GAO Highlights

Highlights of GAO-18-211, a report to congressional committees

February 2018

# CRITICAL INFRASTRUCTURE PROTECTION

## Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption

## Why GAO Did This Study

Our nation's critical infrastructure includes the public and private systems and assets vital to national security, economic stability, and public health and safety. Federal policy identifies 16 critical infrastructure sectors, including the financial services, energy, transportation, and communications sectors. To better address cyber-related risks to critical infrastructure, in 2014, NIST developed, as called for by federal law and policy, *the Framework for Improving Critical Infrastructure Cybersecurity,* a voluntary framework of cybersecurity standards and procedures for industry to adopt.

The Cybersecurity Enhancement Act of 2014 included provisions for GAO to review aspects of the cybersecurity standards and procedures in the framework developed by NIST. GAO's objective was to assess what is known about the extent to which critical infrastructure sectors have adopted the framework. To do so, GAO analyzed documentation, such as sector-specific guidance and tools to facilitate implementation, and interviewed relevant federal and nonfederal officials from the 16 critical infrastructure sectors.

## What GAO Recommends

GAO is making nine recommendations that methods be developed for determining framework adoption by the sector-specific agencies across their respective sectors, in consultation with their respective sector partner(s), such as the sector coordinating councils, the Department of Homeland Security, and NIST, as appropriate. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed.

View GAO-18-211. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

## What GAO Found

Most of the 16 critical infrastructure sectors took action to facilitate adoption of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* by entities within their sectors. Federal policy directs nine federal lead agencies—referred to as sector-specific agencies (SSA)—in consultation with the Department of Homeland Security and other agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

In response, guidance for 12 of the 16 sectors for implementing the cybersecurity framework was developed. In addition, nonfederal led sector coordinating councils took additional steps to facilitate framework adoption. For example, 3 sectors that developed implementation guidance encouraged the alignment of the framework with existing cybersecurity guidelines used within their respective sectors.

Nevertheless, officials from the Department of Homeland Security, NIST, SSAs, and the sector coordinating councils identified four challenges to cybersecurity framework adoption, as reported by entities within their respective sectors. Specifically, some entities

- May be limited in their ability to commit necessary resources towards framework adoption.
- May not have the necessary knowledge and skills to effectively implement the framework.
- May face regulatory, industry, and other requirements that inhibit adopting the framework.
- May face other priorities that take precedence over conducting cyber-related risk management or adopting the framework.

Further, the nation's plan for national critical infrastructure protection efforts states that federal and nonfederal sector partners (including SSAs) are to measure the effectiveness of risk management goals by identifying high-level outcomes and progress made toward national goals and priorities, including securing critical infrastructure against cyber threats. However, none of the SSAs had measured the cybersecurity framework's implementation by entities within their respective sectors. None of the 16 coordinating councils reported having qualitative or quantitative measures of framework adoption because they generally do not collect specific information from entities about critical infrastructure protection activities. SSA officials also stated that the voluntary nature and other factors are impediments to collecting such information. While other entities, including a trade association and universities, had attempted to determine the use of the framework within certain sectors; none of those efforts yielded results that would articulate a sector-wide level of framework adoption.

Until SSAs have a more comprehensive understanding of the use of the cybersecurity framework by entities within the critical infrastructure sectors, they will be limited in their ability to understand the success of protection efforts or to determine where to focus limited resources for cyber risk mitigation.