Fact Sheet: Cyber Storm Exercise

Release Date: September 13, 2006

Cyber Storm Exercise Report *(PDF, 23 pages - 667 KB)*

The U.S. Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) successfully executed Cyber Storm, the first national cyber exercise Feb. 6 thru Feb. 10, 2006. The exercise was the first government-led, full-scale cyber security exercise of its kind. NCSD, a division within the department's Preparedness Directorate, provides the federal government with a centralized cyber security coordination and preparedness function called for in the National Strategy for Homeland Security, the National Strategy to Secure Cyberspace and Homeland Security Presidential Directive 7. NCSD is the focal point for the federal government's interaction with state and local government, the private sector and the international community concerning cyberspace vulnerability reduction efforts.

Goals and Objectives

Cyber Storm was designed to test communications, policies and procedures in response to various cyber attacks and to identify where further planning and process improvements are needed. Activities included:

- Exercising interagency coordination through the activation of the National Cyber Response Coordination Group (NCRCG) and the Interagency Incident Management Group (IIMG)
- Exercising inter-governmental and intra-governmental coordination and incident response
- Identifying policies and issues that either hinder or support cyber security requirements
- Identifying public and private information sharing mechanisms to address communications challenges
- Identifying the interdependence of cyber and physical infrastructures
- Raising awareness of the economic and national security impacts associated with a significant cyber incident
- Highlighting available tools and technologies for cyber incident response and recovery

Participants

- Participants included federal and state agencies and private sector partners from the IT, telecommunications, energy, and transportation industries, as well as foreign governments
- Participants provided support staff to help plan and control the exercise, and to ensure that their organizations' objectives were met

The Scenario

The exercise simulated a sophisticated cyber attack campaign through a series of scenarios directed at several critical infrastructure sectors. The intent of these scenarios was to highlight the interconnectedness of cyber systems with physical infrastructure and to exercise coordination and communication between the public and private sectors. Each scenario was developed with the assistance of industry experts and was executed in a closed and secure environment.

Cyber Storm scenarios had three major adversarial objectives:

- To disrupt specifically targeted critical infrastructure through cyber attacks
- To hinder the governments' ability to respond to the cyber attacks
- To undermine public confidence in the governments' ability to provide and protect services

The exercise was a simulated event with no real-world effects on, tampering with, or damage to any critical infrastructure. While the scenarios were based on hypothetical situations, they were not intended as a forecast of future terrorist-related events.

Related Information

DHS Releases Cyber Storm Public Exercise Report, September 13, 2006