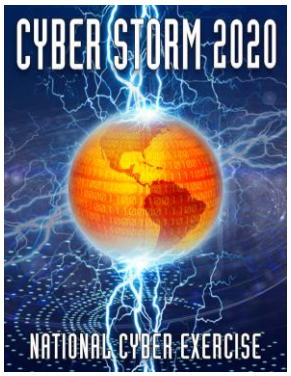
CYBER STORM 2020: NATIONAL CYBER EXERCISE

JULY 2020



BACKGROUND

Cyber Storm is the Cybersecurity and Infrastructure Security Agency's (CISA) national-level cyber exercise that brings together the public and private sector to simulate response to a cyber crisis impacting the nation's critical infrastructure. Designed to assess cybersecurity preparedness and examine incident response processes, procedures, and information sharing, the exercise provides a venue for players to simulate the discovery of and response to a widespread coordinated cyberattack, absent the consequences of a real-world event. With more than one thousand players nationwide participating in three days of live exercise play, Cyber Storm is the nation's most extensive cybersecurity exercise series. Cyber Storm 2020 represents the seventh iteration of the National Cyber Exercise.

QUICK FACTS

Date	Duration	Location	# of Players	Types of Players
Summer 2020	3 days of live play	Virtual across distributed player work locations	1,000+	All types of cyber incident responders (technical, IT, operations, product, legal, communication, leadership)

ENHANCING CYBER INCIDENT RESPONSE CABABILITIES

The dynamic nature of cybersecurity threats demands consistent review and assessment of the nation's cyber incident response capabilities. Cyber Storm provides a unique venue where aspects of the nation's critical infrastructure – federal, state, and local entities along with the private sector owner and operators – can examine collective cyber incident response capabilities with the goal of identifying areas for growth and improvement.

Cyber Storm 2020:

- Builds upon the outcomes of previous exercises and changes to the cybersecurity landscape;
- Evaluates and improves the capabilities of the cyber response community;
- Promotes public-private partnerships and strengthens relationships; and
- Integrates new critical infrastructure partners, while providing an opportunity for Cyber Storm veterans to return.

PARTICIPATION BENEFITS

Previous participants realized benefits such as these through participation:

- Improved understanding of cyber risks within/across sectors
- Awareness of resources
- New and lasting relationships
- Operational familiarity with vendors and partners
- Refined communications strategies

CYBER STORM 2020 PARTICIPATION SNAPSHOT

Cyber Storm participation represents a diverse group of CISA stakeholders and includes organizations from the below communities of interest.

CYBER STORM 2020 GOAL AND OBJECTIVES

Cyber Storm 2020'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 cyberattack targeting critical infrastructure.

Cyber Storm 2020's specific objectives include:

- Examine the implementation and effectiveness of national cybersecurity plans and policies;
- Strengthen and enhance information sharing and coordination mechanisms used across the cyber ecosystem during a cyber incident;
- Reinforce public and private partnerships and improve their ability to share relevant and timely information; and
- Exercise communications aspects of cyber incident response to refine and mature communications strategies.

PAST HIGHLIGHTS

Cyber Storm I, 2006, marked the first time the cyber response community came together to examine the national response to cyber incidents.

Cyber Storm II, 2008, exercised individual response capabilities and leadership decision making.

Cyber Storm III, 2010, focused on response according to national-level frameworks and provided the first operational test of the National Cybersecurity and Communications Integration Center (NCCIC).

Cyber Storm IV included 15 building block exercises between 2011 and 2014 to help communities and states exercise cyber response capabilities for escalating incidents.

Cyber Storm V, 2016, included more than 1,000 distributed players and brought together new sectors, including retail and healthcare participants.

Cyber Storm VI, *2018,* focused on response to an incident affecting to non-traditional IT devices and included new participants from critical manufacturing and the automotive industry.