April 2013

COMMUNICATIONS NETWORKS

Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-275, a report to congressional requesters

Why GAO Did This Study

Ensuring the effectiveness and reliability of communications networks is essential to national security, the economy, and public health and safety. The communications networks (including core and access networks) can be threatened by both natural and human-caused events, including increasingly sophisticated and prevalent cyber-based threats. GAO has identified the protection of systems supporting the nation's critical infrastructure—which includes the communications sector—as a government-wide high-risk area.

GAO was asked to (1) identify the roles of and actions taken by key federal entities to help protect communications networks from cyber-based threats, (2) assess what is known about the extent to which cyber incidents affecting the communications networks have been reported to the FCC and DHS, and (3) determine if Defense's pilot programs to promote cybersecurity in the defense industrial base can be used in the communications sector. To do this, GAO focused on core and access networks that support communication services, as well as critical components supporting the Internet. GAO analyzed federal agency policies, plans, and other documents; interviewed officials; and reviewed relevant reports.

What GAO Recommends

GAO recommends that DHS collaborate with its partners to develop outcome-oriented measures for the communications sector. DHS concurred with GAO's recommendation.

View GAO-13-275. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

While the primary responsibility for protecting the nation's communications networks belongs to private-sector owners and operators, federal agencies also play a role in support of their security, as well as that of critical components supporting the Internet. Specifically, private-sector entities are responsible for the operational security of the networks they own, but the Federal Communications Commission (FCC) and the Departments of Homeland Security (DHS), Defense, and Commerce have regulatory and support roles, as established in federal law and policy, and have taken a variety of related actions. For example, FCC has developed and maintained a system for reporting network outage information; DHS has multiple components focused on assessing risk and sharing threat information; Defense and DHS serve as co-chairs for a committee on national security and emergency preparedness for telecommunications functions; and Commerce has studied cyber risks facing the communications infrastructure and participates in standards development. However, DHS and its partners have not yet initiated the process for developing outcome-based performance measures related to the cyber protection of key parts of the communications infrastructure. Outcome-based metrics related to communications networks and critical components supporting the Internet would provide federal decision makers with additional insight into the effectiveness of sector protection efforts.

No cyber-related incidents affecting core and access networks have been recently reported to FCC and DHS through established mechanisms. Specifically, both FCC and DHS have established reporting mechanisms to share information on outages and incidents, but of the outages reported to FCC between January 2010 and October 2012, none were related to common cyber threats. Officials within FCC and the private sector stated that communication networks are less likely to be targeted themselves because they provide the access and the means by which attacks on consumer, business, and government systems can be facilitated.

Attributes of two pilot programs established by Defense to enhance the cybersecurity of firms in the defense industrial base (the industry associated with the production of defense capabilities) could be applied to the communications sector. (See table below.) The department's pilot programs involve partnering with firms to share information about cyber threats and responding accordingly. Considering these attributes can inform DHS as it develops procedures for expanding these pilot programs to all critical infrastructure sectors, including the communications sector.

Relevant Attributes of the Defense Industrial Base Cyber Pilots
Agreements
Government sharing of unclassified and classified cyber threat information
Feedback mechanism on government services
Government cyber analysis, mitigation, and digital forensic support
Government reporting of voluntarily reported incidents
Internet service providers deploying countermeasures based on classified threat indicators for organizations

Source: GAO analysis of Defense and DHS data.