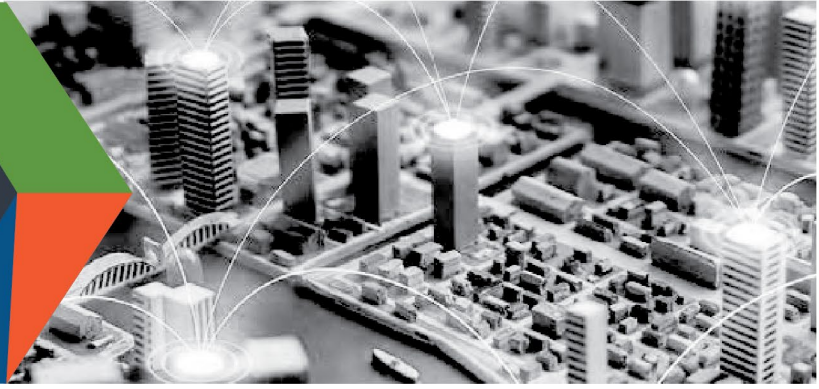
CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW



CISA TABLETOP EXERCISE PACKAGE

OVERVIEW

The **CISA Tabletop Exercise Package (CTEP)** is designed to assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders. CTEP allows users to leverage pre-built exercise templates and vetted scenarios to build tabletop exercises to assess, develop, and update information sharing processes, emergency plans, programs, policies, and procedures.

This program provides exercise planners with tools, scenarios, question sets, and guidance in developing an interactive discussion-based exercise for their communities of interest. Each CTEP template can be customized and further developed to exercise and evaluate specific areas of concern for critical infrastructure owners and operators. CTEP fosters effective partnership building through the development of improved information sharing and collaboration. In addition, CTEP enables the development of after-action reports that support mitigating risks while increasing the resilience of critical infrastructure.

BACKGROUND

CTEP is an all-hazards preparedness and training tool that has been tailored and used by several sectors within U.S. critical infrastructure, including the Dams Sector, the Chemical Sector, and multiple Commercial Facilities Subsectors. CTEP materials provide model exercise and support documentation that can be refined and further developed to exercise and evaluate specific areas of concern for critical infrastructure owners and operators.

RESOURCE ACCESS

CTEP includes over 50 sample situation manuals addressing a variety of critical infrastructure sectors, threat vectors, and scenarios. These situation manuals are ready-made documents that can be used as templates and deployed with minor editing or combined to create customized documents.

All CTEP situation manual templates are available on the Infrastructure Stakeholder Security Exercise Program (formerly Stakeholder Readiness and Exercise Section) portal on the Homeland Security Information Network–Critical Infrastructure (HSIN-CI). They are currently available by sector.

Planned updates to the portal will expand the ways to access CTEP content for users across the spectrum of exercise experience.

CONNECT WITH US
www.cisa.gov

For more information, email CISA Exercises at CISAExercises@cisa.dhs.gov

Linkedin.com/company/cybersecurity and infrastructure security agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA

SCENARIOS

[NOTE: There is overlap between categories due to combined elements.]

<table>
<tr><td colspan="3">Physical Attacks (including: Active Shooter, Anthrax / Plague, Complex Coordinated Attack, Edged Weapon, Hazardous Materials, Hostages, Improvised Explosive Device / Vehicle-Born Improvised Explosive Device [IED / VBIED], Poisoning, Suicide Bomber, Vehicle Ramming)</td></tr>
<tr><td>Active Shooter – Dams Active Shooter, Gaming Industry, Insider Threat, Large Box Store, Lodging Sector Information Sharing, Nuclear Power Station Integrated Response, Outdoor Events Active Threat, Violent Extremist Attack</td><td rowspan="2">IED / VBIED – Chemical Sector Domestic Terror, Defense Industrial Base, Emergency Services, Faith-Based Organizations, Food and Agriculture, Government Facilities, Healthcare and Public Health IED, Lodging Subsector Information Sharing, Maritime Transportation, Multi-Jurisdictional IED, National Monuments and Icons, Outdoor Events Active Threat, Outdoor Events Terrorist Attack, Sports Facilities Domestic Terror, Sports Leagues Domestic Terror, Violent Extremist Attack</td><td rowspan="2">Anthrax / Plague – Healthcare and Public Health Bioterrorism

Edged Weapon – Outdoor Events Active Threat

Hostages – Outdoor Events Active Threat

Vehicle Ramming – Higher Education Active Threat, Outdoor Events Active Threat

Poisoning – Insider Threat

Sabotage Incident – Electricity Substation

Suicide Bomber – Food and Agriculture

Others – Hazardous Materials, Unmanned Aircraft System</td></tr>
<tr><td>Complex Coordinated Attack – Faith-Based Organizations, Higher Education Active Threat, Large Box Store, Lodging Sector Information Sharing, Sports Facilities Domestic Terror, Sports Leagues Domestic Terror, Violent Extremist Attack</td></tr>
<tr><td colspan="3">Threat Vectors (including: Adversarial Threat, Border Crossing Closure, Domestic Threat, International Attack, Multi-staged Attack, Suspicious Package, Terrorist Threat)</td></tr>
<tr><td colspan="2">Chemical Sector Domestic Threat
Dams Adversarial Threat
Food and Agriculture
Lodging Subsector Information Sharing</td><td>Multi-Jurisdictional IED
Supply Chain Border Crossing Closure
Supply Chain Terrorist Threat
Violent Extremist Attack</td></tr>
<tr><td colspan="3">Weather Incidents (including: Earthquake, Flooding, Hurricane, Tornado, Wildfire, Winter Weather)</td></tr>
<tr><td colspan="2">Earthquake Continuity of Operations
Major Earthquake
Supply Chain Hurricane
Supply Chain Severe Flooding</td><td>Supply Chain Winter Weather
Twisted Fate
Wildfire</td></tr>
<tr><td colspan="3">Cyber Attack (including: cyber-only and cyber-attacks combined with physical threat vectors)</td></tr>
<tr><td colspan="2">Banking and Finance Subsector
Chemical Sector
Communications
Critical Manufacturing
Emergency Services
Electricity Subsector</td><td>Health Care and Public Health
Natural Gas Subsector
Petroleum Subsector
Transportation
Water and Wastewater Systems</td></tr>
</table>

PROGRAM MATERIALS

EXERCISE PLANNER GUIDANCE

CTEP provides the following guidance documentation for prospective planners. These documents provide information on the program, guidance for planning and executing exercises, and avenues for providing feedback to the program that enable CTEP to make continuous improvements to the resources it provides critical infrastructure stakeholders:

- **Welcome Letter** – The official introduction letter for CTEP. This letter includes a brief description of the included documents and information on how to contact the exercise section.
- **Exercise Planner Handbook** – A guide for the exercise planners. 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 assist in capturing information and feedback during the exercise for developing the After-Action Report / Improvement Plan (AAR / IP).
- **Exercise Planner Feedback Form** – A feedback form used by the exercise planners and the facilitator to consolidate players' feedback on exercise improvement.

EXERCISE DESIGN TEMPLATES

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 the official invitation to exercise participants.
- **Exercise Brief Slide Deck Template** – A PowerPoint Presentation that 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 from exercise players, such as recommendations and key outcomes from the exercise, as well as feedback on the exercise design and conduct.
- **After-Action Report / Improvement Plan Template** – A Homeland Security Tabletop Exercise and Evaluation Program (HSEEP) compliant AAR / IP template to aid exercise planners and evaluators / data collectors in organizing and implementing the findings of the exercise.
- **Situation Manual** – A manual that provides the scenario, supporting background information, and suggested discussion questions to be posed to the exercise players. Throughout the exercise, players should be encouraged to use the manual to help supplement the information in the Exercise Brief Slide Deck

IMPACT AND RESILIENCE

The ability for public and private sector organizations to plan and execute HSEEP-based exercises on their own will continue to enhance security and resilience by enabling these organizations to identify strengths and areas for improvement within their operating plans, techniques, and procedures, and then to develop an improvement plan that clearly outlines the measures necessary to improve on current concepts. CTEP acts as a force multiplier for the critical infrastructure community by providing owners and operators with the tools needed to enhance the security of their operations, and significantly increases the number of stakeholders that the Cybersecurity and Infrastructure Security Agency can reach with exercise products.

ACCESS TO HSIN-CI

Access to HSIN-CI is available for qualified Critical Infrastructure sector owners and operators. If you currently do not have a HSIN-CI account and wish to gain access, please email your name, employer, work email address, and associated sector to HSINCI@hq.dhs.gov.

For password reset or technical assistance, please contact the **HSIN Helpdesk** at (866) 430-0162 or send an email to HSIN.helpdesk@hq.dhs.gov.