CISA Resources Applicable to Threats Against Healthcare & Public Health Sector

The Cybersecurity and Infrastructure Security Agency (CISA) works with the Healthcare and Public Health (HPH) Sector to enhance the security and resilience of hospitals and healthcare providers to cyber and physical threats, including potential heightened threats of targeted violence and terrorism. CISA offers a multitude of no-cost resources focused on the security of facilities and personnel.

CISA currently offers four HPH-specific security resources that help inform security and resilience enhancements:

1. Hospitals & Healthcare Facilities Action Guide: describes potential indicators of nefarious intent, actions that should be taken if an active shooter incident occurs, and a series of suggested protective measures and mitigation strategies. Link
2. Healthcare and Public Health Facility Annex to the Security and Resilience Guide for Countering Improvised Explosive Devices (SRG C-IED): defines actions that management and staff at healthcare facilities can take to understand and improve the ability to perform counter-IED activities and make security decisions. Link
3. CISA Tabletop Exercise Packages (CTEPs) for Healthcare and Public Health: downloadable exercise packages that assist in the conduct of independent exercises. Includes all the needed materials that can be tailored to the organization's needs. Available scenarios specific to HPH include Suspicious Package, Suicide Bomber, Vehicle Bomb, and Cyber Attack. Link
4. Healthcare and Public Health Cybersecurity: provides key resources for HPH organizations at every level. CISA, HHS and the Health Sector Coordinating Council are providing this toolkit filled with remedies to give sector stakeholders a greater ability to proactively assess vulnerabilities and implement solutions. Link

Additionally, CISA's broader security resources are also applicable to facilities and threats commonly associated with the HPH Sector regardless of location and type.

Regional Support

Security Advisors: More than 250 security subject matter experts located across the continental U.S., Puerto Rico, Alaska, Hawaii, and Guam, who assist in threat mitigation, facility vulnerability assessments, and training. See contact information below. Link

Information Sharing

Technical Resource for Incident Prevention (TRIPwire): online portal that combines up-to-date threat information and

security resources specific to bombing incidents to help users anticipate, identify, and prevent bombing-related incidents. Link

National Cyber Awareness System (NCAS): provides access to timely information about cybersecurity topics and threats. Link

Priority Telecommunication Services: enable essential personnel to communicate when networks are degraded or congested. Link

Security Assessments

Security Assessment at First Entry (SAFE): rapid, onsite physical security assessment led by PSAs that provides structured feedback on observed vulnerabilities and options to improve security. Link

Self-Assessment Tools

Vehicle Ramming Self-Assessment Tool: evaluates varying areas immediately outside of a facility against the risk of a vehicle ramming attack and offers suggested corresponding protective measures. Link

Insider Threat Self-Assessment Tool: assesses the maturity of an organization's program and determines potential immunity to insider threat incidents; includes corresponding measures to enhance capabilities. Link

Guidance

Insider Threat Mitigation Guide: comprehensive guidance in support of the establishment or enhancement of an insider threat mitigation program. Link

De-Escalation Series: helps to recognize the warning signs of someone on a path to violence; assess if the situation or person of concern is escalating; de-escalate the situation taking place; and report the situation through organizational mechanisms or 9-1-1 for immediate threats. *Available in multiple languages*. Link

Protecting Infrastructure During Public Demonstrations: conveys easily implementable and cost-effective protective measures that can be leveraged to enhance the security of a facility during protests. Link

Personal Security Considerations: encourages vigilance and reporting of suspicious behaviors and contains several easily implementable security measures that can mitigate threats to personal safety. *Available in multiple languages*. Link

Mitigating the Impacts of Doxing on Critical Infrastructure: defines and provides examples of doxing; explains its potential impacts; and offers protective and preventative measures, mitigation options, and additional resources for individuals and organizations. Link

What To Do – Bomb Threat Guidance: procedures and multimedia aids for bomb threats and unattended or suspicious items along with additional planning and resource information that will help prepare and react appropriately during events. *Available in Spanish*. Link

Counter-Improvised Explosive Device (IED) Awareness Products: instructional reference cards, posters, checklists, guides, videos, briefings, and applications that inform appropriate actions to prevent, protect against, respond to, and mitigate bombing incidents. *Available in Spanish*. Link

Training

Active Shooter Preparedness: instructor-led and online training modules, as well as resources, focused on behavioral indicators, emergency action plan creation, actions that may be taken to increase probability of survival, and how to quickly recover from an incident. *Resources are available in multiple languages*. Link

Counter-IED: accredited training through instructor-led sessions, online via a virtual instructor-led training platform, and independent study training focused on a range of practical prevention, protection, response, and mitigation actions for bombing incidents. *Available in Spanish*. Link

Interoperable Communications Technical Assistance Program (ICTAP): available to state, local, tribal, and Territorial emergency communications partners to assist in areas such as cybersecurity, interoperability, and communications personnel training. Link

Exercises

Exercises Planning and Conduct Services: provides government and industry partners end-to-end exercise planning and conduct support, including an after-action report for cyber and physical security exercises. Link

Contacts

CISA Central: mechanism for critical infrastructure stakeholders to engage with CISA; a simplified entry point for stakeholders to request assistance. Link or contact directly via Central@cisa.gov.

- Region 8 (Colorado, Utah, Wyoming, Montana, North Dakota, and South Dakota): CISARegion8@hq.dhs.gov
- Region 9 (Arizona, Nevada, California, Guam, American Samoa, Commonwealth of Northern Mariana Islands (CNMI) and Hawaii): CISARegion9@hq.dhs.gov
- Region 10 (Washington, Oregon, Idaho, and Alaska): CISARegion10@hq.dhs.gov