GAO@100

Highlights

Highlights of GAO-21-236, a report to congressional requesters

March 2021

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation

Why GAO Did This Study

Threats to the nation's critical infrastructures and the information technology systems that support them require a concerted effort among federal agencies; state, local, tribal, and territorial governments; and the private sector to ensure their security. The seriousness of the threat was reinforced by the December 2020 discovery of a cyberattack that has had widespread impact on government agencies, critical infrastructures, and private-sector companies.

Federal legislation enacted in November 2018 established CISA to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructures in the face of both physical and cyber threats. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.

GAO was asked to review CISA's organizational transformative initiative and its ability to coordinate effectively with stakeholders. The objectives of GAO's review were to (1) describe CISA's organizational transformation initiative, (2) assess the current progress of the initiative, (3) determine the extent to which CISA's transformation efforts align with key practices for effective agency reform, and (4) identify any challenges in CISA's coordination with stakeholders, and assess strategies the agency has developed to address such challenges.

View GAO-21-236. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Nathan Anderson at (206) 287-4804 or andersonn@gao.gov.

What GAO Found

To implement the requirements of the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018, CISA leadership within the Department of Homeland Security launched an organizational transformation initiative. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency. (See figure 1 below.) CISA completed the first two of three phases of its organizational transformation initiative, which resulted in, among other things, a new organization chart, consolidation of multiple incident response centers, and consolidation of points of contact for infrastructure security stakeholders. Phase three is intended to fully implement the agency's planned organizational changes.

Figure 1: Five Key Responsibilities Assigned to the Cybersecurity and Infrastructure Security Agency (CISA)

- Secure federal information and information systems
- Coordinate national efforts to secure and protect against critical infrastructure risks
- Coordinate with federal and nonfederal entities, including international partners
- Respond to requests from critical infrastructure owners and operators with analysis, expertise, and other technical assistance as needed
- Carry out emergency communications responsibilities under existing law

Source: GAO analysis of the CISA Act of 2018; images: Buffaloboy/stock.adobe.com. | GAO-21-236

While CISA intended to fully implement the transformation by December 2020, it had completed 37 of 94 planned tasks for phase three by mid-February 2021. Among the tasks not yet completed, 42 of them were past their most recent planned completion dates. Included in these 42 are the tasks of finalizing the mission-essential functions of CISA's divisions and issuing a memorandum defining incident management roles and responsibilities across CISA. Tasks such as these appear to be critical to CISA's transformation initiative and accordingly its ability to effectively and efficiently carry out its cyber protection mission. In addition, the agency had not established an updated overall deadline for completing its transformation initiative. Until it establishes updated milestones and an overall deadline for its efforts, and expeditiously carries out these plans, CISA will be hindered in meeting the goals of its organizational transformation initiative. This in turn may impair the agency's ability to identify and respond to incidents, such as the cyberattack discovered in December 2020 that caused widespread damage.

To do this, GAO reviewed relevant information on CISA's efforts to develop an organizational transformation initiative to meet the requirements of the CISA Act of 2018. To assess the progress of CISA's efforts, GAO analyzed agency documentation to determine the status of activities related to the three phases of the organizational transformation and reasons for any delays in its progress. GAO also assessed CISA's efforts against selected key practices identified by GAO that can contribute to the effectiveness of agency reform efforts. In addition, GAO interviewed selected stakeholders related to CISA's primary mission areas to identify any pertinent challenges and analyzed strategies CISA developed to address these challenges.

What GAO Recommends

GAO is making 11 recommendations to CISA:

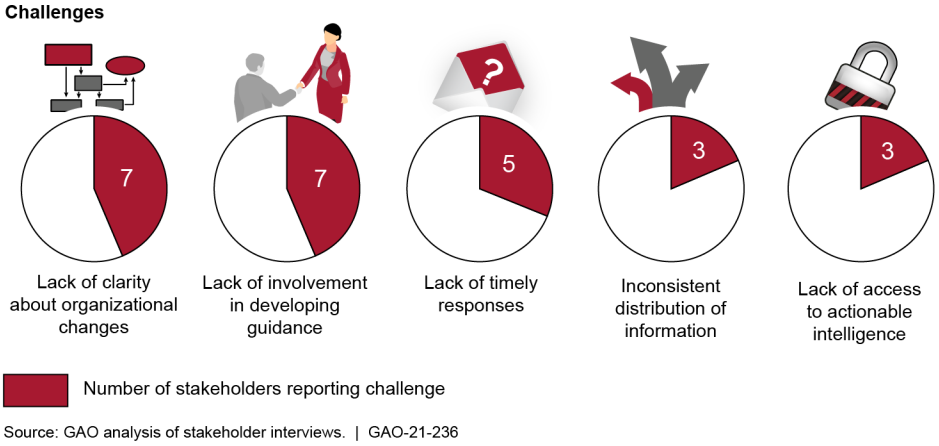
- Establish new expected completion dates for the phase three tasks that are past their completion dates, with priority given to tasks critical to mission effectiveness.
- Establish an overall deadline for the completion of the transformation initiative.
- Fully address each of the six reform practices that have been either partially or not addressed.
- Develop strategies to mitigate each of the three infrastructure challenges that remain outstanding.

The Department of Homeland Security agreed with GAO's recommendations.

Of 10 selected key practices for effective agency reforms previously identified by GAO, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. For example, CISA generally addressed practices related to using data and evidence to support its planned reforms and engaging its employees in the organizational change process. The agency partially addressed practices related to, for example, defining goals and outcomes and conducting workforce planning. Workforce planning is especially important for CISA, given the criticality of hiring and retaining experts who, among other things, can help identify and respond to complex attacks. CISA did conduct an initial assessment of its cybersecurity workforce in 2019; however, it is still working on analyzing capability gaps and determining how to best fill those gaps. Finally, CISA did not address the practice of ensuring that its employee performance management system was aligned with its new organizational structure and transformation goals. Until it fully addresses workforce planning and the five other practices that are either partially or not addressed, CISA's ability to leverage its organizational changes to effectively carry out its mission will be hindered.

Selected government and private-sector stakeholders from the 16 sectors considered to be critical infrastructures, such as banking and financial institutions, telecommunications, and energy, reported a number of challenges in coordinating with CISA. (See figure 2.)

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



Source: GAO analysis of stakeholder interviews. | GAO-21-236

CISA has activities under way to mitigate some of these challenges, including tracking stakeholder inquiries to monitor the timeliness of responses and delivering briefings with intelligence tailored to stakeholder needs. However, it has not developed strategies to clarify changes to its organizational structure, have consistent stakeholder involvement in the development of guidance, and distribute information to all key stakeholders. Organizational structure and information distribution are both considered new challenges associated with the reorganization of CISA. Developing strategies to mitigate these challenges could help provide CISA with assurance that its stakeholders are receiving the information and support needed to make decisions about risks facing the nation's critical infrastructures.