December 2015

CRITICAL INFRASTRUCTURE PROTECTION

Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework

GAO Highlights

Highlights of GAO-16-152, a report to congressional committees

Why GAO Did This Study

U.S. critical infrastructures, such as financial institutions and communications networks, are systems and assets vital to national security, economic stability, and public health and safety. Systems supporting critical infrastructures face an evolving array of cyber-based threats. To better address cyber-related risks to critical infrastructure, federal law and policy called for NIST to develop a set of voluntary cybersecurity standards and procedures that can be adopted by industry to better protect critical cyber infrastructure.

The Cybersecurity Enhancement Act of 2014 included provisions for GAO to review aspects of the cybersecurity standards and procedures developed by NIST. This report determines the extent to which (1) NIST facilitated the development of voluntary cybersecurity standards and procedures and (2) federal agencies promoted these standards and procedures. GAO examined NIST's efforts to develop standards, surveyed a non-generalizable sample of critical infrastructure stakeholders, reviewed agency documentation, and interviewed relevant officials.

What GAO Recommends

GAO recommends that DHS develop metrics to assess the effectiveness of its framework promotion efforts. In addition, DHS and GSA should set a time frame to determine whether implementation guidance is needed for the government facilities sector. DHS and GSA concurred with the recommendations.

View GAO-16-152. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In accordance with requirements in a 2013 executive order which were enacted into law in 2014, the National Institute of Standards and Technology (NIST) facilitated the development of a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure. This process, which involved stakeholders from the public and private sectors, resulted in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. The framework is to provide a flexible and risk-based approach for entities within the nation's 16 critical infrastructure sectors to protect their vital assets from cyber-based threats. To develop the framework in a collaborative manner, NIST solicited input from sector stakeholders through a formal request for information and conducted multiple workshops with critical infrastructure owners and operators, industry associations, government agencies, and other stakeholders. Participants GAO surveyed were generally satisfied with the approach NIST took to develop the framework. Further, the framework meets the requirements established in federal law that it be flexible, repeatable, performance-based, and cost-effective. For example, the framework contains multiple implementation "tiers," which allows it to be adapted to an organization's specific conditions and needs.

Agencies with responsibilities for supporting protection efforts in critical infrastructure sectors (known as sector-specific agencies), and NIST have promoted and supported adoption of the cybersecurity framework in the critical infrastructure sectors. For example, the Department of Homeland Security (DHS) established the Critical Infrastructure Cyber Community Voluntary Program to encourage adoption of the framework and has undertaken multiple efforts as part of this program. These include developing guidance and tools that are intended to help sector entities use the framework. However, DHS has not developed metrics to measure the success of its activities and programs. Accordingly, DHS does not know if its efforts are effectively encouraging adoption of the framework.

Sector-specific agencies have also promoted the framework in their sectors by, for example, presenting to meetings of sector stakeholders and holding other promotional events. In addition, all of the sector-specific agencies except for DHS and the General Services Administration (GSA), as co-SSAs for the government facilities sector, had decided whether or not to develop tailored framework implementation guidance for their sectors, as required by Executive Order 13636. Specifically, DHS and GSA had not yet set a time frame to determine whether sector-specific implementation guidance is needed for the government facilities sector. By not doing so, DHS and GSA may be hindering the adoption of the cybersecurity framework in this sector.