June 2008

CRITICAL INFRASTRUCTURE PROTECTION

Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-607, a report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Technological advances have led to an increasing convergence of previously separate networks used to transmit voice and data communications. While the benefits of this convergence are enormous, such interconnectivity also poses significant challenges to our nation's ability to respond to major disruptions. Two operations centers—managed by the Department of Homeland Security's (DHS) National Communications System and National Cyber Security Division—plan for and monitor disruptions on voice and data networks. In September 2007, a DHS expert task force made three recommendations toward establishing an integrated operations center that the department agreed to adopt. To determine the status of efforts to establish an integrated center, GAO reviewed documentation, interviewed relevant DHS and private sector officials, and reviewed laws and policies to identify DHS's responsibilities in addressing convergence.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security complete (1) its strategic plan and (2) define tasks and milestones for completing remaining integration steps. DHS concurred with GAO's first recommendation. With regard to the second, DHS stated it supports integrating overlapping functions, but does not support merging the centers. However, there is strong evidence supporting the need to merge the centers to enhance incident response.

To view the full product, including the scope and methodology, click on GAO-08-607. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

DHS has taken the first of three steps toward integrating its centers that are responsible for planning for, monitoring, and responding to disruptions to the communications infrastructure, including voice and data networks, and the security of data and applications that use these networks. Specifically, in November 2007, it moved the operations center for communications infrastructure (NCC Watch) to office space adjacent to the center for data and applications (US-CERT). This close proximity allows the approximately 41 coordination center and 95 readiness team analysts to, among other things, readily collaborate on planned and ongoing activities. In addition, the centers have jointly acquired common software tools to identify and share physical, telecommunications, and cyber information related to performing their missions. For example, the centers use one of the tools to develop a joint "morning report" specifying their respective network security issues and problems, which is used by the analysts in coordinating responses to any resulting disruptions.

While DHS has completed the first integration step, it has yet to implement the remaining two steps. Specifically, although called for in the task force's recommendations, the department has not organizationally merged the two centers or invited key private sector critical infrastructure officials to participate in the planning, monitoring, and other activities of the proposed joint operations center. A key factor contributing to DHS's lack of progress in implementing the latter two steps is that completing the integration has not been a top DHS priority. Instead, DHS officials stated that their efforts have been focused on other initiatives, most notably the President's recently announced cyber initiative, which is a federal governmentwide effort to manage the risks associated with the Internet's nonsecure external connections. Nevertheless, DHS officials stated that they are in the process of drafting a strategic plan to provide overall direction for the activities of the National Communications System and the National Cyber Security Division. However, the plan is in draft and has been so since mid-2007. In addition, DHS officials could not provide a date for when it would be finalized. Consequently, the department does not have a strategic plan or related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the two remaining integration steps.

Until DHS completes the integration of the two centers, it risks being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need.