CYBER STORM IX
National Cyber Exercise

Cyber Storm (CS), the congressionally mandated National Cyber Exercise, sponsored by the Cybersecurity and Infrastructure Security Agency (CISA), represents one of the few opportunities for the Federal Government, state and local government, the private sector, and international partners to come together and address cyber response as a whole community. Now on its ninth iteration, Cyber Storm IX (CS IX) will help critical infrastructure sectors and government participants exercise their internal incident response policies and external coordination and information sharing capabilities.

CS IX PARTICIPATION

CS IX includes organizations across federal, state, and international governments and the private sector. Participating organizations will work directly with CISA to understand CISA's role and capabilities in a cyberattack. Participants operate in working groups to meet organization- and sector-specific objectives and improve coordination capabilities through the exercise.

| Federal | Critical Infrastructure | States | CISA | LE/I/DoD* | International |

Law Enforcement/Intelligence/Department of Defense)

CS IX VALUE OF PARTICIPATION

❖ Work with partners across the private sector, and state, national and international government during the National Cyber Exercise 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

❖ Foster relationships with counterparts across the public and private sector in an immersive and interactive exercise that replicates the challenges of cyber incident response in a no-fault learning environment

❖ Improve cyber readiness and resilience by having a voice in the interpretation of the exercise findings and recommendations that are leveraged to inform national cybersecurity policy

CS IX: A FIRST LOOK

Building on the success and momentum of Cyber Storm VIII (CS VIII), CS IX is slated to be the nation's most extensive cyber exercise to date. CS IX will provide a venue to:

❖ **Evaluate** and **improve** the capabilities of the cyber response community

❖ **Promote** public-private partnerships and strengthen relationships

❖ **Integrate** critical infrastructure partners, while providing an opportunity for CS veterans to return

❖ **Build** on outcomes of previous exercises

❖ Provide a venue to **examine** cyber-physical interdependencies

❖ **Incorporate** past-participant feedback on desired elements for inclusion

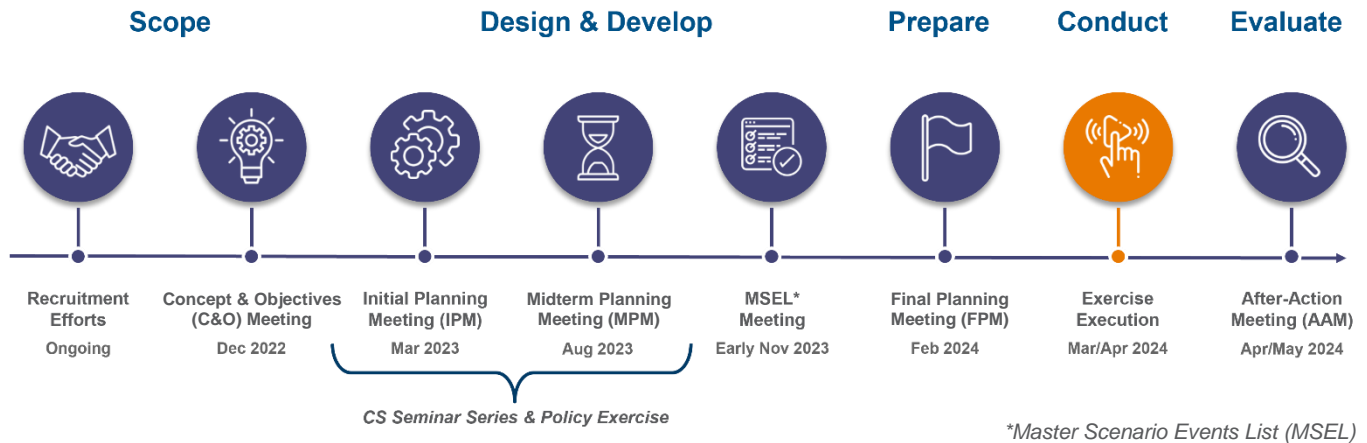## FOR MORE INFORMATION, PLEASE CONTACT:

Gary Benedict
Section Lead, National Exercises
National Cyber Exercise Program
CISA
gary.benedict@cisa.dhs.gov

Cyber Storm Mailbox
cyberstorm@cisa.dhs.gov

CS IX INITIAL PLANNING TIMELINE

Scope   **Design & Develop**   **Prepare**   **Conduct**   **Evaluate**

Recruitment Efforts	Concept & Objectives (C&O) Meeting	Initial Planning Meeting (IPM)	Midterm Planning Meeting (MPM)	MSEL* Meeting	Final Planning Meeting (FPM)	Exercise Execution	After-Action Meeting (AAM)
Ongoing	Dec 2022	Mar 2023	Aug 2023	Early Nov 2023	Feb 2024	Mar/Apr 2024	Apr/May 2024

CS Seminar Series & Policy Exercise

Master Scenario Events List (MSEL)

The CS IX planning process is divided into five phases to support the planning, execution, and evaluation. Within each phase, a series of events, milestones, and general planning goals move the process forward.

CS EXERCISE SERIES

Exercised **14 of the 16** critical infrastructure sectors

over 12,000 Participants

260⁺ Private sector organizations

17 Partner nations

40 States

70 Federal departments and agencies

More than **65** critical infrastructure sector coordination bodies

FREQUENTLY ASKED QUESTIONS

❖ **Who is participating in CS IX?** CS IX plans to engage partner organizations across federal, state, and local governments, the International Watch and Warning Network (IWWN), and critical infrastructure sectors, such as Communications and Information Technology (IT).

❖ **Who from my organization participates?** CS is designed for any staff involved in an organization's cyber incident response (e.g., technical, 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).

❖ **How does the exercise work?** The CS IX Planning Team and organizational representatives run, manage, and track the exercise from an exercise control (ExCon) cell located in the Washington, D.C. area. Players participate from their normal 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 IX participant community. A final report will be published on CISA.gov after the exercise. To view past CS after-action reports, go to https://www.cisa.gov/cyber-storm-securing-cyber-space