U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Comptroller General
of the United States

September 2, 2025

The Honorable Sean Cairncross
Director
Office of the National Cyber Director
1600 Pennsylvania Ave NW
Washington, DC 20500

Priority Open Recommendations: Office of the National Cyber Director (ONCD)

Dear Director Cairncross:

Congratulations on your appointment. The purpose of this letter is to call your personal attention to three open priority recommendations from GAO's past work, which are enclosed.[1] Additionally, there is one other open GAO recommendation that we will continue to work with your staff to address.[2]

We are highlighting the following area that warrants your timely and focused attention:

Improving national cybersecurity strategies. ONCD needs to take additional steps to improve various national strategies pertaining to cybersecurity. In March 2023, the White House publicly issued a new National Cybersecurity Strategy, and subsequently published the accompanying implementation plan in July 2023.[3] Additionally, ONCD, along with several other federal entities, issued various documents contributing to an emerging national quantum cybersecurity strategy. However, we previously reported that the National Cybersecurity Strategy, including the National Cybersecurity Strategy Implementation Plan,[4] and the quantum

[1]GAO considers a recommendation to be a priority if when implemented, it may significantly improve government operations, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue.

[2]GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*. GAO-23-105468. (Washington, D.C.: September 26, 2023). We recommended that ONCD should identify outcome-oriented performance measures for the eight cyber threat information sharing initiatives that are included in the National Cybersecurity Strategy Implementation Plan.

[3]The White House, National Cybersecurity Strategy, (Washington, D.C.: Mar. 2023) and National Cybersecurity Strategy Implementation Plan (Washington, D.C.: July 2023).

[4]GAO, *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*. GAO-24-106916. (Washington, D.C.: Feb. 1, 2024).

cybersecurity documentation do not meet all the desirable characteristics of a national strategy.[5] These desirable characteristics include, among others: (1) the purpose, scope, and methodology of the strategy, addressing why the strategy was produced, the scope of its coverage, and the process by which it was developed; (2) a problem definition and risk assessment, including the national problems and threats the strategy is directed toward and an analysis of threats to and vulnerabilities of critical assets and operations; and (3) goals, subordinate objectives, activities, and performance measures, specifying what the strategy is trying to achieve, steps toward achieving those results, and how those results will be gauged.

To address this, ONCD should (1) develop performance measures to gauge effectiveness in meeting the goals and objectives of the National Cybersecurity Strategy, (2) assess initiatives from the strategy to identify those that warrant a cost estimate and develop such cost estimates, and (3) lead the coordination of a national quantum computing cybersecurity strategy that addresses all the desirable characteristics of a national strategy. By fully implementing these recommendations, ONCD can more effectively carry out its leadership responsibilities needed to ensure the cybersecurity of the nation.

ONCD plays a critical role in leading coordination efforts to face cybersecurity challenges. These challenges are long-standing. Ensuring the Cybersecurity of the Nation first appeared as a government-wide area on GAO's High Risk List as information security in 1997. We expanded this high-risk area in 2003 to include protecting the cybersecurity of critical infrastructure. In 2015, we expanded it again to include protecting the privacy of personally identifiable information.

In June 2024, we identified urgent actions needed to address cybersecurity challenges facing the nation.[6] For example, these actions include developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace and improving federal efforts to protect privacy and sensitive data. Since 2010, we have made 4,310 recommendations to address cybersecurity weaknesses, of which, as of August 2025, 515 remain open. We are continuing to work with agencies across the government, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, to monitor the implementation of these recommendations. Further, ONCD plays a critical role in addressing these weaknesses in light of its congressionally established mandate to facilitate the high-level attention and coordination needed to address cyber threats and challenges facing the nation.

Please see Enclosure 1 for additional details about the status and actions needed to fully implement all three open priority recommendations.

We also list in Enclosure 2 additional relevant management challenges from our High-Risk List that apply to ONCD. In response to legislation enacted in December 2022, this enclosure also includes information on additional congressional oversight actions that can help agencies

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

[6]GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation.* GAO-24-107231. (Washington, D.C.: Jun. 13, 2024).

implement priority recommendations and address any underlying issues relating to such implementation.

Copies of this letter are being sent to the appropriate congressional committees. The letter will also be available on the GAO website at Priority Open Recommendation Letters | U.S. GAO.

If you have any questions or would like to discuss any of the issues outlined in this letter, please do not hesitate to contact me or Nicholas H. Marinos, Managing Director, Information Technology and Cybersecurity, at marinosn@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this letter. Our teams will continue to coordinate with your staff on addressing these open recommendations. I appreciate ONCD's continued commitment and thank you for your personal attention to these important issues.

Sincerely,

//SIGNED//

Gene L. Dodaro
Comptroller General
of the United States

Enclosures - 2

cc: Dr. Madhu Gottumukkala, Acting Director of the Cybersecurity & Infrastructure Security Agency

Enclosure 1

Priority Open Recommendations to the Office of the National Cyber Director (ONCD)

Improving National Cybersecurity Strategies

Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy. GAO-24-106916. Washington, D.C.: February 1, 2024.

Year Recommendations Made: 2024

Recommendation: The Director of ONCD should work with relevant federal entities to assess the initiatives from the National Cybersecurity Strategy that lend themselves to outcome-oriented performance measures and develop such performance measures for those initiatives in a timely manner to gauge effectiveness in meeting the goals and objectives of the National Cybersecurity Strategy.

Actions Needed: ONCD partially agreed with this recommendation. In August 2025, ONCD officials told us that the office is in the process of developing and incorporating outcome-oriented performance measures for future iterations of the National Cybersecurity Strategy Implementation Plan. Further, the officials said they are working with the relevant federal entities that are responsible for implementing the implementation plan's initiatives to refine these performance measures in 2025 and intend to include the measures in the 2026 update to the implementation plan.

To fully address the recommendation, ONCD should continue to work with relevant federal entities to develop the outcome-oriented performance measures for the initiatives that lend themselves to such measures and incorporate them into the National Cybersecurity Strategy Implementation Plan. Until ONCD does so, it will be limited in its ability to demonstrate the effectiveness of the strategy in meeting its goals of better securing cyberspace and the nation's critical infrastructure.

Recommendation: The Director of ONCD should work with relevant federal entities to assess the initiatives from the National Cybersecurity Strategy to identify those that warrant a cost estimate and develop such cost estimates.

Actions Needed: ONCD disagreed with this recommendation. ONCD stated that the Office of Management and Budget's (OMB) guidance restricts agencies from disclosing future year budget plans outside of the current budget cycle, thereby preventing ONCD from providing details such as cost estimates of the initiatives. ONCD also referenced a joint memorandum it issued with OMB that identified the cybersecurity budget priorities to help agencies align their budgets with the priorities in the strategy and implementation plan.

We acknowledge the value of ONCD and OMB providing guidance on cybersecurity budget priorities through their joint memorandum. Further, we agree that this guidance is a good step toward assisting agencies in determining how much it will cost to implement their respective initiatives. However, we continue to maintain that developing a specific cost estimate is essential to effectively managing programs. Without such information, uncertainty can emerge about investing in programs.

As of August 2025, ONCD continued to disagree with this recommendation and had not provided updates on its actions. To fully address this recommendation, ONCD should identify the initiatives that warrant cost estimates, coordinate with the relevant federal agencies, and document any associated cost estimates to inform future planning. Implementing this recommendation would help ONCD be confident that adequate resources are available to support implementing the National Cybersecurity Strategy.

High-Risk Area: Ensuring the Cybersecurity of the Nation and Improving IT Acquisitions and Operations

Director: Marisol Cruz Cain, Information Technology and Cybersecurity

Contact Information: CruzCainM@gao.gov

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

Year Recommendation Made: 2025

Recommendation: 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.

Actions Needed: ONCD did not agree or disagree with the recommendation. In August 2025, ONCD officials told us that they did not have any comments for us at that time. They stated that they are open to the recommendation, but it ultimately depends on the concurrence of the new Director of the office.

While we understand that new leadership will have different priorities from prior National Cyber Directors, a national quantum computing strategy will assist the federal government in addressing the threat that quantum computers pose to cryptography on unclassified systems. It will also avoid putting agency and critical infrastructure systems that rely on cryptography for security at risk. ONCD is well-positioned to fill the gap in implementing desirable characteristics of a national strategy and provide a comprehensive roadmap for the transition to post-quantum cryptography.[7]

To fully address this recommendation, ONCD should take the lead in coordinating the development of a national quantum computing cybersecurity strategy that addresses the desirable characteristics of a national strategy.

High-Risk Area: Ensuring the Cybersecurity of the Nation

Director: Marisol Cruz Cain, Information Technology and Cybersecurity

Contact Information: CruzCainM@gao.gov

[7]Post-quantum cryptography refers to new cryptographic methods intended to withstand attacks from both quantum and conventional computers.

Enclosure 2

Key Information About the Status of GAO Recommendations and Improving Agency Operations

Recommendation Implementation Rate

In November 2024, we reported that, on a government-wide basis, 70 percent of our recommendations made 4 years ago were implemented.[8] As of August 2025, ONCD had four open recommendations.

High-Risk List

In February 2025, we issued our biennial update to our High-Risk List.[9] This list identifies government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement. It also identifies the need for transformation to address economy, efficiency, or effectiveness challenges.

In addition to Ensuring the Cybersecurity of the Nation, and Improving IT Acquisitions and Operations, we urge your continued attention to the other government-wide high-risk issues as they relate to the Office of the National Cyber Director (ONCD). Further, achieving meaningful progress on high-risk areas requires coordinated efforts across federal agencies. We have developed eight leading practices for effective interagency collaboration on shared goals, which could be a helpful resource as ONCD coordinates implementation of the nation's cybersecurity strategy.

Congress's Role on GAO Recommendations

We also recognize the key role Congress plays in providing oversight and maintaining focus on our recommendations to ensure they are implemented and produce their desired results. Legislation enacted in December 2022 includes a provision for GAO to identify any additional congressional oversight actions that can help agencies implement priority recommendations and address any underlying issues relating to such implementation.[10]

Congress can use various strategies to address our recommendations, such as incorporating them into legislation. Congress can also use its budget, appropriations, and oversight processes to incentivize executive branch agencies to act on our recommendations and monitor their progress. For example, Congress can hold hearings focused on ONCD's progress in

---

[8]GAO, *Performance and Accountability Report, Fiscal Year 2024*, GAO-25-900570 (Washington, D.C.: Nov. 15, 2024). Moving forward, GAO will use 5 years (instead of 4 years) to calculate the percentage of recommendations implemented.

[9]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

[10]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, § 7211(a)(2), 136 Stat. 2395, 3668 (2022); H.R. Rep. No. 117-389 (2022) (accompanying Legislative Branch Appropriations Act, H.R. 8237, 117th Cong. (2022)).

implementing GAO's priority recommendations, withhold funds when appropriate, or take other actions to provide incentives for agencies to act. Moreover, Congress can follow up during the appropriations process and request periodic updates.

Congress also plays a key role in addressing any underlying issues related to the implementation of these recommendations. For example, Congress can pass legislation providing an agency explicit authority to implement a recommendation or requiring an agency to take certain actions to implement a recommendation.