National Cyber Security Division Cyber Exercise Program

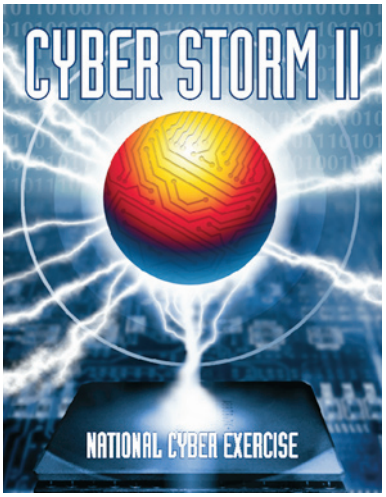
The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. The **National Cyber Security Division (NCSD)** is the Department's lead agency for securing cyberspace and our Nation's cyber assets and networks.

Critical infrastructures are dependent on information technology systems and computer networks for essential operations. Particular emphasis should be placed on the reliability and resiliency of the systems that comprise and interconnect these infrastructures. NCSD collaborates with partners from across public, private, and international communities to advance this goal by developing and implementing coordinated security measures to protect against physical and cyber threats.

NCSD also seeks to assess and mitigate cyber vulnerabilities, and to integrate cyber security best practices into national preparedness and response efforts. In addition to the Department's principal national-level exercise series Cyber Storm, NCSD focuses on developing proactive measures in areas such as critical infrastructure protection, incident response, software assurance, control systems security, stakeholder awareness, and training and education.

NCSD Cyber Exercises Enhance Cyber Preparedness

The **NCSD–Cyber Exercise Program (CEP)** improves the Nation's cyber security readiness, protection, and incident response capabilities by developing, designing, and conducting cyber exercises and workshops at the State, Federal, regional, and international level. The NCSD-CEP employs scenario-based exercises that focus on risks to the cyber and information technology infrastructure.



Through exercises, participants are able to validate policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations (COOP). The controlled environment allows stakeholders to safely explore real-world situations, to improve communication and coordination, and to advance the efficacy of the broad-based critical infrastructure protection partnership.

Building Relationships through Exercises

Exercises are an effective tool to assess preparedness and to identify areas for improvement absent the consequences of an actual incident. By engaging in the full exercise process – from planning through evaluation – participants are also able to establish and strengthen relationships that result in improved awareness, policy development, and information sharing. The NCSD-CEP engages public and private sector partners in the planning process so that scenarios and objectives reflect the input and requirements of all involved.

The interconnected nature of cyberspace and the interdependencies between critical infrastructures demand this kind of diverse involvement by partner and stakeholder organizations. From emergency managers, homeland security advisors, state and local government officials, to law enforcement, private sector owners and operators as well as academia, media outlets, and community groups, the NCSD-CEP creates an environment for all of these partners to avail themselves of the different perspectives and mutually beneficial relationships that emerge through the exercise process.

Homeland Security

NCSD Exercise Activities

As a leader in cyber exercise design and facilitation, NCSD-CEP has created an array of exercise approaches to address a range of threats, scenarios, and partner capabilities. The NCSD-CEP is committed to fostering an environment for information sharing and collaboration across the full spectrum of partner groups and jurisdictions. The NCSD-CEP complies with the DHS Homeland Security Exercise Evaluation Program Guidelines (HSEEP) for the development and execution of its exercises, and shares lessons learned through the DHS Lessons Learned Information Sharing portal (LLIS).

Examples of NCSD-CEP exercise efforts:

- **Cyber Storm Exercise Series:** The National Cyber Exercise Series - Cyber Storm - improves incident response and coordination capabilities by assessing communications, coordination, and relationships in response to a large-scale cyber incident. The program focuses on simulated cyber-specific threat scenarios intended to highlight critical infrastructure interdependencies and further integrate Federal, State, international and private sector response and recovery efforts. As the Department's cyber exercise sponsor, NCSD hosted the first Cyber Storm exercise in February 2006, and the second in March 2008. The Cyber Storm series was created to support the goals laid out in both the National Strategy to Secure Cyberspace and Homeland Security Presidential Directive 8.

- **State Exercises:** The NCSD-CEP facilitates the design of tabletop and functional exercises at the State level. Upon request, NCSD-CEP provides subject matter expertise to States to help familiarize emergency managers and incident responders with roles, responsibilities, policies, plans, and procedures related to cyber incidents.

- **Federal Exercises:** The NCSD-CEP actively participates in planning and executing intra- and inter-agency national level exercises requiring a coordinated Federal response under the National Response Framework (NRF). This planning includes coordination with the Federal Emergency Management Agency (FEMA) exercise initiatives, the TOP OFFICIALS exercise series (TOPOFF), and other federal agency exercises as appropriate. The NCSD-CEP also plans exercises with the National Cyber Response and Coordination Group (NCRCG), a forum of 13 principal agencies that coordinates intra-governmental preparedness operations for responding to large-scale cyber attacks.

- **Regional Coalitions:** The NCSD-CEP engages with regional partners to manage and mitigate cyber risks. The NCSD-CEP has facilitated and participated in several tabletop exercises in the Gulf Coast, Pacific Northwest, and Northeast regions to strengthen all-hazards and cross-sector response and to mitigate the consequences of cyber incidents.

- **International Partnerships:** The international community recognizes that cyberspace does not adhere to political or geographical boundaries. The CEP supports efforts to improve international cooperation on cyber security topics through bilateral and multi-lateral efforts. The NCSD-CEP also leads exercise workshops at a variety of international conferences to advance cyber security coordination strategies worldwide.

For more information please visit:

- *National Cyber Security Division:* **www.dhs.gov/xabout/structure/editorial_0839.shtm**
- *United States Computer Emergency Readiness Team (US-CERT):* **www.us-cert.gov**
- *DHS Homeland Security Exercise Evaluation Program (HSEEP):* **www.hseep.dhs.gov**
- *DHS Lessons Learned Information Sharing (LLIS):* **www.llis.dhs.gov**