DHS Conducts First Full-Scale Cyber Security Exercise to Enhance Nation's Cyber Preparedness

Release Date: 02/10/06 00:00:00

For Immediate Release
Office of the Press Secretary
Contact: 202-786-9899
February 10, 2006

Washington, DC -- U.S. Department of Homeland Security (DHS) announced the completion of Cyber Storm, the first full-scale government-led cyber security exercise to examine response, coordination, and recovery mechanisms to a simulated cyber-event within international, federal, state, and local governments, in conjunction with the private sector. In total, 115 public, private, and international agencies, organizations, and companies were involved in the planning and implementation of Cyber Storm.

"Cyber security is critical to protecting our nation's infrastructure because information systems connect so many aspects of our economy and society," said George W. Foresman, DHS Under Secretary for Preparedness. "Preparedness against a cyber attack requires partnership and coordination between all levels of government and the private sector. Cyber Storm provides an excellent opportunity to enhance our nation's cyber preparedness and better manage risk."

Cyber Storm emphasizes the Administration's commitment to cyber security and preparedness. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures. For example, one of the scenarios simulated a cyber incident where a utility company's computer system is breached, causing numerous disruptions to the power grid. The intent of this scenario is to highlight the interconnectedness of cyber security with the physical infrastructure and to exercise coordination and communication between the public and private sectors. Each of the scenarios was developed with the assistance of industry experts and was executed in a closed and secure environment.

Cyber Storm exercised national cyber incident response within the context of a large-scale cyber incident affecting the energy, information technology, telecommunications, and transportation sectors. Capabilities examined, include:

- Interagency coordination through the National Cyber Response Coordination Group;
- Identification of policy issues that affect response and recovery;
- Identification of critical information sharing paths and mechanisms among public and private sectors; and
- Improvement and promotion of public and private sector interaction.

Organizations that participated in this exercise in addition to the DHS include:

- Department of Commerce
- Department of Defense
- Department of Energy
- Department of State
- Department of Transportation
- Department of Treasury
- Department of Justice
- Director of National Intelligence
- Central Intelligence Agency
- National Security Agency
- National Security Council
- Homeland Security Council
- States of Michigan, Montana and New York
- FBI
- U.S. Secret Service
- NORTHCOM
- American Red Cross
- Canada (PSEP-C)

The exercise was a simulated event, and there were no real world effects on, tampering with, or damage to any critical infrastructure. While the exercise scenario was based on a hypothetical situation, it was not intended as a forecast of

future terrorist threats.

Cyber Storm participants included members of the public sector (federal and state agencies), the private sector (information technology, telecommunications, energy and transportation firms selected by Industry Information Sharing and Analysis Centers (ISACs) and Sector Specific Agencies (SSAs)), and select international government partners.

The National Cyber Security Division (NCSD), a part of the department's new Preparedness Directorate, provides the federal government with a centralized cyber security coordination and preparedness function. The 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.