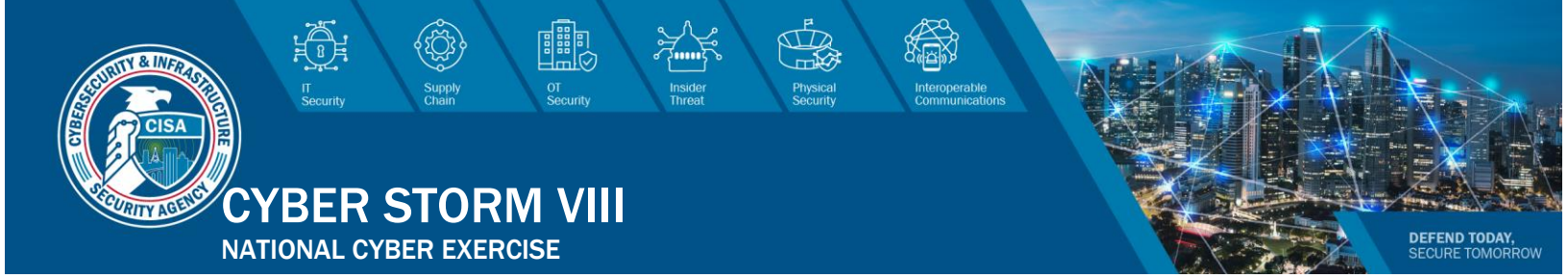
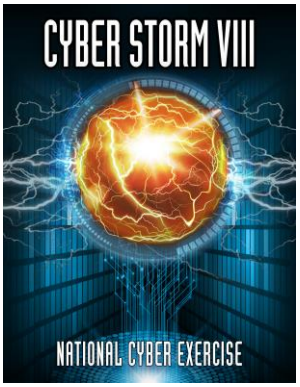


THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) SPONSORS THE BIENNIAL CYBER STORM (CS) EXERCISE SERIES, THE NATION'S MOST EXPANSIVE CYBER EXERCISE, PARTERNING WITH ALL LEVELS OF GOVERNMENT AND THE PRIVATE SECTOR TO SECURE AGAINST THE EVOLVING RISKS OF TOMORROW.



BACKGROUND

The CS exercise series provides a venue for the Federal Government, state and local government, the private sector, and international partners to come together to simulate response to a large-scale, coordinated significant cyber incident impacting the Nation's critical infrastructure. Cyber Storm VIII (CS VIII), planned for Spring 2022, will allow participants to exercise their incident response plans and identify opportunities for coordination and information sharing. CS exercises have historically engaged more than one thousand distributed players over the course of three days of live exercise play. Building on the success and momentum of Cyber Storm 2020 (CS 2020) and lessons learned from real world events, CS VIII is positioned to meaningfully prepare participants for response to emerging and evolving threats.

ENHANCING CYBER INCIDENT RESPONSE CAPABILITIES

The cyber threat landscape continues to expand and advance, requiring the public and private sectors to constantly evaluate their cyber incident response capabilities. Building on the outcomes of previous iterations, CS VIII will examine all aspects of cyber incident response to include potential or actual physical impacts of a coordinated cyberattack targeting critical infrastructure. CS provides a unique opportunity for organizations to not only evaluate their internal cyber incident response plans, but also coordinate with those at the sector, state, and federal levels. Together, participants will identify areas for growth and improvement to strengthen their cyber resiliency.

The CS Exercise Series:

CS VIII PARTICIPATION

- CS includes organizations across the private sector and state, national, and international governments. Within participating organizations, any staff involved in cyber incident response may participate.
- Participating organizations have the opportunity to work directly with CISA to understand CISA's role and capabilities in a cyberattack.
- Participants operate in working groups which provide them a single point of contact on the CS Planning Team to help meet organization- and sector-specific objectives and improve coordination capabilities through the exercise.
- Benefits of participation include improved understanding of current cyber risks, awareness of incident response resources, strengthened relationships with counterparts, and refined communications strategies.

CS VIII Working Groups

CS VIII GOAL AND OBJECTIVES

CS VIII's primary goal is to strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.

The exercise allows participants to stress-test their response capabilities absent of the consequences of a real-world event (there are no actual system attacks). Participants play from their regular work locations and operate within the responsibilities of their real-world role, communicating through standard channels as well as exercise channels as needed.

CS VIII's specific objectives include:

1. Examine the effectiveness of national cybersecurity plans and policies
2. Explore the roles and responsibilities during a cyber incident with potential or actual physical impacts
3. Strengthen information sharing and coordination mechanisms used during a cyber incident
4. Foster public and private partnerships and improve their ability to share relevant and timely information across partners

PAST HIGHLIGHTS

The CS exercise series has evolved over time in step with the dynamic nature of cyber threats and the maturation of cyber incident response plans and policies. During CS 2020, more than two thousand distributed players from over 210 organizations across critical infrastructure sectors exercised incident response procedures in a remote environment. CS 2020 raised awareness of long-standing and ongoing vulnerabilities in the core infrastructure of the Internet.

CS VIII PLANNER ROLES AND RESPONSIBILITIES

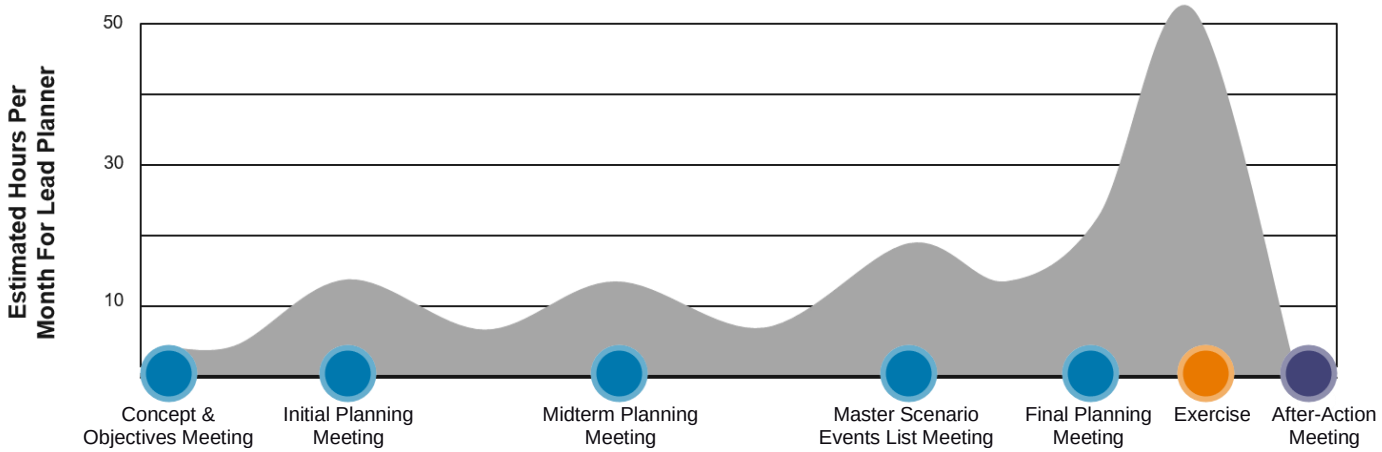
CS planners serve as the primary point of contact for all planning interactions for their organization. Planners represent either a Victim Organization or a Monitor and Respond (M/R) Organization according to resources, real-world cyber incident response roles, and the projected applicability of scenario play. Planners will have varying responsibilities based on their organization's level of play.

- **Victim Organization:** Receive customized scenario injects (developed by organizational planners) and are directly affected by the incident during the exercise. Typical victim organizations include critical infrastructure organizations, state departments and agencies, federal departments and agencies, and international participants.
- **M/R Organization:** 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.

[1] Law Enforcement/Intelligence/Department of Defense (LE/I/DoD)

ESTIMATED TIME COMMITMENT FOR CS VIII PLANNERS

CS VIII participation is scalable, and it is up to the individual organization to determine level of play (i.e., number of players, internal objectives to examine, scenario impacts, inject complexity, etc.). An organization's level of play will impact the time commitment required by a lead planner(s) during exercise planning, exercise execution, and the after-action process.



Planning Activities Include:

Participating in teleconferences and planning meetings, reviewing documents and providing input/updates, creating injects, and coordinating internally to identify and staff participants

Exercise Activities Include:

Participating in exercise meetings, reviewing injects and emails, and coordinating with Exercise Control (ExCon) and participants as needed

After-Action Activities Include:

Participating in meetings and reviewing the After-Action Reports (AAR) and CS Annexes as needed

FREQUENTLY ASKED QUESTIONS

- **What is the goal of CS VIII?** The CS VIII goal is to strengthen cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.
- **Who is participating in CS VIII?** CS VIII plans to engage partner organizations across federal, state, and local governments, the International Watch and Warning Network (IWWN), and critical infrastructure sectors, such as Chemical, Communications, Dams, Information Technology (IT), Water and Wastewater Systems, and Transportation's Pipeline Systems subsector.
- **Who from my organization participates?** CS is designed for any staff involved in an organization's cyber incident response (e.g., technical experts, crisis communicators, legal staff, or leadership).
- **Does CS attack live networks?** CS provides a venue to simulate discovery of and response to a large-scale, coordinated significant cyber incident impacting critical infrastructure (i.e., no actual attacks).
- **When will CS VIII take place?** CS VIII execution is slated for Spring 2022.
- **How does the exercise work?** The CS VIII Planning Team and organizational representatives run, manage, and track the exercise from an ExCon cell located in the Washington, D.C. area. 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.
- **Will CISA release any publicly available lessons learned following the exercise?** Exercise outcomes and findings will be developed collaboratively across the CS VIII participant community. A final report will be published on CISA.gov after the exercise.

For more information on CS VIII, please contact cyberstorm@hq.dhs.gov.