February 2020

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions Needed to Identify Framework Adoption and Resulting Improvements

GAO Highlights

Highlights of GAO-20-299, a report to congressional committees

Why GAO Did This Study

Cyber threats to the nation's critical infrastructure (e.g., financial services and energy sectors) continue to increase and represent a significant national security challenge. To better address such threats, NIST developed, as called for by federal law, a voluntary framework of cybersecurity standards and procedures.

The *Cybersecurity Enhancement Act of 2014* included provisions for GAO to review aspects of the framework. The objectives of this review were to determine the extent to which (1) SSAs have developed methods to determine framework adoption and (2) implementation of the framework has led to improvements in the protection of critical infrastructure from cyber threats. GAO analyzed documentation, such as implementation guidance, plans, and survey instruments. GAO also conducted semi-structured interviews with 12 organizations, representing six infrastructure sectors, to understand the level of framework use and related improvements and challenges. GAO also interviewed agency and private sector officials.

What GAO Recommends

GAO is making ten recommendations—one to NIST on establishing time frames for completing selected programs—and nine to the SSAs to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed and one partially agreed. GAO continues to believe that all ten recommendations are warranted.

View GAO-20-299. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

Most of the nine agencies with a lead role in protecting the 16 critical infrastructure sectors, as established by federal policy and referred to as sector-specific agencies (SSAs), have not developed methods to determine the level and type of adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (framework), as GAO previously recommended. Specifically, two of the nine SSAs had developed methods and two others had begun taking steps to do so. The remaining five SSAs did not yet have methods to determine framework adoption. Most of the sectors (13 of 16), however, noted that they had taken steps to encourage and facilitate use of the framework, such as developing implementation guidance that links existing sector cybersecurity tools, standards, and approaches to the framework. In addition, all of the 12 selected organizations that GAO interviewed described either fully or partially using the framework. Nevertheless, implementing GAO's recommendations to the SSAs to determine the level and type of adoption remains essential to the success of protection efforts.

The 12 selected organizations using the framework reported varying levels of resulting improvements. Such improvements included identifying risks and implementing common standards and guidelines. However, the SSAs have not collected and reported sector-wide improvements. The SSAs and organizations identified impediments to doing so, including the (1) lack of precise measurements of improvement, (2) lack of a centralized information sharing mechanism, and (3) voluntary nature of the framework. NIST and the Department of Homeland Security (DHS) have initiatives to help address these impediments.

- Precise measurements: NIST is in the process of developing an information security measurement program that aims to provide the tools and guidance to support the development of information security measures that are aligned with an individual organization's objectives. However, NIST has not established a time frame for the completion of the measurement program.
- Centralized sharing: DHS identified its homeland security information network as a tool that was intended to be the primary system that could be used by all sectors to report on best practices, including sector-wide improvements and lessons learned from using the framework.
- Voluntary nature: In April 2019, NIST issued its *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, version 1.1, which included a tool for organizations to self-assess how effectively they manage cybersecurity risks and identify improvement opportunities.

While these initiatives are encouraging, the SSAs have not yet reported on sector-wide improvements. Until they do so, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructures from threats will be largely unknown.