July 2016

GAO Highlights

Highlights of GAO-16-791T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed

Why GAO Did This Study

Protecting the security of CI is a top priority for the nation. CI includes assets and systems, whether physical or cyber, that are so vital to the United States that their destruction would have a debilitating impact on, among other things, national security or the economy. Multiple federal entities, including DHS, are involved in assessing CI vulnerabilities, and assessment fatigue could impede DHS's ability to garner the participation of CI owners and operators in its voluntary assessment activities.

This testimony summarizes past GAO findings on progress made and improvements needed in DHS's vulnerability assessments, such as addressing potential duplication and gaps in these efforts.

This statement is based on products GAO issued from May 2012 through October 2015 and recommendation follow-up conducted through March 2016. GAO reviewed applicable laws, regulations, directives, and policies from selected programs. GAO interviewed officials responsible for administering these programs and assessed related data. GAO interviewed and surveyed a range of stakeholders, including federal officials, and CI owners and operators.

What GAO Recommends

GAO made recommendations to DHS in prior reports to strengthen its assessment efforts. DHS agreed with these recommendations and reported actions or plans to address them. GAO will continue to monitor DHS efforts to address these recommendations.

View GAO-16-791T. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov

What GAO Found

GAO's prior work has shown the Department of Homeland Security (DHS) has made progress in addressing barriers to conducting voluntary assessments but guidance is needed for DHS's critical infrastructure (CI) vulnerability assessments activities and to address potential duplication and gaps. For example:

Determining why some industry partners do not participate in voluntary assessments. In May 2012, GAO reported that various factors influence whether CI owners and operators participate in voluntary assessments that DHS uses to identify security gaps and potential vulnerabilities, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority CI declined to participate. GAO concluded that collecting data on the reason for declinations could help DHS take steps to enhance the overall security and resilience of high-priority CI crucial to national security, public health and safety, and the economy, and made a recommendation to that effect. DHS concurred and has taken steps to address the recommendation, including developing a tracking system in October 2013 to capture declinations.

Establishing guidance for areas of vulnerability covered by assessments. In September 2014, GAO reported that the vulnerability assessment tools and methods DHS offices and components use vary with respect to the areas of vulnerability—such as perimeter security—assessed depending on which DHS office or component conducts or requires the assessment. As a result it was not clear what areas DHS believes should be included in its assessments. GAO recommended that DHS review its vulnerability assessments to identify the most important areas of vulnerability to be assessed, and establish guidance, among other things. DHS agreed and established a working group in August 2015 to address this recommendation. As of March 2016 these efforts were ongoing with a status update expected in the summer of 2016.

Addressing the potential for duplication, overlap, or gaps between and among the various efforts. In September 2014, GAO found overlapping assessment activities and reported that DHS lacks a department-wide process to facilitate coordination among the various offices and components that conduct vulnerability assessments or require assessments on the part of owners and operators. This could hinder the ability to identify gaps or potential duplication in DHS assessments. GAO identified opportunities for DHS to coordinate with other federal partners to share information regarding assessments. In response to GAO recommendations, DHS began a process of identifying the appropriate level of guidance to eliminate gaps or duplication in methods and to coordinate vulnerability assessments throughout the department. GAO also recommended that DHS identify key CI security-related assessment tools and methods used or offered by other federal agencies, analyze them to determine the areas they capture, and develop and provide guidance for what areas should be included in vulnerability assessments of CI that can be used by DHS and other CI partners in an integrated and coordinated manner. DHS agreed, and as of March 2016, established a working group to address GAO recommendations.