June 5, 2024

CYBERSECURITY

Efforts Initiated to Harmonize Regulations, but Significant Work Remains

Highlights of GAO-24-107602, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

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 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.

GAO initially identified cybersecurity as a High-Risk area in 1997 and expanded it in 2003 to include critical infrastructure cybersecurity. Due to the persistent threat and need for urgent action, GAO continues to view the area as high risk.

Because the private sector owns most of the nation's critical infrastructure, it is vital that the public and private sectors work together to protect these assets and systems. However, according to ONCD, when critical infrastructure sectors are subject to multiple cybersecurity regulations, the result can be conflicting guidance, inconsistencies, and redundancies.

GAO was asked to testify on harmonizing cybersecurity regulations. This testimony summarizes the Administration's current efforts to address cybersecurity regulatory harmonization.

This statement is based on prior GAO reports and public information, as of May 2024, regarding the Administration's plans to harmonize regulations.

View GAO-24-107602. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

What GAO Found

Harmonization refers to the development and adoption of more consistent standards and regulations. Such consistency is important when critical infrastructure sectors are subject to multiple cybersecurity regulations. According to the White House, harmonizing regulatory requirements can lead to better security outcomes at lower costs.

Without harmonization, adverse impacts can occur. For example, GAO reported in 2020 that four federal agencies had established cybersecurity requirements for states to follow in securing data. However, these requirements had conflicting parameters such as the number of unsuccessful log-on attempts prior to locking out users. The percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent. Slightly more than half of state officials surveyed said that such requirements led to a great increase or very great increase in the time and staff hours needed to address the conflicts. GAO made 12 recommendations to agencies; eight of them are implemented and four are not including two priority ones to the Office of Management and Budget to ensure agencies collaborate on requirements and state cybersecurity assessments.

Recognizing the importance of harmonizing cybersecurity regulations for our nation's critical infrastructure sectors, the Administration and Congress have begun relevant initiatives.

- **National cybersecurity strategy and implementation plan.** In March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and an accompanying implementation plan. Among other things, the strategy and implementation plan identified the need to establish an initiative on cyber regulatory harmonization but did not provide a time frame for completing subsequent actions to harmonize regulations.
- **Request for information on cybersecurity regulation harmonization.** In August 2023, the Office of the National Cyber Director (ONCD) issued a request for information seeking input on challenges with cybersecurity regulatory overlap and received over 100 public comments. ONCD has not published a summary of the comments.
- **National security memorandum on critical infrastructure security and resilience.** In April 2024, the Administration released *National Security Memorandum-22 on Critical Infrastructure Security and Resilience*. The memorandum calls for the Department of Homeland Security (DHS) to develop a plan to harmonize cybersecurity regulations as part of a national plan for infrastructure risk management, which is to be issued by April 2025.
- **Cyber incident reporting legislation.** The Cyber Incident Reporting for Critical Infrastructure Act was enacted in 2022 to help prioritize efforts to combat cyber threats by requiring certain entities to submit cyber incident reports to DHS. Pursuant to the act, in September 2023, DHS issued a report with eight recommendations and three proposed legislative changes to streamline and harmonize cyber incident reporting.

These key initial steps can inform the broader effort to harmonize cybersecurity regulations. Following through and executing specific plans and meeting established time frames are essential to achieving harmonization.