March 26, 2014

CRITICAL INFRASTRUCTURE PROTECTION

Observations on Key Factors in DHS's Implementation of Its Partnership Approach

GAO Highlights

Highlights of GAO-14-464T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Federal efforts to protect the nation's critical infrastructure from cyber threats has been on GAO's list of high-risk areas since 2003. Critical infrastructure is assets and systems, whether physical or cyber, so vital to the United States that their destruction would have a debilitating impact on, among other things, national security and the economy. Recent cyber attacks highlight such threats. DHS, as the lead federal agency, developed a partnership approach with key industries to help protect critical infrastructure.

This testimony identifies key factors important to DHS implementation of the partnership approach to protect critical infrastructure.

This statement is based on products GAO issued from October 2001 to March 2014. To perform this work, GAO reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs. GAO interviewed DHS officials responsible for administering these programs and assessed related data. GAO also interviewed and surveyed a range of other stakeholders including federal officials, industry owners and operators, industry groups, and cybersecurity experts.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen its partnership efforts. DHS generally agreed with these recommendations and reports actions or plans to address many of them. GAO will continue to monitor DHS efforts to address these recommendations.

View GAO-14-464T. For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov, or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

GAO's prior work has identified several key factors that are important for the Department of Homeland Security (DHS) to implement its partnership approach with industry to protect critical infrastructure. DHS has made some progress in implementing its partnership approach, but has also experienced challenges coordinating with industry partners that own most of the critical infrastructure.

- **Recognizing and Addressing Barriers to Sharing Information.** Since 2003, GAO has identified information sharing as key to developing effective partnerships. In July 2010, GAO reported some barriers affecting the extent to which cyber-related security information was being shared between federal and industry partners. For example, industry partners reported concerns that sharing sensitive, proprietary information with the federal government could compromise their competitive advantage if shared more widely. Similarly, federal partners were restricted in sharing classified information with industry officials without security clearances. GAO recommended that DHS work with industry to focus its information-sharing efforts. DHS concurred and has taken some steps to address the recommendation, including sponsoring clearances for industry.

- **Sharing Results of DHS Assessments with Industry.** GAO has found that DHS security assessments can provide valuable insights into the strengths and weaknesses of critical assets and drive industry decisions about investments to enhance security. In a May 2012 report, GAO found that DHS was sharing the results of its assessments with industry partners, but these results were often late, which could undermine the relationship DHS was attempting to develop with these partners. GAO recommended that DHS develop time frames and milestones to ensure the timely delivery of the assessments to industry partners. DHS concurred and reported that it has efforts underway to speed the delivery of its assessments.

- **Measuring and Evaluating Performance of DHS Partnerships**. GAO's prior work found that taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In an April 2013 report, GAO examined DHS's chemical security program and assessed, among other things, the extent to which DHS has communicated and worked with industry owners and operators to improve security. GAO reported that DHS had increased its efforts to communicate and work with industry to help them enhance security at their facilities. However, GAO found that DHS was not obtaining systematic feedback on its outreach. GAO recommended that DHS explore opportunities and take action to systematically solicit and document feedback on industry outreach. DHS concurred and reported that it had taken action to address the recommendation.

However, the cyber security of infrastructure remains on GAO's high-risk list and more needs to be done to accelerate the progress made. DHS still needs to fully implement the many recommendations on its partnership approach (and other issues) made by GAO and inspectors general to address cyber challenges.