United States Government Accountability Office

Report to Congressional Addressees

February 2024

CYBERSECURITY

National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy

GAO-24-106916

GAO Highlights

Highlights of GAO-24-106916, a report to congressional addressees

February 2024

CYBERSECURITY

National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy

Why GAO Did This Study

For over 25 years GAO has identified cybersecurity as a high-risk area. During this period, the threat of cyber-based intrusions and attacks on IT systems by malicious actors has continued to grow.

A national strategy to guide the government's cybersecurity activities is needed to address this threat. Recognizing the need for national cybersecurity leadership, Congress established ONCD to support the nation's cybersecurity and lead the development of a national strategy. In March 2023, the White House issued the *National Cybersecurity Strategy* to outline how the administration will manage the nation's cybersecurity. In July 2023, ONCD issued an implementation plan defining how the strategy will be executed.

GAO's objective was to examine the extent to which the *National Cybersecurity Strategy* and implementation plan addressed desirable characteristics of a national strategy. To do so, GAO assessed relevant documents and other evidence against desirable characteristics of a national strategy. GAO also interviewed ONCD staff.

What GAO Recommends

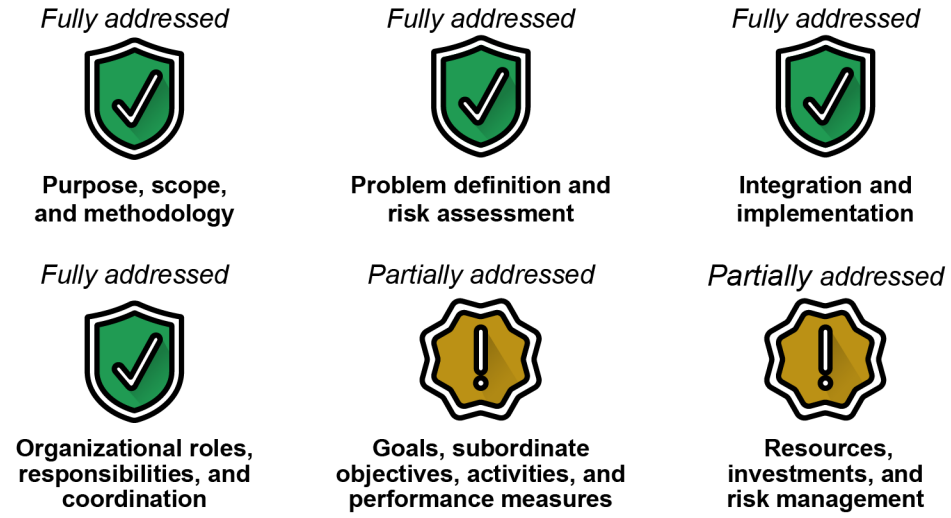
GAO is making two recommendations to ONCD to develop outcome-oriented measures and estimate costs of implementation activities. ONCD agreed with GAO's recommendation on outcome-oriented measures but disagreed with the recommendation on estimating costs. GAO continues to believe that ONCD should assess the plan's initiatives to identify those that warrant a cost estimate and develop such cost estimates.

View GAO-24-106916. For more information, contact Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov

What GAO Found

The *National Cybersecurity Strategy* and its implementation plan jointly addressed four of six desirable characteristics identified in prior GAO work and partially addressed the other two (see figure).

Extent to Which the March 2023 *National Cybersecurity Strategy* and July 2023 Implementation Plan Addressed GAO's Desirable Characteristics of a National Strategy



Source: GAO analysis and icon; yevheniia/stock.adobe.com (icons). | GAO-24-106916

For the partially addressed characteristics, the documents did not fully describe:

- *Outcome-oriented performance measures.* Office of the National Cyber Director (ONCD) staff said it was not realistic to develop outcome-oriented measures at this point. However, GAO believes it is feasible to develop such measures where applicable. For example, regarding the key initiative of disrupting ransomware attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value was about $886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness.
- *Resources and estimated costs.* While the implementation plan outlined initiatives that require executive visibility and interagency coordination, it did not identify how much it will cost to implement the initiatives. ONCD staff said estimating the cost to implement the entire strategy was unrealistic. However, while certain initiatives may not warrant a specific cost estimate, other activities supporting some of the key initiatives with potentially significant costs justify the development of a cost estimate. Such cost estimates are essential to effectively managing programs. Without such information, uncertainty can emerge about investing in programs.

Without actions to address these shortcomings, ONCD will likely lack information on plan outcomes and encounter uncertainty on funding of activities.

Contents

Abbreviations

OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 1, 2024

Congressional Addressees

Our nation continues to depend on computer-based information systems and electronic data to execute fundamental operations and to process, maintain, and report crucial information. Nearly all federal and nonfederal operations, including the nation's critical infrastructure, are supported by such information systems and electronic data.[1] Therefore, it would be difficult, if not impossible, for federal and nonfederal entities to carry out their missions and account for their resources without these information assets. Hence, the safety of these systems and data is critical to public confidence and the nation's security, success, and welfare.

However, cyber-based intrusions and attacks on both federal and nonfederal systems by malicious actors are becoming more common and more disruptive. These attacks threaten the continuity, confidence, integrity, and accountability of these essential systems. Moreover, the risks to these systems—including insider threats from witting or unwitting employees, mounting threats from around the globe, and the rise of new and more destructive attacks—collectively threaten to compromise sensitive data and destabilize critical operations.

Recognizing the growing threat, we have designated information security as a government-wide high-risk area since 1997. Subsequently in 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded this high-risk area in 2015 to include protecting the privacy of personally identifiable information.[2] In our most recent update on this high-risk area in April 2023, we continued to report that fully establishing and

[1]The term "critical infrastructure" as defined in the Critical Infrastructures Protection Act of 2001 refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2]In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual.

implementing a national cybersecurity strategy is needed to protect our information systems and infrastructure.[3]

We performed this work under the authority of the Comptroller General to conduct a review of the administration's recently issued national cybersecurity strategy to assist Congress with its oversight responsibilities. Specifically, our objective was to examine the extent to which the *National Cybersecurity Strategy* and accompanying implementation plan[4] addressed the desirable characteristics of a national strategy.

To address this objective, we assessed the March 2023 *National Cybersecurity Strategy* and its accompanying implementation plan against the desirable characteristics of a national strategy, as identified in prior GAO work.[5] In particular, we reviewed the documents and compared them to the following desirable characteristics:

- purpose, scope, methodology;
- problem definition and risk assessment;
- goals, subordinate objectives, activities, and performance measures;
- resources, investments, and risk management;
- organizational roles, responsibilities, and coordination; and
- integration and implementation.

We also interviewed relevant Office of the National Cyber Director (ONCD) staff to discuss the strategy and implementation plan, explain the desirable characteristics we were assessing the strategy and plan against, and obtain necessary additional information.

Based on our assessment, we determined whether the *National Cybersecurity Strategy* and implementation plan addressed the desirable characteristics of a national strategy as:

[3]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).

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

[5]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

- fully addressed, if available evidence demonstrated all aspects of the selected characteristic;
- partially addressed, if available evidence demonstrated some, but not all, aspects of the selected characteristic; and
- not addressed, if available evidence did not demonstrate any aspects of the selected characteristic.

Additional details on our objective, scope, and methodology can be found in appendix I.

We conducted this performance audit from June 2023 to February 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Enterprise IT systems and operational technology systems supporting federal agencies and our nation's critical infrastructures are inherently at risk because they are highly complex and dynamic, technologically diverse, and often geographically dispersed.[6] This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including via the internet. This increases the number of avenues for attack and expands their attack surface. As systems become more integrated, cyber threats pose an increasing risk to national security, economic wellbeing, and public health and safety.

Cybersecurity Incidents Continue to Affect Federal and Nonfederal Systems

Cybersecurity incidents continue to pose a serious challenge to economic, national, and personal privacy and security. In 2023, the Office of Management and Budget (OMB) reported that, for fiscal year 2022, common types of information security incidents were improper usage,

[6]Enterprise IT systems encompass traditional IT computing and communications hardware and software components that may be connected to the internet. Operational technology systems monitor and control sensitive processes and physical functions, such as offshore oil and gas operations.

email/phishing,[7] web attacks, and loss or theft of equipment.[8] Separately, in its 2023 annual data breach investigations report, Verizon reported analyzing 16,312 security incidents.[9] Of these incidents, 5,199 were confirmed data breaches. Further, according to the report, the three primary ways in which an attacker accessed an organization were stolen credentials, phishing, and exploitation of vulnerabilities. The following examples highlight the impact of such incidents in both the public and private sector:

- In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyberattack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. According to a joint advisory released by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, the company proactively disconnected certain pipeline operational technology systems to ensure the safety of the pipeline.[10] This resulted in a temporary halt to all pipeline operations, which led to gasoline shortages throughout the southeast United States.
- The Department of Education reported a major incident involving the breach of personally identifiable information involving a loan servicing vendor's system. Beginning in June of 2022, a nonstate criminal actor began attacking a web application, leveraging a vulnerability on a vendor-operated loan registration website. The attacker maintained a presence on the system until July 2022 when the activity was detected, and the system was immediately shut down. Following the incident, the vendor took mitigating steps to better secure its systems through implementation of additional user validations and penetration

[7]Phishing is a digital form of social engineering in which adversaries send hyperlinks in authentic-looking, but fake, emails to direct users to fake websites that download malware onto users' networks and collect sensitive information from users. Malware is malicious software intended to perform an unauthorized process that will have an adverse effect on the confidentiality, integrity, or availability of an information system. Examples of sensitive information are usernames and passwords.

[8]OMB, *Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2022* (Washington, D.C.: May 1, 2023). According to OMB, the highest number of reported incidents fell into the "Other/Unknown" vector category. The "Other/Unknown" vector represented an attack method that does not fit into any other vector or the cause of attack is unidentified.

[9]Verizon, *2023 Data Breach Investigation Report* (Basking Ridge, N.J.: June 6, 2023).

[10] Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Alert AA21-131A (Washington, D.C.: May 11, 2021).

testing exercises. Notification and credit monitoring services were offered to potentially affected individuals.

The Office of the National Cyber Director Was Established to Provide Cybersecurity Leadership

During the last several administrations, expert commissions have consistently highlighted the importance of central leadership to overcome cyber threats to the nation and have made related recommendations to establish clear roles and responsibilities for a leadership position. For example:

- In December 2008, the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency issued a report that stressed the need to lead cybersecurity from the White House and proposed creating a new office for cyberspace in the Executive Office of the President.[11]
- In December 2016, the Commission on Enhancing National Cybersecurity recommended that the federal government better match cybersecurity responsibilities with the structure of, and positions in, the Executive Office of the President.[12] It stressed that effective implementation of cybersecurity priorities would require strong leadership, beginning at the top, and that agencies must receive clear direction from the President and be granted corresponding authorities.
- In March 2020, the Cyberspace Solarium Commission issued its final report, which addressed the strategic approach needed to defend the nation against cyberattacks, and the policies and legislation needed to implement that strategy.[13] The Solarium Commission recommended that Congress establish a National Cyber Director within the Executive Office of the President, who would be Senate-confirmed and would be supported by their office.

[11]Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency* (Washington, D.C.: December 2008).

[12]Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Washington, D.C.: Dec. 1, 2016).

[13]The John S. McCain National Defense Authorization Act for Fiscal Year 2019 established the Cyberspace Solarium Commission, a federal commission made up of members of Congress, appointees selected by congressional officials, and designees from the Office of the Director of National Intelligence, Department of Homeland Security, Department of Defense, and the Federal Bureau of Investigation. Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018).

Recognizing the urgency and necessity of clearly defining a national cybersecurity leadership role, Congress established an office and 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 ONCD within the Executive Office of the President.[14] The act created the position of the National Cyber Director to head the office and gave the director the following roles and responsibilities, among others:

- 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,
  - monitoring and assessing, in coordination with the heads of relevant federal departments and agencies, the effectiveness of the implementation of national cyber policy and strategy by federal departments and agencies; and
  - 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.

In June 2021, the Senate confirmed a director to lead the office; however, this official resigned from the position in February 2023. From February 2023 to December 2023, the office was led by an acting director. In December 2023, the Senate confirmed the President's nomination of a new individual to serve as the new National Cyber Director.

[14]Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021), codified at 6 U.S.C. § 1500.

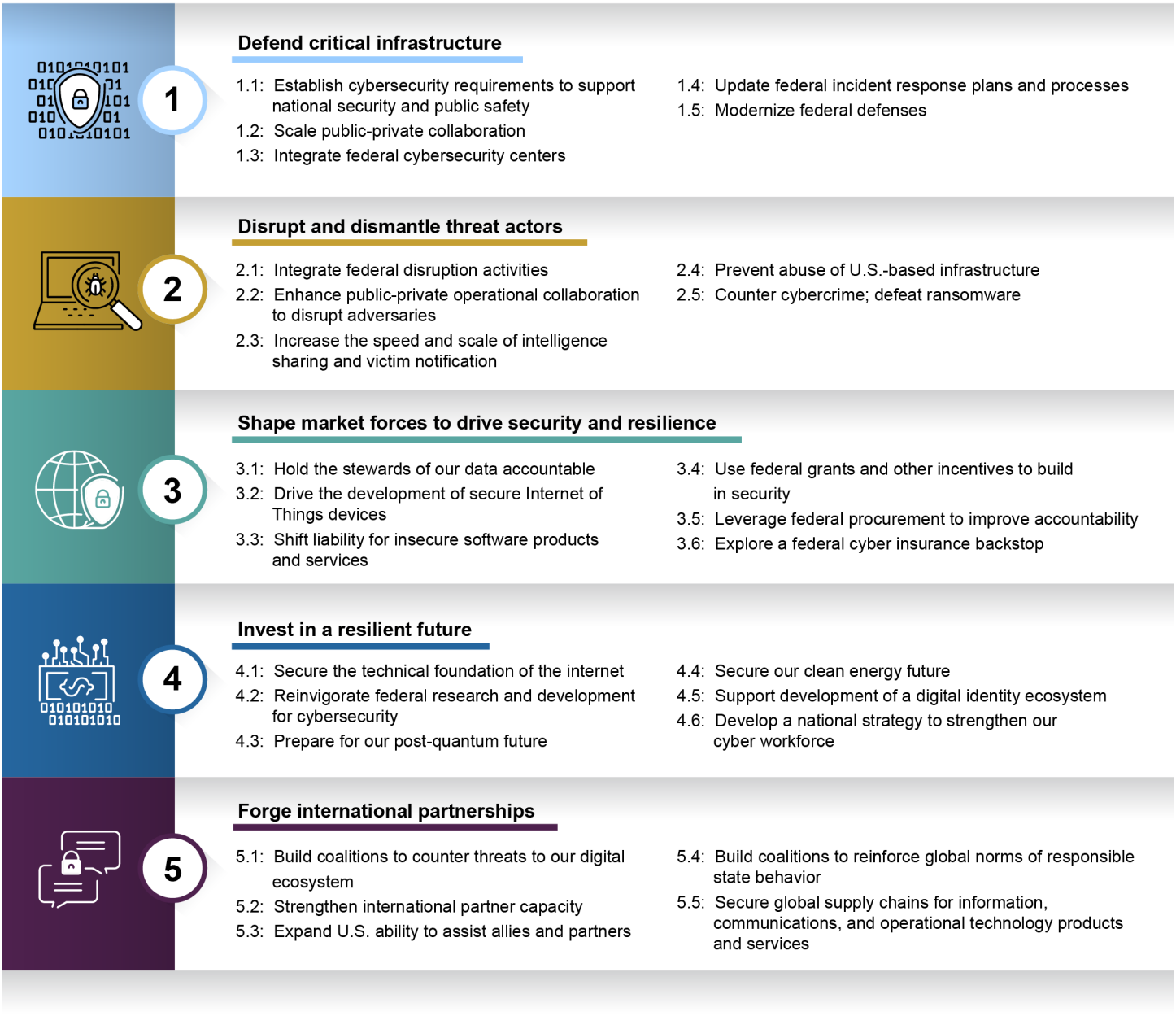
The White House Released the New National Cybersecurity Strategy and Accompanying Implementation Plan

In September 2018, the White House issued its *National Cyber Strategy*, which described actions that federal agencies and the executive branch were to take to secure critical infrastructure, among other things. Additionally, the strategy outlined the executive branch's approach to cybersecurity through a variety of priority actions needed to address the nation's cybersecurity challenges, such as centralizing management and oversight of federal civilian department and agency network cybersecurity and working with other countries to contribute to greater predictability and stability in cyberspace. The strategy assigned National Security Council staff to coordinate with departments, agencies, and OMB on a plan to implement the strategy.

Following the establishment of ONCD in January 2021, the 2018 strategy was replaced when the White House publicly issued a new *National Cybersecurity Strategy* in March 2023. The new strategy detailed the approach ONCD plans to take, particularly between the public and private sectors, to better secure cyberspace and ensure the United States is in the strongest position to realize all the benefits and potential of a digital future. In accordance with the law establishing the office, ONCD is responsible for leading the coordination of implementing the strategy (a role assigned to National Security Staff under the previous strategy). Further, the strategy stated that ONCD would work with interagency partners to develop and publish an implementation plan to set out the federal lines of effort necessary to implement this strategy.

The strategy outlined how the administration will manage the nation's cybersecurity through five pillars and 27 underlying strategic objectives, as depicted in figure 1.

Figure 1: Five Pillars and 27 Strategic Objectives of the March 2023 *National Cybersecurity Strategy*



Sources: GAO analysis of the *National Cybersecurity Strategy*; marinashevchenko/stock.adobe.com (icons). | GAO-24-106916

Subsequently, in July 2023, the White House publicly issued the accompanying *National Cybersecurity Strategy Implementation Plan*. The implementation plan described 69 initiatives that the federal government intends to carry out to achieve the strategy's objectives. The implementation plan is structured to align each of the initiatives with the *National Cybersecurity Strategy's* pillars and strategic objectives.

The implementation plan stated that it is a living document, which will be updated annually, and that initiatives will be added to the plan as the evolving cyber landscape demands.

GAO Has Reported on the Importance of National Strategy and Centralized Cybersecurity Leadership

For more than a decade, we have reported on the need for a comprehensive strategy and clearly defined leadership to address national cybersecurity issues.

- In July 2010, we reported on challenges the government faced regarding international cooperation in addressing global cybersecurity and governance.[15] Specifically, we reported that the government faced several challenges that impeded its ability to formulate and implement a coherent approach to addressing the global aspects of cybersecurity. For example, the White House Cybersecurity Coordinator's authority and capacity to effectively coordinate and forge a coherent national approach to cybersecurity policy were still under development.[16] Accordingly, we recommended that the Special Assistant to the President and Cybersecurity Coordinator, in collaboration with other federal entities and the private sector, make recommendations to appropriate agencies and interagency coordination committees to more effectively coordinate and forge a coherent national approach to cyberspace policy. The national Cybersecurity Coordinator and his staff generally concurred with the recommendation, and the White House subsequently released a strategy and other critical infrastructure guidance to implement our recommendation.
- In February 2013, we observed that the government's cybersecurity strategy documents, at the time, generally addressed several of the desirable characteristics of national strategies. However, the documents lacked certain key elements, such as milestones and

[15]GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

[16]In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator.

performance measures, costs and resources, roles and responsibilities, and linkages with other key strategy documents.[17] As a result, we recommended that the White House Cybersecurity Coordinator develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy. The National Security Staff within the Executive Office of the President agreed that more needed to be done to develop a coherent and comprehensive strategy on cybersecurity but did not believe producing another strategy document would be beneficial. However, in October 2015, the Director of OMB and the Federal Chief Information Officer issued a memorandum titled *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* that addressed our recommendation.

- In March 2019, we reported that the September 2018 *National Cyber Strategy* lacked key elements, including clearly defined roles and responsibilities and information on the resources needed to carry out the goals and objectives.[18] The strategy stated that National Security Council staff were to coordinate with departments, agencies, and OMB to determine the resources needed to support the strategy's implementation. However, it did not identify which official maintained overall responsibility for coordinating these efforts, especially in light of the elimination of the White House Cybersecurity Coordinator position in May 2018.[19] We stressed that it would be critical for the White House to clearly define the roles and responsibilities of key agencies and officials to foster effective coordination and hold agencies accountable for carrying out planned activities to address the cybersecurity challenges facing the nation.
- In April 2020, we reported that OMB and the Department of Homeland Security had yet to develop a government-wide cybersecurity strategic workforce plan that assessed the effects of a government-wide reform

[17]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[18]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[19]The White House Cybersecurity Coordinator position was created in December 2009 to, among other things, coordinate interagency cybersecurity policies and strategies, and to develop a comprehensive national strategy to secure the nation's digital infrastructure.

proposal to address the cybersecurity workforce shortage.[20] Therefore, we recommended that OMB, working with the Department of Homeland Security, develop a government-wide workforce plan that assessed the administration's reform proposal to solve the cybersecurity workforce shortage.[21] In July 2023, ONCD released the White House's *National Cyber Workforce and Education Strategy*, which included information and guidance for agencies to help strengthen the cybersecurity workforce, thus addressing our recommendation.[22]

- In September 2020, we reported that the White House's September 2018 *National Cyber Strategy* and the National Security Council's accompanying June 2019 *Implementation Plan* addressed several of the desirable characteristics of a national strategy, but lacked certain key elements.[23] Therefore, we recommended the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include (1) an assessment of cyber-related risk, based on an analysis of the threats to, and vulnerabilities of, critical assets and operations; (2) measures of performance and formal mechanism to track progress of the execution of activities; and (3) an analysis of the cost and resources needed to implement the strategy. National Security Council staff neither agreed nor disagreed with our recommendation. However, as discussed earlier, the responsibility for leading the coordination and implementation of the national cyber strategy has shifted to ONCD, and the 2018 strategy has been replaced by the *National Cybersecurity Strategy* issued in 2023. The new strategy partially addressed this recommendation, as discussed later in this report.

  Further, we reported that it was unclear which official ultimately maintained responsibility for coordinating execution of the strategy and implementation plan and for holding federal agencies accountable once activities were implemented. Accordingly, we stated that Congress should consider legislation to designate a leadership

[20]GAO, *Federal Management: Selected Reforms Could Be Strengthened by Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: Apr. 23, 2020).

[21]We also designated this as a priority open recommendation to OMB in July 2022. See GAO, *Priority Open Recommendations: Office of Management and Budget*, GAO-22-105582 (Washington, D.C.: July 15, 2022).

[22]The White House, ONCD, *National Cyber Workforce and Education Strategy*, (Washington, D.C.: July 31, 2023).

[23]GAO-20-629.

position in the White House with the commensurate authority—for example, over budgets and resources—to implement and encourage action in support of the nation's cyber critical infrastructure, including the implementation of the *National Cyber Strategy*. As noted above, Congress established the position of the National Cyber Director in January 2021.

- In June 2023, we reported that a timely issuance of an implementation plan to accompany the 2023 *National Cybersecurity Strategy*, with specific details on the implementation of key activities (e.g., performance measures, needed resources, and roles and responsibilities) was critical.[24] Specifically, the details needed to be issued expeditiously so agencies could begin planning and allocating resources to properly execute the strategy. As discussed earlier, the White House issued the accompanying *National Cybersecurity Strategy Implementation Plan* in July 2023.

The National Cybersecurity Strategy and Implementation Plan Fully Addressed Four of the Six Desirable Characteristics

We previously identified a set of desirable characteristics to aid responsible parties in developing and implementing national strategies, to enhance such strategies' usefulness in resources and policy decisions, and to better assure accountability.[25] We have stated that a national strategy should ideally contain all these characteristics. The characteristics that we identified are:

- **Purpose, scope, and methodology.** Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.
- **Problem definition and risk assessment.** Addresses the national problems and threats the strategy is directed toward and entails a risk assessment that includes an analysis of threats to, and vulnerabilities of, critical assets and operations.
- **Integration and implementation.** Addresses how a national strategy is related to other strategies, objectives, and activities and to subordinate levels of government and their plans to implement the strategy.
- **Organizational roles, responsibilities, and coordination.** Addresses who will be implementing the strategy, what their roles will

[24]GAO, *Cybersecurity: Launching and Implementing the National Cybersecurity Strategy*, GAO-23-106826 (Washington, D.C.: June 29, 2023).

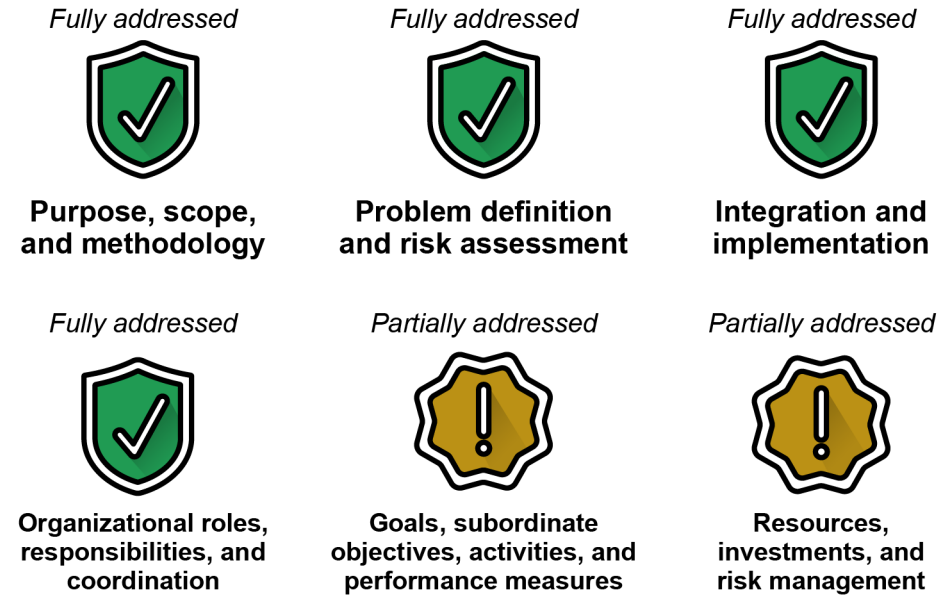
[25]GAO-04-408T.

be compared to others, and mechanisms for them to coordinate their efforts.

- **Goals, subordinate objectives, activities, and performance measures.** Addresses what the strategy is trying to achieve and steps to achieve those results, as well as priorities, milestones, performance measures, and a monitoring mechanism to gauge results.
- **Resources, investments, and risk management.** Addresses what the strategy will cost, the sources and types of resources and investment needed, and where resources and investments should be targeted based on balancing risk reductions with costs.

The recently issued *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan* jointly addressed four of the six desirable characteristics of a national strategy and partially addressed two other characteristics (see fig. 2).

Figure 2: Extent to Which the March 2023 *National Cybersecurity Strategy* and July 2023 *National Cybersecurity Strategy Implementation Plan* Addressed GAO's Desirable Characteristics of a National Strategy



Source: GAO analysis and icon; yevheniia/stock.adobe.com (icons). | GAO-24-106916

The Strategy and Implementation Plan Fully Addressed Four Desirable Characteristics

The *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan* fully addressed the following four characteristics of a national strategy: purpose, scope, and methodology; problem definition and risk assessment; integration and implementation; and organizational roles, responsibilities, and coordination.

Purpose, scope, and methodology. The two documents addressed why the strategy was produced, the scope of its coverage, and the process by which it was developed. With respect to addressing why the strategy was produced, the strategy detailed the approach the administration will take to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of the digital future. Additionally, the strategy stated that it will position the United States and its allies and partners to build a digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with the nation's values.

The strategy and implementation plan also addressed the scope of the strategy's coverage, including describing the major functions, mission areas, and activities it will cover. As previously mentioned, the strategy was organized around five pillars and 27 strategic objectives. The pillars organizing this strategy articulated a vision of shared purpose and priorities for stakeholder communities (i.e., public sector, private industry, civil society, and international allies and partners). In addition, the implementation plan described 69 initiatives that the federal government intends to carry out to achieve the strategy's objectives. Further, the titles and descriptions of each initiative identified the major action and activities associated with that initiative. The implementation plan's initiatives were also structured by pillar and strategic objective, which aligned with the *National Cybersecurity Strategy*.

Regarding the process by which it was developed, the strategy stated that it was built on existing policy and significant achievements that were already shaping the strategic environment and digital ecosystem. The strategy also stated that it was developed alongside the *National Security Strategy* and the *2022 National Defense Strategy* by a broad, interagency team and though a consultation process with the private sector and civil society.[26]

[26]The White House, *National Security Strategy*, (Washington, D.C.: Oct. 12, 2022) and Department of Defense, *2022 National Defense Strategy* (Washington, D.C.: Oct. 27, 2022).

Problem definition and risk assessment. The strategy and implementation plan addressed the national problems and threats the strategy is directed toward and identified where risk assessments will need to be done in the future. Specifically, the strategy discussed the strategic environment, including emerging trends and malicious actors. In addition, the strategy stated that emerging trends are creating both new opportunities for further advancement and new challenges to overcome. It added that malicious actors threaten the nation's progress toward a digital ecosystem that is inclusive, equitable, promotes prosperity, and aligns with the nation's democratic values.

The *National Cybersecurity Strategy Implementation Plan* identified initiatives that are aimed at addressing specific national problems and threats that the strategy is directed toward. For example, for pillar two, Disrupt and Dismantle Threat Actors, the implementation plan described multiple initiatives that are aimed at addressing national problems and threats. Specifically, initiative 2.5.2 is intended to disrupt ransomware crimes and initiative 2.1.4 is focused on proposing legislation to disrupt and deter cybercrime and cyber-enabled crime.

In addition, the implementation plan identified where risk assessments will be needed to implement an initiative. For example, initiative 1.1.2 was aimed at setting cybersecurity requirements across critical infrastructure sectors. To accomplish this initiative, sector risk management agencies and regulators are to analyze the cyber risk in their industries and outline how they will use their existing authorities to establish cyber requirements that mitigate risk in their sectors, account for sector-specific needs, identify gaps in authorities, and develop proposals to close them. The inclusion of this information in the new strategy and implementation plan partially addressed our outstanding recommendation related to the prior strategy that it, among other things, address an assessment of cyber-related risks.[27]

Integration and implementation. The documents addressed how the strategy relates to other strategies and plans for implementation, and how it relates to subordinate levels of government. With regard to addressing how the *National Cybersecurity Strategy* relates to other strategies, the strategy stated that it was informed by and implements values of the

[27]GAO-20-629.

Declaration for the Future of the Internet[28] and the Freedom Online Coalition.[29] In addition, the strategy stated that it carries forward the foundational direction of Executive Order 14028;[30] the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*;[31] and the *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*.[32]

Further, regarding the strategy's relationship to subordinate levels of government and their plans to implement the strategy, the implementation plan identified other entities' plans that need to be updated to implement the strategy's goals. For example, initiative 1.4.1 instructed the Cybersecurity and Infrastructure Security Agency to lead a process to update the *National Cyber Incident Response Plan*—which is subordinate to Presidential Policy Directive 41—to strengthen processes, procedures, and systems.

Regarding plans to implement the strategy, the implementation plan is to serve as guidance for how each of the initiatives are to be implemented. For each initiative, the implementation plan explained the activities associated with implementing the action that will support the overall outcome of that initiative. The implementation plan also demonstrated that it is vertically integrated with relevant documents from other implementing organizations. For example, initiative 2.1.1 stated that the Department of Defense will develop an updated Cyber Strategy that is aligned with the *National Security Strategy, National Defense Strategy,*

[28]In April 2022, the United States and the governments of 60 countries and the European Commission launched the Declaration for the Future of the Internet, bringing together a broad, diverse coalition of partners—the largest of its kind—around a common, democratic vision for an open, free, global, interoperable, reliable, and secure digital future.

[29]Since being established in 2011, the Freedom Online Coalition is currently an intergovernmental coalition that includes the governments of 38 countries and is committed to supporting Internet freedom and protecting human rights—free expression, association, and peaceful assembly, and privacy rights online—worldwide.

[30]The White House, *Improving the Nation's Cybersecurity,* Executive Order 14028 (Washington, D.C.: May 12, 2021).

[31]The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (Washington, D.C.: Jul. 28, 2021).

[32]The White House, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (Washington, D.C.: Jan. 19, 2022).

and *National Cybersecurity Strategy* to focus on challenges posed by nation-states and other malicious actors.[33] In addition, initiative 5.1.2 tasked the Department of State with publishing an International Cyberspace and Digital Policy Strategy. This strategy is to incorporate bilateral and multilateral activities to expand coalitions; build the capacity of international allies and partners; and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Organizational roles, responsibilities, and coordination. The *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan* addressed who will be implementing the strategy, what their roles will be in relation to other agencies, and how coordination will occur. For example, the strategy stated that, under the oversight of National Security Council staff and in coordination with OMB, ONCD is to coordinate implementation of the strategy. Toward this end, the office worked with its interagency partners to develop and publish the implementation plan to set out the federal lines of effort necessary to execute the strategy. Further, initiative 6.1.1 stated that ONCD will report on the effectiveness of the *National Cybersecurity Strategy*.

With regard to addressing what agencies' roles will be when compared to others, for each of the initiatives, the implementation plan identified the responsible agency for implementing that initiative and identified contributing entities, where applicable. The implementation plan explained that the responsible agency is the federal agency accountable for leading the specific initiative with other stakeholders. Further, the contributing entities were identified as federal departments or agencies that have a significant role in the development and execution of the initiative, including by contributing expertise or resources, engaging in complementary efforts, or coordinating on elements of a program.

Regarding coordination, the strategy and implementation plan described the approaches to be used to facilitate coordination among the various entities responsible for implementing the strategy. For example, the strategy stated that National Security Council staff will use the processes described in *National Security Memorandum on Renewing the National Security Council System* to address issues related to the review of

[33]In September 2023, the Department of Defense released an unclassified summary of its classified *2023 Cyber Strategy*. See https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

existing policy or the development of new policy.[34] In addition, several initiatives in the implementation plan identified existing interagency mechanisms to facilitate coordination. For example, initiative 1.2.2 references the Federal Senior Leadership Council, a chartered interagency body, as the mechanism to provide recommendations to the Secretary of Homeland Security on critical infrastructure sector and sector risk management agency designations. In addition, initiative 4.1.3 tasked the National Institute of Standards and Technology with using the Interagency International Cybersecurity Standardization Working Group to coordinate and enhance federal agency participation in international cybersecurity standardization.

ONCD staff also noted that the office is designated by statute to lead the coordination of implementation of national cyber policy and strategy, including the National Cyber Strategy.[35] They further stated that the public release of the strategy and implementation plan underscores the need for coordination and collaboration and assists in holding responsible agencies and contributing entities accountable for their respective initiatives. ONCD staff also described several other processes for coordination among the responsible agencies and entities. These included monthly meetings with all "action officers"—who are the leads for their respective agencies—about the progress made across the entire plan. They also included ongoing engagement between ONCD and individual agencies related to their initiatives, including ongoing communications with agency leadership on progress, as well as meetings among subject matter experts collaborating on specific initiatives. The staff added that the office maintains escalation pathways to the Assistant Secretary and Deputy Secretary levels, if needed to resolve a disagreement. Lastly, ONCD maintained a list that identifies the agency point of contacts for each of the initiatives. ONCD staff stated that they shared this list with the full implementation community to facilitate less formal collaboration on initiatives, as appropriate.

The Strategy and Implementation Plan Partially Addressed Two Desirable Characteristics

The *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan* partially addressed the two desirable characteristics of a national strategy related to goals, subordinate objectives, activities,

[34]The White House, *Memorandum on Renewing the National Security Council System,* National Security Memorandum-2 (Washington, D.C.: Feb. 4, 2021).

[35]6 U.S.C. § 1500(c)(1)(C).

and performance measures; and resources, investments, and risk management:

Goals, subordinate objectives, activities, and performance measures. The *National Cybersecurity Strategy* and *National Cybersecurity Strategy Implementation Plan* jointly addressed what the strategy is trying to achieve, prioritize the steps to achieve those results, and identify milestones to gauge results. With respect to what the strategy is trying to achieve (i.e., goals), the strategy, as previously discussed, laid out five pillars and identifies 27 strategic objectives. Further, in the implementation plan, each strategic objective was further broken down into a list of 69 initiatives for the federal government to carry out to achieve the strategy's goals. The strategy and implementation plan also described the steps that are needed to achieve results. For example, under each of the initiatives in the implementation plan, there was a description of the specific actions or discrete deliverables that need to be completed or delivered to achieve the desired result.

The implementation plan also established milestones and priorities by laying out specific estimated completion dates by quarter for each initiative. According to ONCD staff, each of the 69 initiatives in the implementation plan is a priority, which justifies its inclusion in the initial version of the implementation plan. Further, in interagency documentation, the office established more detailed deliverables and interim milestones for each initiative to monitor progress made toward completing them. In addition, to gauge results, ONCD staff stated that the office has monthly check-in meetings with each agency identified in the plan to monitor and track progress of initiative implementation, and communicates with agency leaders to hold agencies to agreed timelines. According to the same staff, 10 of the 11 initiatives that were scheduled to be implemented by the end of fiscal year 2023 had been completed. They added that they would provide a public update on the status of all the initiatives concurrently with the release of the second version of the implementation plan. These actions also partially addressed our recommendation on the prior strategy that it have a mechanism to track progress of the execution of activities.[36]

However, neither the strategy nor the implementation plan included outcome-oriented performance measures for the initiatives or for the overall objectives of the strategy to gauge success. Specifically, while the

[36]GAO-20-629.

initiatives included deliverables, milestones, and estimated completion dates, they did not include measures to assesses the extent to which the initiatives are achieving outcome-oriented objectives, such as improving information sharing or modernizing federal agency defenses.

ONCD staff stated that the percentage of the 69 initiatives being completed on time will serve as an overall performance measure but added that it was not feasible to develop additional outcome-oriented measures at this point. They acknowledged the value of having meaningful outcome-oriented performance measures to assess cybersecurity effectiveness but stated that such measures do not currently exist in the cybersecurity field in general.

However, as we reported in September 2023, we believe that it is feasible for ONCD to develop outcome-oriented measures, when applicable for an initiative, to help ensure that the ongoing implementation of the initiatives are achieving results.[37] For example, with respect to initiative 1.4.2 on issuing the final Cyber Incident Reporting for Critical Infrastructure Act of 2022 rule, ONCD may be able to measure the number of threat information products (e.g., alerts) that are developed based on incident reporting under this rule. In doing so, the office could survey users of these threat information products to determine what specific impacts these products had on the security of their networks.

In addition, initiative 2.1.2 called for strengthening the National Cyber Investigative Joint Task Force's capacity to coordinate takedown and disruption campaigns with greater speed, scale, and frequency. ONCD may be able to measure the number of government disruption campaigns that occurred and the speed at which the joint task force is able to coordinate the takedown of these disruption campaigns. In doing so, the office would have the data to determine if the joint task force has increased its capacity to address these types of disruption campaigns with greater speed, scale, and frequency. Further, regarding initiative 2.5.2 on disrupting ransomware crime attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value

[37]We also 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. See GAO, *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, GAO-23-105468 (Washington, D.C.: Sept. 26, 2023).

was about $886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness.

Until ONCD assesses the initiatives to identify those that lend themselves to having outcome-oriented performance measures and develops such measures for those initiatives, 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.

Resources, investments, and risk management. The *National Cybersecurity Strategy Implementation Plan* addressed risk management by instructing agencies to focus their resources and investments on certain actions based on balancing risk reduction with cost. For example, initiative 1.5.2 tasked OMB with leading the development of a multiyear lifecycle plan to accelerate federal civilian executive branch technology modernization, and prioritizing federal efforts on eliminating legacy systems which are costly to maintain and difficult to defend. As a result, agencies should be able to save costs and reduce risks if they focus their efforts on modernizing their IT systems as opposed to maintaining legacy systems.

Also, the strategy and implementation plan partially addressed the sources and types of resources and investments needed to carry out the initiatives. For example, initiative 5.5.2 called for the federal government to use the Department of State's newly created International Technology Security and Innovation Fund to invest in secure supply chains for semiconductors. In addition, the implementation plan identified initiatives to assist with budget prioritization and resource allocation. For example, initiative 6.1.3 was intended to align budgetary guidance with *National Cybersecurity Strategy* implementation. This initiative resulted in a joint memorandum from ONCD and OMB that identified the cybersecurity budget priorities for fiscal year 2025 to help agencies align their budgets with the priorities in the strategy and implementation plan.[38] ONCD staff added a similar memorandum will be issued annually to support budget submissions for future fiscal years.

However, neither the strategy nor the implementation plan included specific details on the estimated cost of the plan's initiatives. For example, while the implementation plan outlined initiatives that require

[38]OMB and ONCD, *Administration Cybersecurity Priorities for the FY 2025 Budget*, M-23-18 (Washington, D.C.: June 27, 2023).

executive visibility and interagency coordination, it did not identify how much it will cost to implement the initiatives.

To its credit, ONCD staff demonstrated that the office has accounted for the staff resources and contract arrangements necessary to implement the initiatives it is responsible for implementing. The staff added that they included this in the office's budget requests.

In addition, ONCD staff said the office is working with the agencies to ensure that activities related to the initiatives are included in their budget submissions. However, ONCD staff stated that estimating the cost to implement the entire strategy and implementation plan was an unrealistic goal due to the current nature of the budget process, where costs may be embedded in agencies' baseline budgets.

While we agree that certain initiatives may not warrant a specific cost estimate, other activities supporting some of the key initiatives with potentially significant costs justify the development of a cost estimate. For example, initiative 1.2.5 tasked the Cybersecurity and Infrastructure Security Agency with establishing and codifying a sector risk management agency support office capability to serve as the single point of contact for all sector risk management agencies. A cost estimate for this initiative would provide the Cybersecurity and Infrastructure Security Agency with information to support a request in its budget submission for funding this capability.

In addition, initiative 2.1.3 tasked the Department of Justice with expanding its organizational platforms dedicated to disruption campaigns and increasing the number of qualified attorneys dedicated to cyber work. A cost estimate for this initiative would provide the department with information to support a request in its budget submission for funding the expansion of its organizational platforms and the labor costs to support the increase of attorneys.

Moreover, cost estimates are essential to effectively managing programs. Without such information, uncertainty can emerge about investing in programs. Further, we believe that ONCD and implementing agencies could demonstrate budgetary commitment to ensuring strategy implementation if cost estimates are developed for certain initiatives, even if the costs will be funded through baseline budgets. Once the relevant estimates have been established, the office can work with the agencies to ensure that those estimates are documented in the agencies' upcoming budget submissions. Accordingly, until ONCD assesses the initiatives to

identify those that warrant a cost estimate and works with the relevant agencies to develop estimates for those initiatives, the office cannot be confident that adequate resources are available to support implementing the strategy.

Conclusions

Fully establishing a national strategy to guide the federal government's cybersecurity activities, including its coordination with the private sector, is a critical component of the leadership commitment needed to ensure the cybersecurity of the nation. Developing such a strategy has been a long-standing effort spanning multiple administrations.

Most recently, ONCD was established to provide a central leadership role in overcoming the nation's cyber-related threats and challenges, including leading the coordination of implementation of a national cyber policy and strategy. The White House has utilized the office to take important steps, including developing and publicly releasing the *National Cybersecurity Strategy* and its accompanying implementation plan.

However, while the strategy and implementation plan addressed some of the characteristics of an effective national strategy, they did not fully incorporate outcome-oriented performance measures and estimated resources and costs. Without outcome-based performance measures, ONCD and its stakeholders will be limited in gauging the effectiveness of actions taken to implement the strategy. Further, without estimating the costs of implementing applicable initiatives, ONCD and other implementing agencies will be challenged in ensuring that adequate resources are available for those initiatives.

Recommendations for Executive Action

We are making two recommendations to ONCD:

- The Director of ONCD should work with relevant federal entities to assess the initiatives 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. (Recommendation 1)
- The Director of ONCD should work with relevant federal entities to assess the initiatives to identify those that warrant a cost estimate and develop such cost estimates. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to ONCD for review and comment. In its written comments, the office partially agreed with one finding and agreed with the related recommendation, disagreed with one recommendation, and disagreed with one recommendation originally included in our draft report.

- ONCD partially agreed with our finding on outcome-oriented measures and agreed with the related recommendation to assess the initiatives to identify those that warrant outcome-oriented performance measures. ONCD said certain initiatives in the implementation plan lend them themselves to output-based measures as a proxy (though not a substitute) for outcome-oriented measures. It added that the office has already made use of such output-based measures as part of the deliverables and milestones agencies must complete, which was discussed earlier in this report. ONCD further stated that the example measures we identified earlier in the report are not outcome-based but output-based measures of success. ONCD further noted that developing outcome-oriented measures remains an open research problem.

  We agree that a combination of output-based and outcome-oriented performance measures would be useful in gauging the effectiveness of actions taken to implement the strategy. In addition, we believe the examples we described earlier in the report support the need for ONCD to develop outcome-oriented measures for the initiatives that lend themselves towards having outcome-oriented performance measures. For example, regarding initiative 2.5.2 on disrupting ransomware crime attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value was about $886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness. Accordingly, we maintain that ONCD should work with relevant federal entities to assess the initiatives that lend themselves to outcome-oriented performance measures and develop such performance measures for those initiatives.

- ONCD disagreed with our finding and associated recommendation that the strategy and implementation plan did not include specific details on the estimated cost of the plan's initiatives. ONCD stated that it is unable to provide details such as cost estimates for implementing any of the initiatives identified in the implementation plan due to OMB guidance that restricts agencies from disclosing future year budget plans outside of the current budget cycle.

ONCD also referenced the joint memorandum it issued with OMB that identified the cybersecurity budget priorities for fiscal year 2025 to help agencies align their budgets with the priorities in the strategy and implementation plan. ONCD believes this memorandum will appropriately drive resource allocation and investment in accordance with the strategy. ONCD also noted that the President's Budget for fiscal year 2025 has not yet been released. Thus, the office stated, it is premature for us to assert that the administration's approach is insufficient.

We acknowledge the value of ONCD and OMB providing guidance on cybersecurity budget priorities through their joint memorandum. We agree this guidance is a good step toward assisting agencies in determining how much it will cost to implement respective initiatives. However, we identified initiatives that may require significant costs. As such, we maintain that ONCD should work with the relevant agencies to assess the initiatives in the implementation plan to identify those that warrant the development of a cost estimate and develop such cost estimates. As noted in our report, neither the strategy nor the implementation plan identifies specific costs associated with any of the initiatives. Further, the implementation plan stated that it is a living document, which will be updated annually, and that initiatives will be added to the plan as the evolving cyber landscape demands. Accordingly, as new initiatives are added to the implementation plan, it will be important for ONCD to work with the agencies to identify the initiatives that warrant the development a cost estimate and create such estimates to help inform the agencies' future budget submissions.

- ONCD disagreed with a recommendation included in the draft of this report to detail and document how the entities identified in the *National Cybersecurity Strategy Implementation Plan* are to coordinate and collaborate, including how conflicts would be resolved, to implement their respective initiatives. The office provided additional information and context related to the coordination mechanisms that are in place to ensure that the entities identified in the implementation plan are effectively executing their assigned activities. Upon our review of the information, we agreed that ONCD had sufficiently addressed the organizational roles, responsibilities, and coordination characteristic. Accordingly, we removed this finding and withdrew the recommendation from the final report.

ONCD's comments are reprinted in appendix II. The office also provided technical comments, which we incorporated into the report, as appropriate.

We are sending copies of this report to the appropriate congressional committees, ONCD, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Margaret Wood Hassan
Chairwoman
The Honorable Mitt Romney
Ranking Member
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
House of Representatives

The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Frank Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Darrell Issa
Chairman
Subcommittee on Courts, Intellectual Property, and the Internet
Committee on the Judiciary
House of Representatives

The Honorable Andrew Garbarino
Chairman
The Honorable Eric Swalwell
Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection
Committee on Homeland Security
House of Representatives

The Honorable Nancy Mace
Chairwoman
The Honorable Gerald E. Connolly
Ranking Member
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Committee on Oversight and Accountability
House of Representatives

The Honorable Mike Gallagher
Representative
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to examine the extent to which the *National Cybersecurity Strategy* and accompanying implementation plan addressed the desirable characteristics of a national strategy.

To address this objective, we assessed the March 2023 *National Cybersecurity Strategy* and the accompanying *National Cybersecurity Strategy Implementation Plan* dated July 2023. Specifically, we reviewed the strategy, the accompanying implementation plan, and related Office of the National Cyber Director (ONCD) internal documentation to determine if they met the desirable characteristics of a national strategy, as identified in prior GAO work.[1] These characteristics provide additional guidance for those developing and implementing strategies, as well as enhance strategy usefulness as guidance for resource and policy decision-makers and to better assure accountability. Table 1 identifies the six characteristics of a national strategy included in our review.

Table 1: National Strategy Characteristics and Definitions Used to Examine the *National Cybersecurity Strategy* and Implementation Plan

Characteristic	Definition	Examples
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed.	• Statement of broad or narrow purpose, as appropriate • How it compares and contrasts with other national strategies • Major functions, mission areas, or activities it covers
Problem definition and risk assessment	Addresses the particular national problems and threats the strategy is directed toward and entails a risk assessment that includes an analysis of threats to, and vulnerabilities of, critical assets and operations.	• Discussion or definition of problems, their causes, and operating environment • Risk assessment (analysis of threats/vulnerabilities) • Quality of data available (e.g., constraints and deficiencies)
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results.	• Overall results desired (i.e., “end-state”) • Hierarchy of strategic goals and subordinate objectives • Specific activities to achieve results • Priorities, milestones, and performance measures

[1]GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

Characteristic	Definition	Examples
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs.	• Resources and investments associated with the strategy • Types of resources needed (budgetary, human capital, information technology, research/development, contracts) • Sources of resources (e.g., federal, state, local, and private) • Economic principles, such as balancing benefits, costs
Organizational roles, responsibilities, and coordination	Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts.	• Roles and responsibilities of specific federal agencies, departments, or offices • Roles and responsibilities of state, local, private, and international sectors • Lead, support, and partner roles and responsibilities
Integration and implementation	Addresses how a national strategy relates to other strategies' goals, objectives, and activities, as well as to subordinate levels of government and their plans to implement the strategy.	• Integration with other national strategies (horizontal) • Integration with relevant documents from implementing organizations (vertical) • Implementation guidance

Source: GAO. | GAO-24-106916

To determine the extent to which the strategy and implementation plan had met the desirable characteristics, we assessed the strategy and implementation plan and compared them to the characteristics outlined in the table above. We also interviewed relevant ONCD staff to obtain additional information and to better understand the development process of the *National Cybersecurity Strategy* and accompanying implementation plan. Further, we discussed the desirable characteristics of a national strategy with the relevant ONCD staff.

We assessed whether the *National Cybersecurity Strategy* and accompanying implementation plan addressed the desirable characteristics of a national strategy as:

- fully addressed, if available evidence demonstrated all aspects of the selected characteristic;
- partially addressed, if available evidence demonstrated some, but not all, aspects of the selected characteristic; and
- not addressed, if available evidence did not demonstrate any aspects of the selected characteristic.

As a part of our analysis, we also determined if ONCD had established organizational roles and responsibilities for implementing the national strategy, had defined the process of how it will achieve the strategy's

objectives, and how ONCD shared information to achieve the strategy's objectives.

We conducted this performance audit from June 2023 to February 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Office of the National Cyber Director

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF THE NATIONAL CYBER DIRECTOR
WASHINGTON, D.C. 20503

January 5, 2024

Dear General Dodaro,

Thank you for the opportunity to respond in writing to GAO's report entitled "National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy." The Office of the National Cyber Director (ONCD) appreciates GAO's longstanding interest in cybersecurity challenges facing the U.S. government and our nation, and the work that went into preparing this report.

As discussed below, ONCD submits facts bearing on the accuracy of GAO's findings that ONCD "partially addressed" three desirable characteristics of a national strategy..

Finding 1 – The National Cybersecurity Strategy and National Cybersecurity Strategy Implementation Plan partially addressed the desirable characteristics of a national strategy related to goals, subordinate objectives, activities, and performance measures, but did not include outcome-oriented performance measures for the initiatives

ONCD partly concurs with this finding and concurs with its corresponding recommendation. As detailed in ONCD's response to a prior GAO audit, "developing outcome-based performance measures for cybersecurity is a challenging topic."[1] ONCD agrees with GAO's finding that neither the Strategy nor the Implementation Plan identify "measures to assess the extent to which the initiatives are achieving outcome-oriented objectives," and notes that this open research problem remains one of significant interest.

However, ONCD believes that the example measures GAO provides in the draft report are not "outcome-based"; rather, they are out*put*-based measures of success. As ONCD staff have noted, certain initiatives in the Implementation Plan lend themselves to output-based measures as proxy – though not a substitute – for outcome-based metrics. Where appropriate, ONCD has already made use of such output-based measures as part of the deliverables and milestones agencies must complete.

ONCD does accept GAO's recommendation to assess initiatives that lend themselves to outcome-oriented performance measures and, to the extent that validated measures exist, apply them to initiatives going forward with the benefit of research.

Finding 2 – The National Cybersecurity Strategy and National Cybersecurity Strategy Implementation Plan partially addressed the desirable characteristics of a national strategy related to resources, investments, and risk management, but did not include specific details on the estimated costs of the plan's initiatives.

[1] GAO-23-105468

ONCD does not concur with this finding or its corresponding recommendation.

The Office of Management and Budget (OMB) provides guidance to departments and agencies restricting disclosures of any future year budget plans,[2] thereby preventing ONCD from providing details such as cost estimates of the initiatives.

As part of ONCD's evolving authority to review "the annual budget proposals for relevant Federal departments and agencies and advis[e] the heads of such departments and agencies whether such proposals are consistent with such national cyber policy and strategy,"[3] ONCD and OMB jointly issue an annual memorandum for the heads of executive department and agencies detailing the Administration's cybersecurity priorities for the fiscal year. Departments and agencies formulate their budget requests to address the priorities and achieve the goals, objectives, and initiatives in overarching policy documents. To that end, the fiscal year 2025 Cybersecurity Priorities Memo is the first such guidance to be issued after the National Cybersecurity Strategy was published in March 2023, and the Memo is specifically aligned with the Strategy. ONCD believes the Memo will appropriately drive resource allocation and investment in accordance with the Strategy. ONCD further notes that, as the President's Budget for Fiscal Year 2025 has not yet been released, it is premature for GAO to assert that the Implementation Plan – and the approach taken by the Administration – is insufficient in this regard.

Finding 3 – The National Cybersecurity Strategy and National Cybersecurity Strategy Implementation Plan partially addressed the desirable characteristics of a national strategy related to organizational roles, responsibilities, and coordination, but did not fully detail and document the approach for facilitating coordination among entities responsible for implementation

ONCD does not concur with this finding or its corresponding recommendation. ONCD has consistently described in the plan itself the methods for facilitating coordination to develop the Implementation Plan and assigned organizational roles and responsibilities. The Strategy and Implementation Plan, in addition to supplemental documentation provided by ONCD to GAO, clearly describe an "overarching accountability and oversight framework"[4] with a clear escalation pathway into the National Security Memorandum 2[5] process to resolve disputes and monthly interagency meetings culminating in an annual report. For this reason, the National Cybersecurity Strategy has fully met this characteristic of an effective strategy as detailed below.

Organizations That Will Implement the Strategy

GAO credits the Strategy with identifying the "the specific federal departments, agencies, or offices involved" with implementing the Strategy. As noted in the Implementation Plan, the

[2] OMB Circular A-11, Sec, 22
[3] 6 U.S.C. § 1500(c)(1)(C)(iii)
[4] https://www.gao.gov/assets/gao-04-408t.pdf, p.22
[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system/

process for implementing the Strategy will be iterative, so the agencies directly involved leading or supporting an initiative may change over time. In the initial Implementation Plan GAO reviewed, 29 agencies have an explicit role as either a responsible or contributing entity.

Roles and Responsibilities

GAO also credits the Strategy with clearly outlining roles and responsibilities. As noted in the "Implementation Plan Reading Guide," each initiative has a "Responsible Agency," defined as "[t]he Federal agency responsible for leading the initiative with other stakeholders." Many initiatives also have "Contributing Entities," defined as "Federal agencies that have a significant role in the development and execution of the initiative, including by contributing expertise or resources, engaging in complementary efforts, or coordinating on elements of a program." This directly meets GAO's desirable characteristic of "clarify[ing] implementing organizations' relationships in terms of leading, supporting, and partnering." As noted by ONCD staff, every initiative has a single, clear lead agency, and certain tasks have been subdivided to address "responsibilities between implementing parties where there is otherwise no clear or established hierarchy of lead and support functions."

Methods for Coordination

GAO faults the Strategy for failing to "fully detail and document" the methods used for coordination among entities responsible for implementing the Strategy. However, as GAO itself notes, ONCD staff provided consistent evidence of coordination mechanisms that would "provide for some mechanism to ensure that the parties are prepared to fulfill their assigned responsibilities and use their available resources appropriately to enhance their capabilities and preparedness." ONCD holds monthly agency calls to check in with initiative leaders and ensure that they are making progress towards completing their assigned activities. These calls fall into an "overarching accountability or oversight framework" that culminates in an annual report to the President and Congress outlining progress towards implementing the Strategy.

GAO states that ONCD "had not fully detailed [the coordination or conflict resolution processes] in a formal document," and asserts that "ONCD did not provide details on the escalation pathways used to resolve potential conflicts." ONCD disagrees with this characterization, as ONCD staff explained to GAO that the formal National Security Memorandum 2 process is used for conflict resolution. Furthermore, for documenting roles and responsibilities, ONCD developed and finalized the Implementation Plan itself through a formal interagency coordination process and thus the Plan itself constitutes a formal interagency agreement on roles and responsibilities.

In developing its desirable characteristics for national strategies, GAO praised two strategies for "designat[ing] some specific tools or processes (e.g., steering committee or task force)" related to "coordination between implementing parties."[6] At the initiative level, this is included numerous times in the National Cybersecurity Strategy. For instance, initiative 1.2.2, "Provide recommendations for the designation of critical infrastructure sectors and SRMAs," references

[6] GAO-04-408t

the Federal Senior Leadership Council, a chartered, formal coordination mechanism as the means to make such recommendations. Initiative 2.5.2, "Disrupt Ransomware Crimes," states that the activities will be carried out in coordination with the Joint Ransomware Task Force, a statutorily created body. Initiative 4.1.3, "Accelerate development standardization, and adoption of foundational Internet infrastructure capabilities and technologies," references the Interagency International Cybersecurity Standardization Working Group as the body to carry out this activity. In other words, there are many examples of existing formal mechanisms being used, as appropriate, to drive coordination among the entities involved in an initiative.

The monthly check-in calls mentioned above provide an additional accountability mechanism in cases where there is no existing formal mechanism.

Finally, ONCD notes that much of the work on the Implementation Plan was done in light of GAO's findings in GAO-20-629 that the 2018 National Cyber Strategy and its implementation plan had this same desirable characteristic. ONCD is aware of no additional "detail and document[ation]" from the 2018 Strategy that would meet the standard GAO is describing in its draft report.

ONCD believes that the 2023 National Cybersecurity Strategy and its Implementation Plan clearly possess the desirable characteristic of outlining organizational roles, responsibilities, and coordination. As such, ONCD does not agree with draft finding 3 or its corresponding recommendation.

Conclusion

For the foregoing reasons, ONCD requests that the report be amended to address facts set forth in this response.

Sincerely,

James J. Halpert
General Counsel
Office of the National Cyber Director

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Marisol Cruz Cain, (202) 512-5017 or CruzCainM@gao.gov

Staff Acknowledgments

In addition to the contact named above, Lee McCracken (Assistant Director), Javier Irizarry (Analyst-In-Charge), Amanda Andrade, Kiana Beshir, Rebecca Eyler, Lee Hinga, Franklin Jackson, Smith Julmisse, Ceara Lance, Scott Pettis, Andrew Stavisky, Umesh Thakkar, Sarah Veale, and Marshall Williams, Jr. made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548