IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CISA Tabletop Exercise Packages

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) provides **CISA Tabletop Exercise Packages (CTEPs**) as a comprehensive resource designed to assist stakeholders in conducting their own exercises. CTEPs include pre-developed scenarios and module questions to discuss information sharing, response, and recovery elements. Partners can use CTEPs to initiate discussions within their organizations to assess their preparedness for a variety of threats and incidents.

Each package is customizable and includes sample exercise objectives, scenarios, and discussion questions along with a collection of references and resources to assist exercise planners. Available scenarios cover a broad array of physical security and cybersecurity topics, such as ransomware, natural disasters, pandemics, civil disturbances, industrial control systems, election security, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.

PROGRAM MATERIALS

Exercise Planner Guidance

The CTEP includes guidance documentation for exercise planners. These documents provide information about the program, guidance for planning and executing exercises, and an avenue for receiving feedback:

- **Welcome Letter –** The official introduction letter for the CTEP. This letter includes a brief description of the included documents and information on how to contact the CISA Exercises team.
- **Exercise Planner Handbook –** A guide for the exercise planers. This document provides step-by-step instructions on how to plan, develop, and execute the tabletop exercise.
- **Facilitator and Evaluator Handbook –** A guide for the facilitators and evaluators/data collectors. This document provides instructions and examples for facilitators and evaluators/data collectors to capture information and feedback during the exercise for use when developing the After-Action Report/Improvement Plan (AAR/IP).
- **Exercise Planner Feedback Form** – A feedback form for the exercise planners and the facilitator. This document provides a means to consolidate feedback on exercise improvement.

Exercise Design Templates

The CTEP provides the following templates for planners to use in planning, designing, and developing exercises for their communities of interest:

- **Invitation Letter Template –** A template for the planning team to use to draft an official invitation to exercise participants.
- **Exercise Brief Slide Deck Template –** A PowerPoint presentation the exercise facilitator uses (in conjunction with the Situation Manual) to guide players through scenario modules and discussion questions.
- **Participant Feedback Form Template –** A form that is used after the exercise to gather information, such as recommendations, key outcomes from the exercise, and feedback on the exercise design and conduct, from exercise players.
- **After-Action Report/Improvement Plan Template** – A Homeland Security Exercise and Evaluation Program (HSEEP)-aligned AAR/IP template to aid exercise planners and evaluators/data collectors in organizing and implementing the findings from the exercise.
- **Situation Manual –** A manual that provides the scenario, supporting background information, and suggested discussion questions for use in the exercise. Throughout the exercise, players should be encouraged to use the manual to supplement the information in the Exercise Brief Slide Deck.

RESOURCE ACCESS

The CTEP library includes more than 100 sample situation manuals addressing a variety of critical infrastructure sectors, threat vectors, and scenarios. These situation manuals are ready-made documents that stakeholders can use with minor editing or combine with other CTEP materials to create customized documents to fit the specific needs of the end users at all levels of an organization.

All CTEP products are available on the CISA Tabletop Exercise Packages page on the CISA.gov website. They are currently sorted by threat vector (i.e., cybersecurity, physical security, and convergence).

CISA Exercises continuously works to refine available CTEP materials and expand available scenarios to meet our partners' needs. To provide feedback on this material or suggest new scenarios, please contact CISA Exercises via the contact information below.

SCENARIOS

Active Threat

- COVID-19 Active Shooter
- COVID-19 Sensitive Information
- Hazardous Materials
- Potential Civil Unrest
- ***Chemical Sector*** – Active Shooter, Active Threat, Domestic Threat, Edged Weapon, Improvised Explosive Device (IED), Vehicle-Borne Improvised Explosive Device (VBIED), Vehicle Ramming, Fire as a Weapon, Unmanned Aerial System (UAS), Civil Unrest
- ***Commercial Facilities*** – Outdoor Events Edged Weapon, Outdoor Events Active Shooter, Outdoor Events VBIED & Hostage, Outdoor Events Hostage, Cruise Ship Incident, Indoor Performing Arts Theater
- ***Critical Manufacturing*** – Supply Chain Terrorist Threat, Supply Chain Border Closing
- ***Dams*** –Active Shooter
- ***Defense Industrial Base*** –VBIED
- ***Education*** – K-12 Education Active Threat
- ***Energy*** – Electricity Substation
- ***Food & Agriculture*** – Food Manufacturing Facility (Processing/Packaging/Production)
- ***Government Facilities*** – National Monuments & Icons
- ***Healthcare & Public Health*** – Suicide Bomber, Suspicious Package, VBIED
- ***Transportation*** – Maritime Domestic Terror

Cyber

- Insider Threat
- Elections: Early Voting Same Day or Election Day Registration
- Elections: Election Day Voting Machines
- Elections: Vote by Mail
- Ransomware: Industrial Controls
- Ransomware: Ransomware Third Party Vendor
- Ransomware: Vendor Phishing
- ***Chemical Sector*** – Cyber Attack
- ***Water & Wastewater Systems*** – Cyber Attack

Natural Disaster

- Hurricane
- Pandemic Recovery
- Wildfire
- ***Critical Manufacturing*** – Hurricane Supply Chain, Pandemic Supply Chain Disruption, Severe Flooding Supply Chain, Supply Chain Severe Winter Weather
- ***Emergency Services*** – ESS Disaster Access Management/Re-entry

Complex Coordinated Attack

- Violent Extremist
- ***Chemical Sector*** - Complex Coordinated Attack
- ***Commercial Facilities*** – Large Box Store, Gaming Industry
- ***Dams*** – Adversarial Threat
- ***Education*** – Higher Education Active Threat
- ***Food & Agriculture*** – Supply Chain

CONTACT INFORMATION

If you have any questions about the CTEP or would like additional information on exercise planning, design, or facilitation, please contact cisa.exercises@cisa.dhs.gov.