September 2020

CYBERSECURITY

Clarity of Leadership Urgently Needed to Fully Implement the National Strategy

GAO Highlights

Highlights of GAO-20-629, a report to congressional requesters

Why GAO Did This Study

Increasingly sophisticated cyber threats have underscored the need to manage and bolster the cybersecurity of key government systems and the nation's cybersecurity. The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. In 2018, GAO noted that the need to establish a national cybersecurity strategy with effective oversight was a major challenge facing the federal government.

GAO was requested to review efforts to protect the nation's cyber critical infrastructure. The objectives of this report were to (1) describe roles and responsibilities of federal entities tasked with supporting national cybersecurity, and (2) determine the extent to which the executive branch has developed a national strategy and a plan to manage its implementation.

To do so, GAO identified 23 federal entities responsible for enhancing the nation's cybersecurity. Specifically, GAO selected 13 federal agencies based on their specialized or support functions regarding critical infrastructure security and resilience, and 10 additional entities based on analysis of its prior reviews of national cybersecurity, relevant executive policy, and national strategy documents. GAO also analyzed the *National Cyber Strategy* and *Implementation Plan* to determine if they aligned with the desirable characteristics of a national strategy.

View GAO-20-629. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

Federal entities have a variety of roles and responsibilities for supporting efforts to enhance the cybersecurity of the nation. Among other things, 23 federal entities have roles and responsibilities for developing policies, monitoring critical infrastructure protection efforts, sharing information to enhance cybersecurity across the nation, responding to cyber incidents, investigating cyberattacks, and conducting cybersecurity-related research. To fulfill their roles and responsibilities, federal entities identified activities undertaken in support of the nation's cybersecurity. For example, National Security Council (NSC) staff, on behalf of the President, and the National Institute of Standards and Technology, have developed policies, strategies, standards, and plans to guide cybersecurity efforts. The Department of Homeland Security has helped secure the nation's critical infrastructure through developing security policy and coordinating security initiatives, among other efforts. Other agencies have established initiatives to gather intelligence and share actual or possible cyberattack information. Multiple agencies have mechanisms in place to assist in responding to cyberattacks, and law enforcement components, including the Federal Bureau of Investigation, are responsible for investigating them.

The White House's September 2018 *National Cyber Strategy* and the NSC's accompanying June 2019 *Implementation Plan* detail the executive branch's approach to managing the nation's cybersecurity. When evaluated together, these documents addressed several of the desirable characteristics of national strategies, but lacked certain key elements for addressing others.

***National Cyber Strategy* and *Implementation Plan* are Missing Desirable Characteristics of a National Strategy**

Characteristic	Cyber Strategy and Plan Coverage of Issue
Purpose, scope, and methodology	Addressed
Organizational roles, responsibilities, and coordination	Addressed
Integration and implementation	Addressed
Problem definition and risk assessment	Did not fully address
Goals, subordinate objectives, activities, and performance measures	Did not fully address
Resources, investments, and risk management	Did not fully address

Source: GAO analysis of 2018 *National Cyber Strategy and* 2019 *Implementation Plan*. | GAO-20-629

For example, the *Implementation Plan* details 191 activities that federal entities are to undertake to execute the priority actions outlined in the *National Cyber Strategy*. These activities are assigned a level, or tier, based on the coordination efforts required to execute the activity and the extent to which NSC staff is expected to be involved. Thirty-five of these activities are designated as the highest level (tier 1), and are coordinated by a functional entity within the NSC. Ten entities are assigned to lead or co-lead these critical activities while also tasked to lead or co-lead lower tier activities.

What GAO Recommends

GAO is making one matter for congressional consideration, that Congress should consider legislation to designate a leadership position in the White House with the commensurate authority to implement and encourage action in support of the nation's cybersecurity.

GAO is also making one recommendation to the National Security Council to work with relevant federal entities to update cybersecurity strategy documents to include goals, performance measures, and resource information, among other things. The National Security Council neither agreed nor disagreed with GAO's recommendation.

Leadership Roles for Federal Entities Assigned as Leads or Co-Leads for *National Cyber Strategy Implementation Plan* Activities

Entity	Tier 1 Activities	Tier 2 Activities	Tier 3 Activities
National Security Council	15	7	3
Department of Homeland Security	14	19	15
Office of Management and Budget	7	6	5
Department of Commerce	5	9	35
Department of State	2	5	11
Department of Defense	1	6	17
Department of Justice	1	10	5
Department of Transportation	1	0	5
Executive Office of the President	1	0	0
General Services Administration	1	2	1

Source: GAO analysis of 2018 *National Cyber Strategy* and 2019 *Implementation Plan*. | GAO-20-629

Although the *Implementation Plan* defined the entities responsible for leading each of the activities; it did not include goals and timelines for 46 of the activities or identify the resources needed to execute 160 activities. Additionally, discussion of risk in the *National Cyber Strategy* and *Implementation Plan* was not based on an analysis of threats and vulnerabilities. Further, the documents did not specify a process for monitoring agency progress in executing *Implementation Plan* activities. Instead, NSC staff stated that they performed periodic check-ins with responsible entities, but did not provide an explanation or definition of specific level of NSC staff involvement for each of the three tier designations. Without a consistent approach to engaging with responsible entities and a comprehensive understanding of what is needed to implement all 191 activities, the NSC will face challenges in ensuring that the *National Cyber Strategy* is efficiently executed.

GAO and others have reported on the urgency and necessity of clearly defining a central leadership role in order to coordinate the government's efforts to overcome the nation's cyber-related threats and challenges. The White House identified the NSC staff as responsible for coordinating the implementation of the *National Cyber Strategy*. However, in light of the elimination of the White House Cybersecurity Coordinator position in May 2018, it remains unclear which official ultimately maintains responsibility for not only coordinating execution of the *Implementation Plan*, but also holding federal agencies accountable once activities are implemented. NSC staff stated responsibility for duties previously attributed to the White House Cyber Coordinator were passed to the senior director of NSC's Cyber directorate; however, the staff did not provide a description of what those responsibilities include. NSC staff also stated that federal entities are ultimately responsible for determining the status of the activities that they lead or support and for communicating implementation status to relevant NSC staff. However, without a clear central leader to coordinate activities, as well as a process for monitoring performance of the *Implementation Plan* activities, the White House cannot ensure that entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and ultimately overcome this urgent challenge.