An official website of the United States government Here’s how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Menu

AMERICA’S CYBER DEFENSE AGENCY

Go to this website: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

SHARE:

SERVICE

CISA Tabletop Exercise Packages

Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios.

Task type: Increase your resilience **Readiness Level:** Foundational

RELATED TOPICS: CYBERSECURITY BEST PRACTICES </topics/cybersecurity-best-practices>, MULTIFACTOR AUTHENTICATION </topics/cybersecurity-best-practices/multifactor-authentication>, CYBER THREATS AND ADVISORIES </topics/cyber-threats-and-advisories>

Description

CISA Tabletop Exercise Packages (CTEPs) are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.

Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.

With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

Cybersecurity Scenarios </resources-tools/resources/cybersecurity-scenarios>

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Physical Security Scenarios </resources-tools/resources/physical-security-scenarios>

Active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aircraft systems (UASs), and many more. There are also CTEPs that are geared towards specific industries or facilities to allow for discussion of their unique needs.

Cyber-Physical Convergence Scenarios

</resources-tools/resources/cyber-physical-convergence-scenarios>

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

CTEP Documents </resources-tools/resources/ctep-package-documents>

Leverage pre-built templates to develop a full understanding of roles and responsibilities for exercise planners, facilitators / evaluators, and participants. Additionally, the documentation includes templates for the initial invitation to participants, a slide deck to use for both planning meetings and conduct, a feedback form to distribute to participants post-exercise, and an After Action Report. In conjunction with selecting one of the above situation manuals, your exercise planning team will be able to fully develop your own tabletop exercise and update information sharing processes; emergency response protocols; and recovery plans, policies, and procedures.

- For more information or to request an exercise, please contact: cisa.exercises@cisa.dhs.gov

Tags

Audience: Federal Government </audiences/federal-government>

Topics: Cybersecurity Best Practices </topics/cybersecurity-best-practices>, Multifactor Authentication </topics/cybersecurity-best-practices/multifactor-authentication>, Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Industrial Control Systems </topics/industrial-control-systems>, Critical Infrastructure Security and Resilience </topics/critical-infrastructure-security-and-resilience>, Emergency Communications </topics/emergency-communications>, Active Shooter Preparedness </topics/physical-security/active-shooter-preparedness>, Bombing Prevention </topics/physical-security/bombing-prevention>, Risk Management </topics/risk-management>

Related Services

Mobile Cybersecurity Shared Services </resources-tools/services/mobile-cybersecurity-shared-services>

INCREASE YOUR RESILIENCE | FOUNDATIONAL, INTERMEDIATE, ADVANCED

ASSESS YOUR RISK LEVEL

Malware Next-Generation Analysis </resources-tools/services/malware-next-generation-analysis>

Malware Next-Gen provides malware analysis support for government agencies through multiple tools in a controlled environment.

ASSESS YOUR RISK LEVEL | INTERMEDIATE

Protective Domain Name System Resolver </resources-tools/services/protective-domain-name-system-resolver>

CISA's Protective Domain Name System (DNS) Resolver Service is the evolution and successor to the DNS egress protection capability currently being delivered through E3A DNS Sinkhole.

Security Monitoring </resources-tools/services/security-monitoring>

Receive remediation scanning and quarterly scanning; annual assessments with applicable; and security control assessments for system accreditation.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

888-282-0870 Central@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Accessibility <https://www.dhs.gov/accessibility>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>