Homeland Security

CYBER STORM
NATIONAL CYBER EXERCISE

Fact Sheet

Cyber Storm II National Cyber Exercise

In March 2008, the Department of Homeland Security's National Cyber Security Division (NCSD) will sponsor its second large-scale national cyber exercise, Cyber Storm II. Planned in close coordination with and driven by its stakeholders and participants, the exercise will center on a cyber-focused scenario that will escalate to the level of a cyber incident requiring a coordinated Federal response. Exercises such as Cyber Storm II are critical in maintaining and strengthening cross-sector, inter-governmental and international relationships, enhancing processes and communications linkages, as well as ensuring continued improvement to cyber security procedures and processes. Cyber Storm II is part of Homeland Security's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector.

As the DHS biennial National Cyber Exercise, the goal of Cyber Storm II is to examine the processes, procedures, tools, and organizational response to a multi-sector coordinated attack through, and on, the global cyber infrastructure.

Objectives

- Examine the capabilities of participating organizations to prepare for, protect from, and respond to the potential effects of cyber attacks
- Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures
- Validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information
- Examine means and processes through which to share sensitive information across boundaries and sectors, without compromising proprietary or national security interests

Cyber Storm II will also provide an opportunity to exercise newly developed government and private sector concepts and processes since Cyber Storm I, such as Concepts of Operations and Standard Operating Procedures.

Scenario

The adversary in Cyber Storm II will utilize coordinated cyber and physical attacks on critical infrastructures within selected sectors to meet a specific political and economic agenda. These cyber attacks will be simulated and will not impact any live networks.

Participants

Participation in Cyber Storm II includes Federal, State, local, and international governments, including Australia, Canada, New Zealand, and the United Kingdom. In addition, private sector players from the Information Technology (IT), Transportation (Rail and Pipe), and Chemical sectors along with multiple Information Sharing and Analysis Centers (ISACs) are scheduled to participate.

For additional information on Cyber Storm exercises, please contact Jon Noetzel at Jonathan.Noetzel@associates.dhs.gov. For media inquires, please contact the DHS Press Office at 202-282-8010.