CISA RESOURCES APPLICABLE TO THREATS AGAINST THE LGBTQIA+ COMMUNITY

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) maintains a multitude of capabilities and no-cost resources that can support the LGBTQIA+ community in enhancing security and resilience to cyber and physical threats, including potential heightened threats of targeted violence and terrorism. The National Terrorism Advisory System (NTAS) Bulletin issued on May 24, 2023 highlighted potential threats to the LGBTQIA+ community based on recent attacks and threats of violence.

COMMUNITY SUPPORT RESOURCES

- **Protective Security Advisors**: over 140 security subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.

- **Physical Security Resources**: builds security capacity of the public and private sector to mitigate a wide range of threats including active shooters, vehicle ramming, insider threats, and small unmanned aircraft systems.
  - Securing Public Gatherings
  - Mass Gathering Security Planning Tool
  - Protecting Infrastructure During Public Demonstrations

  - Targeted Violence Prevention
    - Pathway to Violence: Warning Signs and What You Can Do
    - Power of Hello
    - Personal Security Considerations
    - Mitigating the Impacts of Doxing

  - **Active Shooter Preparedness:** a comprehensive set of courses, materials, and workshops that better prepare you to deal with an active shooter situation, focusing on behaviors that represent pre-incident indicators and characteristics of active shooters, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident.
    - Active Shooter Preparedness Webinar
    - Planning and Response to an Active Shooter Guidance
    - Active Shooter Preparedness: Access & Functional Needs – What You Should Know Video
    - Translated Active Shooter Preparedness Resources

  - **Vehicle Ramming Mitigation:** provides mitigation tools for terrorist attacks when a vehicle is used as a weapon.
    - Vehicle Ramming Self-Assessment Tool
    - Vehicle Ramming Action Guide
    - Active Vehicle Barrier Selection Tool
    - Guide to Active Vehicle Barrier Specification and Selection Resources

- **Insider Threat Mitigation:** explains the key steps to mitigate insider threat: Define, Detect and Identify, Assess, and Manage.
  - Insider Threats 101 Fact Sheet
  - Insider Risk Mitigation Program Evaluation Self-Assessment Tool

- **Bombing Prevention Resources:** builds capability within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents.
  - Counter-IED Awareness Products
  - What to Do – Bomb Threat Resources
  - What to Do: Bomb Threat Video
  - Bomb Threat Guidance Brochure
  - Suspicious or Unattended Item Card
  - What to Do: Suspicious or Unattended Item Video

- **School Safety Resources:** builds the capacity of schools and districts to protect against and mitigate security threats and risks.
  - K-12 School Security Guide and School Security Assessment Tool
  - School Climate Topic Page
    - School Climate Resources
  - Mental Health Topic Page
    - Mental Health Resources
  - Bullying & Cyberbullying Topic Page
    - Bullying Prevention Strategies and Resources

- **CISA Tabletop Exercise Packages (CTEPs):** a comprehensive set of resources designed to assist partners initiate discussions within their organizations about their ability to address a variety of threat scenarios.

- Cybersecurity Resources:
  - **Cybersecurity Advisors**: approximately 70 cybersecurity subject matter experts located across the country who conduct security assessments, provide access to security guidance, training, and exercises, and advise on enhanced protective measures.
  - **Cyber Guidance for Small Businesses:** Cyber incidents have surged among small businesses and non-governmental organizations (NGOs) that often do not have the resources to defend against devastating attacks like ransomware. As a small business owner, you have likely come across security advice that is out-of-date or that does not help prevent the most common compromises. This guidance is applicable to both the small business and NGO communities.
  - **Cross-Sector Cybersecurity Performance Goals:** The Cross-Sector Cybersecurity Performance Goals (CPGs) establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts. The CPGs are voluntary, high-impact, high-priority practices for critical infrastructure owners that address common adversary tactics, techniques, and procedures (TTPs) and manage risks to information technology (IT) and operational technology (OT) that CISA commonly observes.

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.

- Federal School Safety Clearinghouse Main Page: provides schools and districts with actionable evidence-based practices and recommendations to create a safe and supportive learning environment.

TRAINING

- Bombing Prevention Training and Resources: CISA's Office for Bombing Prevention offers bombing prevention training throughout the United States on multiple platforms to meet stakeholder needs, including direct-delivery, in-person in a traditional classroom setting or in-residence at the Federal Emergency Management Agency's Center for Domestic Preparedness, online through a Virtual Instructor-Led Training (VILT) platform, and through Independent Study Training.

- Response to Suspicious Behavior and Items Course: 60-minute Virtual Instructor-Led Training (VILT) delivered through live instruction to cover the following topics:
    - Normal behavior and suspicious behavior indicators
    - Physical characteristics that can or cannot be easily changed
    - Unattended and suspicious items
    - Appropriate responses to suspicious behaviors, unattended items, and suspicious items

- Surveillance Detection for Bombing Prevention Course Fact Sheet: provides public safety and security professionals fundamental knowledge and skills to recognize and respond appropriately to hostile surveillance at facilities and planned and unplanned events.

- **Active Shooter:** 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. What You Can Do Online Training.

- Active Shooter Options for Consideration Training Video: demonstrates possible actions to take if confronted with an active shooter scenario. The video also shows how to assist authorities once law enforcement enters the scene.

- Defusing Potentially Violent Situations: provide a description of methods, such as purposeful actions and verbal communications, to prevent potential violence or dangerous situations.

CONTACTS

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

CISA Regional Offices **(including Protective Security Advisors):** executes mission objectives during steady-state and incident operations; provides local and facility-based support to critical infrastructure stakeholders. Contact directly via:

- **Region 1** (Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut): CISARegion1@hq.dhs.gov
- **Region 2** (New York, New Jersey, Puerto Rico, and Virgin Islands): CISARegion2@hq.dhs.gov

- **Region 3** (Pennsylvania, West Virginia, Maryland, Delaware, Virginia, and the District of Columbia): CISARegion3@hq.dhs.gov
- **Region 4** (Kentucky, Tennessee, North Carolina, South Carolina, Mississippi, Alabama, Georgia, and Florida): CISARegion4@hq.dhs.gov
- **Region 5** (Ohio, Michigan, Indiana, Illinois, Wisconsin, and Minnesota): CISARegion5@hq.dhs.gov
- **Region 6** (Louisiana, Arkansas, Oklahoma, Texas, and New Mexico): CISARegion6@hq.dhs.gov
- **Region 7** (Missouri, Kansas, Nebraska, and Iowa): CISARegion7@hq.dhs.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, and Hawaii): CISARegion9@hq.dhs.gov
- **Region 10** (Washington, Oregon, Idaho, and Alaska): CISARegion10@hq.dhs.gov

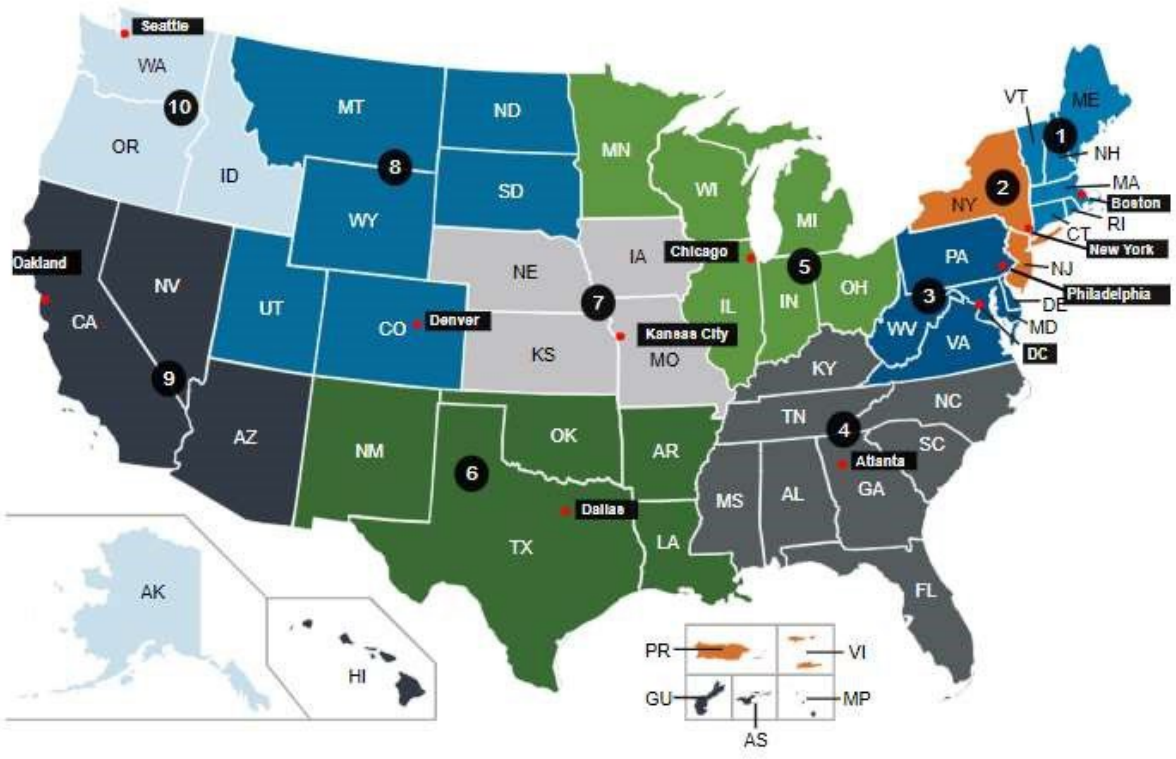

Figure 1: CISA Regions