CYBER STORM IX

NATIONAL CYBER EXERCISE

BACKGROUND

The Cyber Storm 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. The series focuses on policy, procedure, information sharing, coordination, and decision-making.

Cyber Storm IX, the ninth iteration of the series, is scheduled for Spring 2024. Participants will exercise their cyber incident response plans and identify opportunities for coordination and information sharing in a simulated environment. Like previous iterations, Cyber Storm IX will engage over 2,000 distributed participants throughout three days of live exercise play. Cyber Storm IX will assess the most recent national cybersecurity guidance and clarify federal roles and responsibilities as cyber threats continue to evolve.

STRENGTHENING SECURITY PREPAREDNESS

Today's dynamic cyber threat environment requires constant reassessment of our nation's cyber incident response capabilities. Cyber Storm IX will examine all aspects of cyber incident response by depicting a coordinated cyberattack impacting critical infrastructure system confidentiality, integrity, and availability. Organizations will evaluate internal cyber incident response plans, while coordinating with those at the federal, state, local, and private sector levels. Throughout the exercise lifecycle, participants work together to identify applicable strengths and weaknesses, and ultimately find solutions to strengthen their cybersecurity preparedness.

Figure 1: Cyber Storm Exercise Series Benefits

CYBER STORM IX PARTICIPATION

Figure 2: Cyber Storm IX Participants

- Cyber Storm IX includes organizations across federal, state, and international governments, and the private sector
- Participating organizations 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
- Benefits of participation include exercising organizational response plans and capabilities, fostering relationships with counterparts, and improving organizational and national cyber readiness

*Law Enforcement/Intelligence/Department of Defense (LE/I/DoD)

CYBER STORM IX GOAL AND OBJECTIVES

Cyber Storm IX'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.**

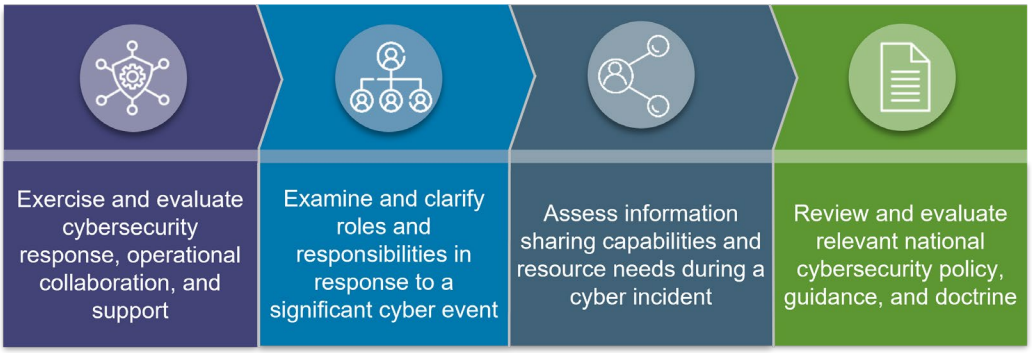

Figure 3: Cyber Storm IX Objectives

The exercise provides participants a safe, realistic environment to evaluate response capabilities without real-world ramifications through simulated attacks and impacts distributed as injects. Players react to the simulated injects from their regular workplaces and communicate through standard channels. The Cyber Storm IX planning team manages all aspects of play from a central exercise control location, while implementing a series of mechanisms to capture player response, player action, and findings to best evaluate systems and ultimately improve cyber resilience.

PAST HIGHLIGHTS

Figure 4: Cyber Storm Exercise Series History

Each iteration of the Cyber Storm exercise series builds on the previous to provide the most relevant environment possible for learning and advancement. In February 2006, the cyber response community came together for the first time in Cyber Storm I to examine the national response to cyber incidents. Cyber Storm IV included 15 building block exercises to help communities and states exercise cyber response capabilities for escalating incidents. The most recent iteration, Cyber Storm VIII, consisted of a multi-layered scenario that impacted both industrial control systems/operational technology and information technology networks, raising awareness of the rapidly expanding cyberattack surface. Cyber Storm IX will have a core scenario that challenges participants to improve their system preparedness against emerging threats.

For more information on the Cyber Storm exercise series, please visit CISA.gov/cyber-storm-securing-cyber-space or contact cyberstorm@cisa.dhs.gov.

Figure 5: Cyber Storm Exercise Series Historical Data