U.S. Government Accountability Office

September 2022

In 2021, Congress established the Office of the National Cyber Director to lead the nation's cybersecurity effort. This product summarizes the Office's initial strategic statement and its intentions regarding a national cybersecurity strategy.

Cybersecurity: Kick-Starting the Office of the National Cyber Director

Leadership Is Needed to Address Cybersecurity Threats and Challenges

Clearly defining a leadership role to coordinate the federal government's efforts to address the nation's cybersecurity threats and challenges is urgent and necessary. Accordingly, the Congress has designated a leadership position in the White House with the authority to implement and encourage action in support of the nation's cybersecurity.

Specifically, in January 2021, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President.[1] The act also created the position of the National Cyber Director to head the Office and serve as the principal advisor to the President on cybersecurity policy and strategy. In June 2021, the Senate confirmed a Director to lead the Office.

Three recently enacted laws added provisions affecting the Director and Office: (1) the Consolidated Appropriations Act, 2022 requires the Director to work with other agencies on cybersecurity;[2] (2) the National Defense Authorization Act for Fiscal Year 2022 establishes authority for the Director to accept detailees to support the Office;[3] and (3) the Infrastructure Investment and Jobs Act appropriated $21 million to the Office through September 30, 2022, to carry out statutory responsibilities.[4]

Moreover, we have identified challenges in federal cybersecurity for decades and first designated information security as a government-wide high-risk area in 1997.[5] Previously, in September 2020, we reported that the prior administration's *2018 National Cyber Strategy* and associated *2019 Implementation Plan* addressed some, but not all, of the desirable characteristics of national strategies. We recommended that the National Security Council work with relevant federal entities to update cybersecurity strategy documents.[6] As part of our ongoing high-risk work, we will continue to evaluate the administration's efforts to develop and implement a comprehensive national cybersecurity strategy.

Recent Efforts by the National Cyber Director

Since June 2021, the Director has outlined the initial strategic statement for the Office and has hired staff. The Office has also described its intentions regarding a national cybersecurity strategy.

Strategic Statement

In October 2021, the Director issued a strategic statement for the Office that summarized its vision, challenge, path, and urgency to improve the nation's cybersecurity.[7]

- **Vision:** the Office's goal is to engage in cyberspace such that digital connectivity unites the nation in an open, interoperable, secure, and reliable internet.
- **Challenge:** the Office was created to overcome challenges posed by cyberspace, such as nation-state actors and criminals stealing Americans' personal information due to social engineering in cyberspace.

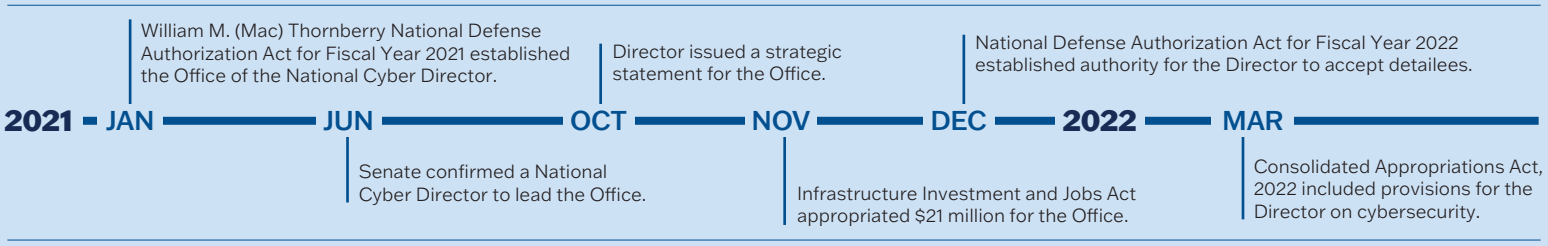
Table 1: Roles and Responsibilities of the National Cyber Director

Federal law	Roles and responsibilities
William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021	• Serve as the principal advisor to the President on cybersecurity policy and strategy. • Lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy by, among other things, o monitoring and assessing the effectiveness of the implementation of national cyber policy and strategy by federal departments and agencies, and o reviewing the annual budget proposals for relevant federal departments and agencies and advising their heads on whether those proposals are consistent with national cyber policy and strategy. • Annually report to Congress on cybersecurity threats and issues facing the United States.

Source: GAO analysis. | GAO-22-105502

[1] Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021).
[2] Pub. L. No. 117-103, Div. Y, §§ 103(a)(2), 106(a), 136 Stat. 49 (Mar. 15, 2022).
[3] Pub. L. No. 117-81, Div. A, Title XV, § 1552, 135 Stat. 1541, 2070 (Dec. 27, 2021).
[4] Pub. L. No. 117-58, Div. J, Title IV, 135 Stat. 429, 1381 (Nov. 15, 2021).
[5] See, for example, GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).
[6] GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).
[7] The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, D.C.: Oct. 28, 2021).

Figure 1: Timeline of Key Events Related to the Office of the National Cyber Director



Source: GAO analysis. | GAO-22-105502

- **Path:** the Office intends to execute the administration's cyber agenda through four outcomes: **ensure federal coherence** by pushing for common standards and practices used to build and operate the nation's digital infrastructures; **improve public-private collaboration** by tackling cyber challenges across sectors; **align resources to aspirations** by ensuring federal departments and agencies are held accountable for their cyber resources; and **increase present and future resilience** by ensuring the nation's workforce, technologies, and organizations are fit for purpose today and future-proofed for tomorrow.

  To achieve these four outcomes, the Office developed seven lines of effort:

  1) National cybersecurity: Protect and defend state, local, and private sector networks.
  2) Federal cybersecurity: Ensure the federal government serves as a model for the private sector actors to follow.
  3) Budget review and assessment: Partner with the Office of Management and Budget to support departments and agencies as they plan and budget their cyber resources.
  4) Technology and ecosystem security: Encourage collaboration between the public and private sectors to develop a more secure digital supply chain.
  5) Planning and incident response: Ensure a coordinated federal defense from and response to cyber incidents.
  6) Workforce development: Ensure public and private sectors benefit from inclusive pathways for cyber talent.
  7) Stakeholder engagement: Work with Congress and the private sector on cyber initiatives.

- **Urgency:** the Office notes that if threats to cyberspace are not addressed now, they will become more difficult to fix.

Staffing

As of August 2022, the Office reported that it had about 55 employees, which could grow to around 75 employees by the end of fiscal year 2022. One of the Director's key appointments was the deputy National Cyber Director for federal cybersecurity, who also serves within the Office of Management and Budget as the federal chief information security officer. According to the Director, the dual-hat role is intended to provide budget and cybersecurity expertise within the Office.[8]

Figure 2: Key Entities within the Executive Office of the President Responsible for Supporting the Nation's Cybersecurity

Source: GAO analysis. | GAO-22-105502

Status of a National Cybersecurity Strategy

As of August 2022, according to the Office, the development of a national cybersecurity strategy by the administration is well underway. The Office noted that it is obtaining feedback on the strategy from many other federal entities, including the National Security Council, on this effort. The federal government needs to fully develop and implement a comprehensive national strategy in order to have a clear roadmap for overcoming the cyber challenges facing our nation.

[8] E. Nakashima, "Biden's new cyber czar is pushing for collective defense inside government and out," *The Washington Post* (October 28, 2021).

Connect with GAO: https://www.gao.gov/about/contact-us/stay-connected.

A. Nicole Clowers, Managing Director, Congressional Relations, (202) 512-4400

Chuck Young, Managing Director, Public Affairs, (202) 512-4800

U.S. Government Accountability Office
441 G Street NW, Washington, DC 20548

We conducted our work from January 2022 to September 2022 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. 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.

For more information about this product, contact: Kevin Walsh, Director, Information Technology and Cybersecurity, (202) 512-6151

Staff acknowledgments: Kush Malhotra (Assistant Director), Umesh Thakkar (Analyst-in-charge), Lauri Barnes, Chris Businsky, Becca Eyler, Hiama Halay, Franklin Jackson, and Scott Pettis.

Cover photo source: Sono Creative/stock.adobe.com