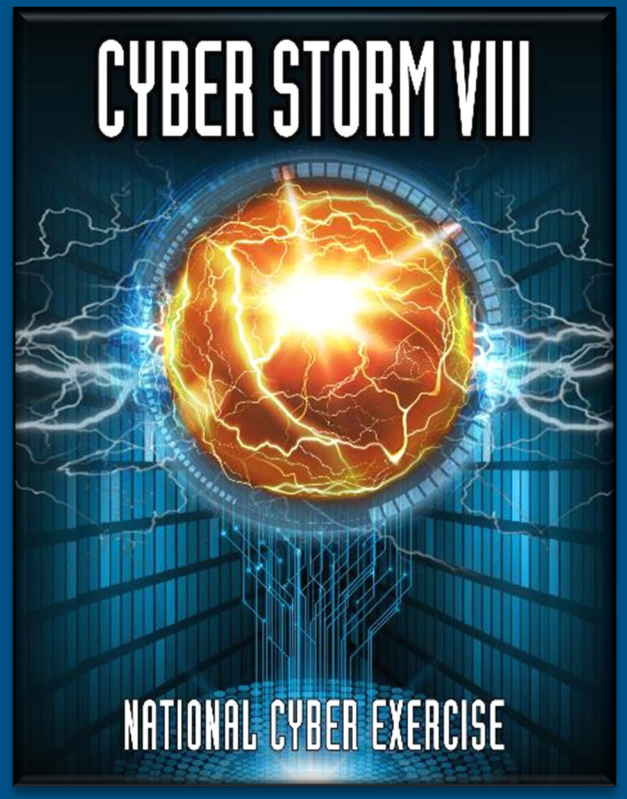
NATIONAL CYBER EXERCISE: CYBER STORM VIII (CS VIII)

STATES WORKING GROUP
OVERVIEW BRIEF



Security Protocol

- Traffic Light Protocol (TLP): **TLP:AMBER**
- For reference purposes and additional information on TLP; https://www.us-cert.gov/sites/default/files/tlp/tlp-v1-letter.pdf

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed
AMBER	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm
GREEN	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels
WHITE	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction

CS Exercise Series Overview

What Is The CS Exercise Series?

- CISA sponsored exercise focused on policy, procedure, information sharing, coordination, and decision-making (i.e., no actual attacks)
- Provides a venue to simulate discovery of and response to a large-scale, coordinated significant cyber incident impacting critical infrastructure

Who Participates?

- Organizations interested in improving cyber readiness and resilience
- Within organizations, CS is designed for any staff involved in cyber incident response to include staff responding to subsequent physical impacts (e.g., technical, crisis communicators, legal staff, business continuity/ emergency management teams, leadership, etc.)

How Does Planning Work?

- Participants identify a lead planner to plug into the established planning structure, collaborating with the CS VIII Planning Team over the course of approximately a year to develop and apply a core scenario that is applicable across participants
- Collaboration largely occurs at five major planning meetings and via teleconferences

How Does The Exercise Work?

- An exercise control (ExCon) cell composed of CS VIII Planning Team members and organizational representatives run, manage, and track the exercise
- Players participate from their actual work locations and receive exercise “injects” that describe scenario impacts to their organization and respond according to policy and procedure

CS VIII Value of Participation

Work with counterparts across the private sector, and state, national and international government to better understand, evaluate, and improve cyber incident response capabilities

Exercise your organization's cyber incident response and coordination capabilities, and meet your organization's specific training objectives as part of a large and complex cyber exercise

Have a voice in both the interpretation of the exercise findings, and in the recommendation of courses of action to improve national and international cyber readiness and resilience

CS VIII Participation Structure

- Participation levels across and within Working Groups will vary based on resources, real-world incident response roles, and the projected applicability of scenario play. Participation levels include:
  - **Victim Organizations:** Receive customized scenario injects (developed by organizational planners) and are directly affected by the incident during the exercise. Typical victim organizations include critical infrastructure, state, and international participants
  - **Monitor and Respond (M/R) Organizations:** Monitor events during exercise execution, responding as appropriate to a victim organization's actions. Typical M/R organizations include law enforcement, intelligence entities, DoD, federal departments and agencies, and coordination bodies (e.g., Information Sharing and Analysis Centers/Organizations [ISACs/ISAOs], etc.)
- Both victim and M/R organizations are encouraged to actively participate throughout the planning, execution, and evaluation process

CS VIII Working Groups

Draft Working Groups

- **CI*** Working Group(s)
- **Federal** Working Group
- **States** Working Group
- **CISA** Working Group
- **LE/I/DoD*** Working Group
- **International** Working Group

- The CS participant set is divided into Working Groups to support planning and collaboration among specific communities of interest (e.g., CI, federal, LE/I/DoD, states, and international partners)
- Each organization is aligned to a primary Working Group with a CS VIII Planning Team Lead – this is where the bulk of planning occurs

**CI (Critical Infrastructure), LE/I/DoD (Law Enforcement/Intelligence/Department of Defense)*

CS VIII Planning Timeline

**Master Scenario Events List (MSEL)*

CS VIII Next Steps

- **To Confirm Participation:**
  - Confirm participation with the CS VIII Planning Team
  - Identify a Lead Planner to represent your organization

- **To Support General Planning Goals:**
  - Identify additional organizations to recruit and provide contact information (e.g., vendors, key partners, etc.)
  - Develop individual objectives – what does success look like?
  - Participate in the CS VIII MPM, scheduled for September 16, 2021

For more information

Gary Benedict
Section Lead, National Exercises
Cyber Exercises Branch, CISA
gary.benedict@cisa.dhs.gov
202-494-3487

Marshall Garnuette
Support Team
Cyber Storm VIII
garnuette_marshall@bah.com
443-764-5898

John Foti
Support Team
Cyber Storm VIII
foti_john@bah.com
703-902-5865

Nathaniel Pendleton
Support Team
Cyber Storm VIII
pendleton_nathaniel@bah.com
703-377-6403

Cyber Storm Mailbox
cyberstorm@hq.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY