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

CISA Tabletop Exercise Package: Faith-Based Organizations

DEFEND TODAY,
SECURE TOMORROW

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. Following the Homeland Security Exercise and Evaluation Program (HSEEP) framework, CTEPs include pre-developed scenarios and module questions to discuss information sharing, response, and recovery elements. Organizations can use CTEPs to initiate discussions to assess their preparedness and security posture in relation to 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 pertinent to the critical infrastructure community generally, and the faith-based community specifically.

FAITH-BASED ORGANIZATION SPECIFIC RESOURCES

CISA provides two situation manuals within the CTEP library to specifically address the concerns of the faith-based community. These scenarios include international and domestic threats, improvised explosive device (IED) and vehicle-borne improvised explosive device (VBIED) attacks, active shooters, and cybersecurity threats (phishing attempts).[1] Additionally, CISA developed videos to accompany these situation manuals, allowing participants to view related video clips of mock news reports to facilitate discussions on information sharing, incident response, and recovery.[2]

PROGRAM MATERIALS

Exercise Planner Guidance

The CTEP includes guidance documentation for exercise planners. These documents provide information about the program, guidance for planning and conducting exercises, and a mechanism 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** – Provides step-by-step instructions on how to plan, develop, and conduct a tabletop exercise.
- **Facilitator and Evaluator Handbook** – 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.
- **Exercise Planner Feedback Form** – Provides a mechanism to consolidate players' feedback on exercise improvement.

Exercise Design Templates

The CTEP provides the following templates for planners to use to design and develop 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** – Leveraged after the exercise to gather information from exercise players,

[1] cisa.gov/cisa-tabletop-exercises-packages
[2] https://www.youtube.com/watch?v=TZQXmcfJqIg&list=PL-BF3N9rHBLJHp2wIn306I6egVofFeS-p

including recommendations, key outcomes from the exercise, and feedback on the exercise design and conduct.

- **After-Action Report / Improvement Plan (AAR / IP) Template** – Aids exercise planners and evaluators / data collectors in organizing and implementing the findings from the exercise.
- **Situation Manual** – 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.

ADDITIONAL RESOURCE ACCESS

The CTEP library includes more than 100 sample situation manuals addressing a variety of critical infrastructure sectors, threat vectors, and scenarios. Stakeholders can leverage these documents with minor editing or combined with other CTEP materials to create customized materials to meet the specific needs of the end users at all levels of an organization. The situation manuals are currently sorted by areas that address cybersecurity, physical security, and integrated (cyber-physical) security. CISA continuously works to refine available scenarios to meet the needs of all stakeholders, including the faith-based community.

FAITH-BASED COMMUNITY SECURITY RESOURCES

CISA provides the faith-based community with a multitude of tools and resources to support risk mitigation efforts through the Faith-Based Organizations – Houses of Worship web presence.[3] Below are just a few examples of resources available, which can be leveraged by security or non-security professionals.

- **Mitigating Attacks on Houses of Worship Security Guide** (cisa.gov/mitigating-attacks-houses-worship-security-guide): An analysis of ten years of targeted attacks on houses of worship and potential risk mitigation solutions designed to achieve a robust and layered approach to security.
- **Houses of Worship Security Self-Assessment Interactive Tool** (cisa.gov/houses-of-worship): Provides a baseline security self-assessment, user guide, and survey that are designed to assess an organization or facility's security posture.[4]
- **Power of Hello for Houses of Worship** (cisa.gov/employee-vigilance-power-hello): Promotes employee and volunteer vigilance by assisting in identifying suspicious behavior, knowing what questions to ask when navigating a potential threat, and recommending when and how to obtain help.
- **Protective Security Advisors** (PSA) (cisa.gov/protective-security-advisors or email central@cisa.dhs.gov): Are a cadre of more than 100 subject matter experts located throughout the nation, available to assist houses of worship with vulnerability assessments, emergency action planning, and coordination.
- **Guide for Developing High Quality Emergency Operations Plans for Houses of Worship** (fbi.gov/file-repository/developing_eops_for_houses_of_worship_final.pdf/view): Provides information for emergency operation planning and discusses actions that can be taken before, during, and after an incident. In addition, the Securing Public Gatherings web presence (cisa.gov/securing-public-gatherings) provides access to a broader range of information regarding the types of threats posed to public gatherings and resources with options for consideration to support risk mitigation activities.

CONTACT INFORMATION

If you have any questions about CISA Tabletop Exercise Packages or would like additional information on exercise planning, design, or facilitation, please contact cisa.exercises@cisa.dhs.gov. You can also visit CISA's website (cisa.gov), LinkedIn (linkedin.com/company/cisagov), Twitter (@CISAgov), Cyber-specific Twitter (@cyber), US-CERT Twitter (@uscert) Facebook (facebook.com/CISA), and Instagram (@cisagov).

[3] cisa.gov/faith-based-organizations-houses-worship
[4] The Houses of Worship Security Self-Assessment user guide and survey are located at cisa.gov/houses-worship-security-self-assessment