September 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-825, a report to congressional requesters

Why GAO Did This Study

Federal policies establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace. As part of its responsibilities, DHS is required to coordinate cyber attack exercises to strengthen public and private incident response capabilities. One major exercise program, called Cyber Storm, is a large-scale simulation of multiple concurrent cyber attacks involving the federal government, states, foreign governments, and private industry. To date, DHS has conducted Cyber Storm exercises in 2006 and 2008.

GAO agreed to (1) identify the lessons that DHS learned from the first Cyber Storm exercise, (2) assess DHS's efforts to address the lessons learned from this exercise, and (3) identify key participants' views of their experiences during the second Cyber Storm exercise. To do so, GAO evaluated documentation of corrective activities and interviewed federal, state, and private sector officials.

What GAO Recommends

GAO is recommending that DHS schedule and complete the corrective activities identified to address lessons learned during the first Cyber Storm exercise, many of which were reiterated during the second Cyber Storm exercise. In written comments, DHS agreed with this recommendation and reported on its efforts to complete corrective activities.

To view the full product, including the scope and methodology, click on GAO-08-825. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

As a result of its first Cyber Storm exercise, in February 2006, DHS identified eight lessons that had significant impact across sectors, agencies, and exercise participants. These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

While DHS has demonstrated progress in addressing the lessons it learned from its first Cyber Storm exercise, more remains to be done to fully address the lessons. In the months following its first exercise, DHS identified 66 activities that address one or more of the lessons, including hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry, and refining their operating procedures. To date, DHS has completed a majority of these activities (see table). However, key activities have not yet been completed. Specifically, DHS identified 16 activities as ongoing and 7 activities as planned for the future. Further, while DHS has identified completion dates for its planned activities, it has not identified completion dates for its ongoing activities. Until DHS schedules and completes its remaining activities, the agency risks conducting subsequent exercises that repeat the lessons learned during the first exercise.

Commenting on their experiences during the second Cyber Storm exercise, in March 2008, participants observed both progress and continued challenges in building a comprehensive national cyber response capability. Their observations addressed several key areas, including the value and scope of the exercise, roles and responsibilities, public relations, communications, the exercise infrastructure, and the handling of classified information. For example, many participants reported that their organizations found value in the exercise because it led them to update their contact lists and improve their response capabilities. Other participants, however, reported the need for clarifying the role of the law enforcement community during a cyber incident and for improving policies governing the handling of classified information so that key information can be shared. Many of the challenges identified during Cyber Storm II were similar to challenges identified during the first exercise.

Summary of Status of Activities

Status of DHS activities	Number of activities
Reported and validated as completed	42
Reported as completed, but not validated due to insufficient evidence	1
Reported as ongoing	16
Reported as planned for the future	7
Total	**66**

Source: GAO analysis of DHS data.