, 2022) (https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers).

[2] California Institute of Technology, *How Will Quantum Technologies Change Cryptography?* (accessed Dec. 6, 2022) (https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography).

[3] IBM, *What is quantum computing?* (accessed Dec. 6, 2022) (https://www.ibm.com/topics/quantum-computing).

[4] *Quantum Computing is Coming. What Can it Do?*, Harvard Business Review, (July 16, 2021) (https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do); California Institute of Technology, *What Is Quantum Computing?* (accessed Dec. 6, 2022) (https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers); California Institute of Technology, *How Will Quantum Technologies Change Cryptography?* (accessed Dec. 6, 2022) (https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography); U.S. Department of Energy, Office of Science, *DOE Explains Quantum Computing* (accessed Dec. 6, 2022) (https://www.energy.gov/science/doe-explainsquantum-computing).

[5] *Worried that quantum computers will supercharge hacking, White House calls for encryption shift*, American Association for the Advancement of Science, (May 5, 2022) (https://www.science.org/content/article/worried-quantum-computers-will-supercharge-hacking-white-house-calls-encryption-shift); *Quantum computers could crack today's encrypted messages. That's a problem*, CNET (May 24, 2021) (https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem).

[6] National Institute of Standards and Technology: *NIST Asks Public to Help Future-Proof Electronic Information* (Dec. 20, 2016); National Institute of Standards and Technology: *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms* (Jul. 5, 2022).

security."[7] The NSM requires a number of actions for agencies to take to migrate information systems to quantum-resistant cryptography, in anticipation of those systems becoming vulnerable as quantum computing technology continues to advance.[8]

S. 4592, the *Quantum Computer Cybersecurity Act*, codifies the NSM and requires Director of OMB and the heads of federal agencies to prepare for the migration of systems to quantum-resistant encryption. The bill requires agencies to inventory their information technology systems and prioritize which systems need to be migrated to quantum-resistant encryption systems. The bill also requires the Director of OMB to submit a report to Congress on strategies to address the vulnerabilities of agency information technology systems based on the potential capabilities of quantum computers, including an estimate of the necessary funding to secure those systems and a description of federal coordination efforts to develop standards for quantum resistant cryptography.

III. LEGISLATIVE HISTORY

Senators Hassan (D–NH) and Portman (R–OH) introduced S. 4592, the *Quantum Computer Cybersecurity Preparedness Act*, on July 21, 2022. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 4592 at a business meeting on August 3, 2022. There were no proposed amendments to the bill. The Committee ordered the bill to be reported favorably by voice vote *en bloc*. Senators present for the voter were: Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Lankford, Romney, Scott, and Hawley.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the name of the bill as the "Quantum Computer Cybersecurity Preparedness Act."

Section 2. Findings; sense of Congress

This section details the findings made by Congress on the potential applications of quantum computers and cryptography. It states that quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

It also states that the rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

Based on these findings, it is the sense of Congress that a strategy to transition information technology into a model of post-quantum cryptography is needed.

---

[7] The White House, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (NSM–10) (May 4, 2022).

[8] *Id.*

Section 3. Definitions

This section defines the terms "classical computer," "Director of CISA," "Director of NIST," "Director of OMB," "executive agency," "information technology," "post-quantum cryptography," and "quantum computer."

Section 4. Inventory of cryptography systems; migration to post-quantum cryptography

Subsection (a) mandates the Director of OMB to require each executive agency to establish and maintain an inventory of each cryptographic system in use by the agency. The requirement by the Director of OMB will be made by rule or binding guidance and must include the following: a description of information technology to be prioritized for migration to post-quantum cryptography, a description of the information required to be reported, and a process for evaluating progress on migrating information technology to post-quantum cryptography. This subsection also grants the Director of OMB with the ability to update the rule or binding guidance as they see fit.

Subsection (b) requires each executive agency to provide an inventory of all information technology in use by the executive agency that is vulnerable to decryption by quantum computers. This inventory report must be provided to the Director of OMB, the Director of CISA, and the National Cyber Director no later than 1 year after the enactment of S. 4592.

Subsection (c) requires the Director of OMB to issue guidance requiring executive agencies to a plan to transition its information technology to post-quantum cryptography. This subsection also directs OMB to issue guidance on which information technologies to prioritize based on their risk and potential to be decrypted by quantum computers.

Subsection (d) requires the Director of OMB to ensure that the designation and prioritizations of specific information technologies are interoperable.

Subsection (e) requires the Director of OMB to submit a report to Congress detailing a strategy to address vulnerabilities within the encryptions of information technologies and their ability to defend against potential breaches from quantum computers. The report must also include an estimate on the necessary funding for executive agencies to develop their defenses and a description of Federal civilian executive coordination efforts.

Subsection (f) requires the Director of OMB to submit a progress report to Congress on the improvements made within executive agencies in adopting post-quantum cryptography standards.

Section 5. Determination of budget effects

This section states that the budgetary effects of this Act will be determined by reference to statement titled "Budgetary Effects of PAYGO Legislation".

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will

have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 16, 2022.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 4592, the Quantum Computing Cybersecurity Preparedness Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 4592, Quantum Computing Cybersecurity Preparedness Act
As ordered reported by the Senate Committee on Homeland Security and Governmental on August 3, 2022

By Fiscal Year, Millions of Dollars	2022	2022-2027	2022-2032
Direct Spending (Outlays)	*	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	*	1	not estimated

Statutory pay-as-you-go procedures apply?	Yes	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2033?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

Quantum computers use advanced algorithms and subatomic particles to process complex problems significantly faster than traditional computers. While still in the early stages of development, quantum computers could allow malicious actors to decrypt classified information stored on federal networks. S. 4592 would require federal agencies to compile inventories of information systems that could be vulnerable to decryption by quantum computers. The bill also would require the Office of Management and Budget to issue guidance to agencies on the adoption of technology that is protected from decryption by quantum computing and to report to the Congress on the effectiveness of its efforts.

National Security Memorandum 10, Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, issued on May 4, 2022, requires federal agencies to prepare for the future risks of quantum decryption. Thus, because most of the planning required under S. 4592 will be completed under current law, CBO expects that satisfying those requirements would not have significant costs. On the basis of similar reports to the Congress, CBO estimates that satisfying the reporting requirements would cost $1 million over the 2022–2027 period. Such spending would be subject to the availability of appropriated funds.

Enacting S. 4592 could affect direct spending by some agencies that use fees, receipts from the sale of goods, and other collections to cover operating costs. CBO estimates that any net changes in direct spending would be negligible because most of those agencies can adjust amounts collected to accommodate changes in operating costs.

On June 7, 2022, CBO transmitted a cost estimate for H.R. 7535, the Quantum Computing Cybersecurity Preparedness Act, as ordered reported by the House Committee on Oversight and Reform on May 11, 2022. The two bills are similar, and CBO's estimates of their costs are the same.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.

○