GAO Highlights

Highlights of GAO-22-105103, a report to congressional committees

February 2022

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Assess Adoption of Cybersecurity Guidance

Why GAO Did This Study

The nation's 16 critical infrastructure sectors provide essential services such as banking, electricity, and gas and oil distribution. However, increasing cyber threats—like the May 2021 ransomware cyberattack on an American oil pipeline system that led to regional gas shortages—represent a significant national security challenge. To better protect against cyber threats, NIST facilitated, as required by federal law, the development of a voluntary framework of cybersecurity standards and procedures for sectors to use.

The *Cybersecurity Enhancement Act of 2014* included provisions for GAO to review aspects of the framework. GAO's report addresses the extent to which SRMAs have (1) determined framework adoption by entities within their respective sectors and (2) identified improvements resulting from sector-wide use. GAO analyzed documentation, such as requests for information, polls, and survey instruments. It also conducted interviews with agency officials from each SRMA and NIST.

What GAO Recommends

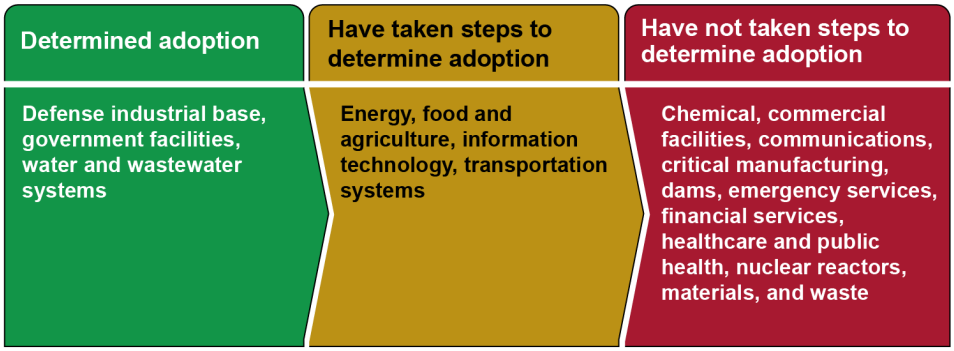
In prior reports, GAO recommended that the nine SRMAs (1) develop methods for determining the level and type of framework adoption by entities across their respective sectors and (2) collect and report sector-wide improvements. Most agencies have not yet implemented these recommendations.

View GAO-22-105103. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

What GAO Found

Federal agencies with a lead role to assist and protect one or more of the nation's 16 critical infrastructures are referred to as sector risk management agencies (SRMAs). The SRMAs for three of the 16 have determined the extent of their sector's adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (framework). In doing so, lead agencies took actions such as developing sector surveys and conducting technical assessments mapped to framework elements. SRMAs for four sectors have taken initial steps to determine adoption (see figure). However, lead agencies for nine sectors have not taken steps to determine framework adoption.

Status of Framework Adoption by Critical Infrastructure Sector



Source: GAO analysis based on agency data. | GAO-22-105103

Regarding improvements resulting from sector-wide use, five of the 16 critical infrastructure sectors' SRMAs have identified or taken steps to identify sector-wide improvements from framework use, as GAO previously recommended. For example, the Environmental Protection Agency identified an approximately 32 percent overall increase in the use of framework-recommended cybersecurity controls among the 146 water utilities that requested and received voluntary technical assessments. In addition, SRMAs for the government facilities sector identified improvements in cybersecurity performance metrics and information standardization resulting from federal agencies' use of the framework. However, SRMAs for the remaining 11 sectors did not identify improvements and were not able to describe potential successes from their sectors' use of the framework.

SRMAs reported various challenges to determining framework adoption and identifying sector-wide improvements. For example, they noted limitations in knowledge and skills to implement the framework, the voluntary nature of the framework, other priorities that may take precedence over framework adoption, and the difficulty of developing precise measurements of improvement were challenges to measuring adoption and improvements. To help address challenges, NIST launched an information security measurement program in September 2020 and the Department of Homeland Security has an information network that enables sectors to share best practices. Implementing GAO's prior recommendations on framework adoption and improvements are key factors that can lead to sectors pursuing further protection against cybersecurity threats.