U.S. Government Accountability Office

June 2023

Cybersecurity: Launching and Implementing the *National Cybersecurity Strategy*

In March 2023, the White House issued the *National Cybersecurity Strategy* to coordinate efforts to secure the nation against cyber risks and threats. This product summarizes the federal government's efforts to implement the strategy.

Threats Highlight the Importance of Establishing Leadership in Cybersecurity

Federal agencies and our nation's critical infrastructure—such as energy, communications, and financial services—depend on technology systems to carry out fundamental operations and to process, maintain, and report vital information. However, malicious actors are becoming more capable of carrying out cyberattacks, threatening the continuity and integrity of these essential systems. We designated information security as a government-wide high-risk area in 1997 and subsequently expanded it to include the protection of cyber critical infrastructure and the privacy of personally identifiable information.

Coordinating the federal government's efforts to address the nation's cybersecurity threats and challenges is urgent and necessary. In September 2020, we reported that the 2018 *National Cyber Strategy* and its 2019 *Implementation Plan* did not address all the desirable characteristics of national strategies (e.g., resources, investments, and risk management).[1] It was also unclear which official was responsible for coordinating execution of the *Implementation Plan*. We recommended that the National Security Council update strategy documents to better reflect desirable characteristics of national strategies. We also recommended that Congress consider legislation to designate a leadership position in the White House to support the nation's cyber critical infrastructure, including implementing the *Cyber Strategy*.

The fiscal year 2021 national defense authorization act established the Office of the National Cyber Director (ONCD) within the Executive Office of the President.[2] The Senate confirmed a National Cyber Director in June 2021 to serve as the principal advisor to the President on cybersecurity policy and strategy. However, this official resigned from the position in February 2023. In March 2023, the White House issued the *National Cybersecurity Strategy*, outlining how the administration will manage the nation's cybersecurity through five pillars.[3] The pillars focus on, among other things, securing cyber critical infrastructure and disrupting cyber threat actors.

The Administration Needs to Fully Develop and Implement the *National Cybersecurity Strategy*

In April 2023, we reported that the goals and strategic objectives included in the strategy provide a good foundation for establishing a more comprehensive

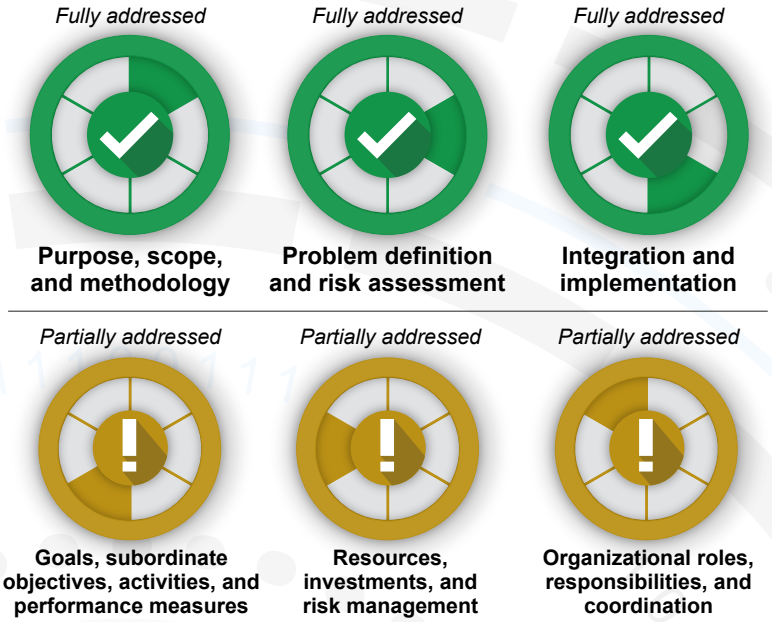
Figure 1. Five Pillars of the *National Cybersecurity Strategy*

Sources: GAO analysis of the *National Cybersecurity Strategy*; marinashevchenko/stock.adobe.com (icons). | GAO-23-106826

[1] GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).
[2] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752(a), 134 Stat. 3388, 4144 (2021).
[3] The White House, *National Cybersecurity Strategy*. (Washington, D.C.: Mar. 1, 2023).

strategy. However, not all of the desirable characteristics of national strategies were addressed.[4]

Figure 2: Extent to Which the *National Cybersecurity Strategy* Addresses the Desirable Characteristics of a National Strategy



Source: GAO (analysis and icons). | GAO-23-106826

- **Goals, subordinate objectives, activities, and performance measures.** The strategy identifies strategic objectives and articulates priorities, such as establishing cybersecurity requirements for critical sectors. However, it does not include specific milestones or performance measures.
- **Resources, investments, and risk management.** The strategy identifies investments for four of the five pillars. However, it does not address cost and does not identify where resources and investments should be targeted.
- **Organizational roles, responsibilities, and coordination.** While the strategy identifies federal roles and responsibilities for many implementation activities, in other instances, defining the federal role is an ongoing activity. For example, in response to our recommendations, agencies are currently assessing the extent to which a federal role and insurance response is necessary in the event of a catastrophic cyber event.

According to the strategy, ONCD will work with federal agencies to develop a plan specifying the lines of effort to implement the strategy and identify budget priorities, among other things. ONCD intends to issue the implementation plan soon. Until the federal government issues the implementation plan and ensures its strategy documents fully address the desirable characteristics of a national strategy, the nation will lack a clear roadmap for overcoming its cyber challenges.

Opportunities

A strategy and a future implementation plan can help the federal government address the four major cybersecurity challenges we previously identified:

- **Establish and implement a comprehensive cybersecurity strategy and perform effective oversight.** The strategy articulates goals and strategic objectives for a more coordinated approach to address the nation's cybersecurity challenges.
- **Secure federal systems and information.** The strategy identifies steps and priorities to mitigate cybersecurity risks in federal systems.
- **Protect cyber critical infrastructure.** The strategy identifies investment priorities to defend critical infrastructure against cyber threats.
- **Protect privacy and sensitive data.** The strategy identifies the need for increased investments in privacy-preserving technology.

Challenges

- **Timely issuance of the implementation plan.** As previously mentioned, ONCD plans to specify details on the implementation of key activities (e.g., performance measures, needed resources, and roles and responsibilities). It is critical that these details be issued expeditiously so agencies can begin planning and allocating resources to properly execute the strategy.
- **Vacant National Cyber Director position.** The National Cyber Director resigned in February 2023 and a replacement has not yet been named. As of June 2023, an acting official continues to carry out the duties. This vacancy leaves unfilled a key leadership role needed to coordinate the federal efforts to address cybersecurity threats and challenges. Further, sustained leadership in this position is essential to ensuring strategy execution and accountability.

[4]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

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 May 2023 to June 2023 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: Marisol Cruz Cain, Director, Information Technology and Cybersecurity, (202) 512-5017

Staff acknowledgments: Lee McCracken (Assistant Director), Keith Kim (Analyst-in-charge), Destin Hinkel, Ashley Mattson, Lauri Barnes, and Chris Businsky.

Cover photo source: KanawatTH/stock.adobe.com