GAO Highlights

Highlights of GAO-24-106917, a report to congressional addressees

July 2024

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements

Why GAO Did This Study

Cybersecurity incidents involving critical infrastructure sectors—the sectors whose assets, systems, and networks provide essential services—cost the United States billions of dollars annually and cause significant disruptions. To provide increased visibility into the growing cyber threats to critical infrastructure, Congress and the President enacted a law on cyber incident reporting. This law calls for DHS to address 13 requirements by March 2024, including publishing a proposed rule for certain entities to submit reports on cyber incidents and ransom payments to DHS.

The law also includes a provision for GAO to report on the implementation of the act. This report (1) examines the extent to which DHS has implemented the act's requirements and (2) describes efforts DHS has made to identify and mitigate challenges with meeting the act's requirements.

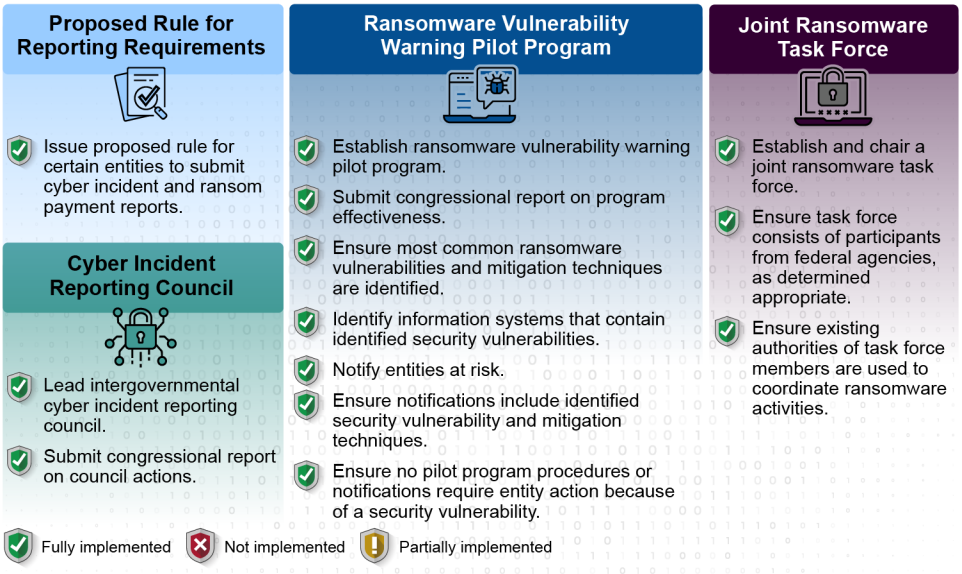
To do so, GAO identified 59 requirements in the act that DHS was responsible for implementing. Of those, 13 requirements were due by March 2024. GAO organized the requirements into four categories: proposed rule for reporting requirements, cyber incident reporting council, ransomware pilot program, and joint ransomware task force. GAO then analyzed the department's implementation of the 13 requirements. GAO also summarized documentation and testimonial evidence regarding challenges DHS faced in implementing the act's requirements and its mitigation plans.

View GAO-24-106917. For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has implemented the 13 requirements from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the act) that were due by March 2024. Specifically, DHS's Cybersecurity and Infrastructure Security Agency (CISA) submitted a proposed rule related to cyber incident reporting requirements to the Federal Register in March 2024, and it was published in April 2024. DHS plans to issue the final rule by October 2025. In addition, the department implemented the remaining 12 requirements (see figure). As a result of these efforts, DHS should be better positioned to coordinate the federal government cybersecurity and mitigation efforts more effectively, as intended by the act. Additionally, DHS should be better positioned to assist entities with defending against cyber incidents on the critical infrastructure.

Extent to Which the Department of Homeland Security (DHS) Implemented 13 Applicable Cyber Incident Reporting for Critical Infrastructure Act of 2022 Requirements



Sources: GAO (shield icons), lovemask/stock.adobe.com (all other icons); starlineart/stock.adobe.com (background). | GAO-24-106917

DHS identified a variety of challenges in implementing the act and is taking steps to address them. These challenges are related to harmonizing cyber incident reporting requirements, addressing cyber incident review responsibilities, and facilitating a more efficient method for federal agencies to begin sharing cyber incident reports. DHS noted that it has taken several mitigation steps to address these challenges, such as (1) identifying four recommendations for federal agencies and three proposals to Congress to address duplicative reporting requirements; (2) updating its technologies; and (3) hiring additional staff to facilitate the review, analysis, and sharing of reports. If implemented effectively, the four recommendations and three proposals can further mitigate challenges and help standardize incident reporting.