CISA RESOURCES APPLICABLE TO COUNTER TRANSNATIONAL REPRESSION

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) provides products and tools that can be leveraged to mitigate certain aspects of the risk associated with transnational repression.[1] Transnational Repression is when foreign governments stalk, intimidate, or assault people, communities, or businesses within the United States.[2] This type of threat limits freedom of speech of individuals, wherever they reside, including in the United States and other democracies. Additionally, there is a risk that transnational repression may have impacts on our Nation's critical infrastructure, especially our information technology and related businesses, given the increasing impact of digital transnational repression.[3] The following publicly available CISA resources can help mitigate the threat of transnational repression by highlighting personal safety best practices.

COMMUNITY SUPPORT RESOURCES

- **Personal Security Considerations**
  - Personal Security Considerations Fact Sheet | CISA: encourages critical infrastructure owners and their personnel to remain vigilant and report suspicious behavior that individuals may exhibit to thwart an attack. These tools can also be used to better protect yourself, being aware of your surroundings, and potentially identify when you are being targeted by a foreign government.
  - Defusing Potentially Violent Situations: provide a description of methods, such as purposeful actions and verbal communications, to prevent potential violence or dangerous situations.

- **Doxing Fact Sheet**
  - CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure | CISA: encourages critical infrastructure owners and their personnel to remain vigilant and report suspicious behavior that individuals may exhibit to thwart an attack. These tools can also be used to better protect yourself, being aware of your surroundings, and potentially identify when you are being targeted by a foreign government.

- **Physical Security Resources**: build security capacity of the public and private sector to mitigate a wide range of threats including insider threats.
  - Insider Threat Mitigation: explains the key steps to mitigate insider threat: Define, Detect, and Identify, Assess, and Manage. Utilizing these steps in real life scenarios can help identify and manage Transnational Repression threats within your community.
    - Insider Threats 101 Fact Sheet
    - Insider Risk Mitigation Program Evaluation Self-Assessment Tool
  - Bombing Prevention Resources: build capability within the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents. Included below

[1] This product is for informational purposes only and is meant to support the security and resilience of critical infrastructure.
[2] Federal Bureau of Investigation, Transnational Repression — FBI
[3] NIC and ODNI assessments-Digital Repression Growing Globally, Threatening Freedoms (dni.gov)

are bombing prevention resources that can assist Transnational Repression victims in protecting themselves if/when they are targeted with a bomb threat.
    - What to Do – Bomb Threat Resources
    - Mass Bomb Threats Postcard

- Cybersecurity Resources: CISA through the High-Risk Community Protection initiative is partnering with civil society organizations and technology companies to understand what actions CISA and our partner organizations need to take to advance the cybersecurity of communities who are experiencing targeting by Advanced Persistent Threat (APT) actors, who lack the resources to defend against these threats, and where additional government support can advance the cyber defense of the community. As part of this effort CISA will be publishing a page on CISA.gov to communicate resources which are available to high-risk communities. These resources will include but not be limited to:
    - Practical guidance on the steps individuals and small organizations can take to protect themselves against cyber attacks
    - A list of low and no cost cybersecurity services available to civil society organizations
    - A page featuring existing cyber volunteer programs through which cybersecurity experts can volunteer their expertise to organizations in need and organizations in need can become aware of the volunteer programs who may be able to provide support.

- **International Collaboration to Advance the Cybersecurity of High-Risk Communities**: CISA understands that transnational repression is an inherently international challenge. CISA and the United Kingdom's National Cyber Security Centre have have convened the Strategic Dialogue on the Cybersecurity of Civil Society Under Threat of Transnational Repression. During the Strategic Dialogue partners partners affirmed that civil society has been shining a light on transnational repression, and the cyber intrusions against them necessitate that the democracies of the world do more to help high-risk communities protect themselves against these threats.

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 (contact your CISA Regional office), 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

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

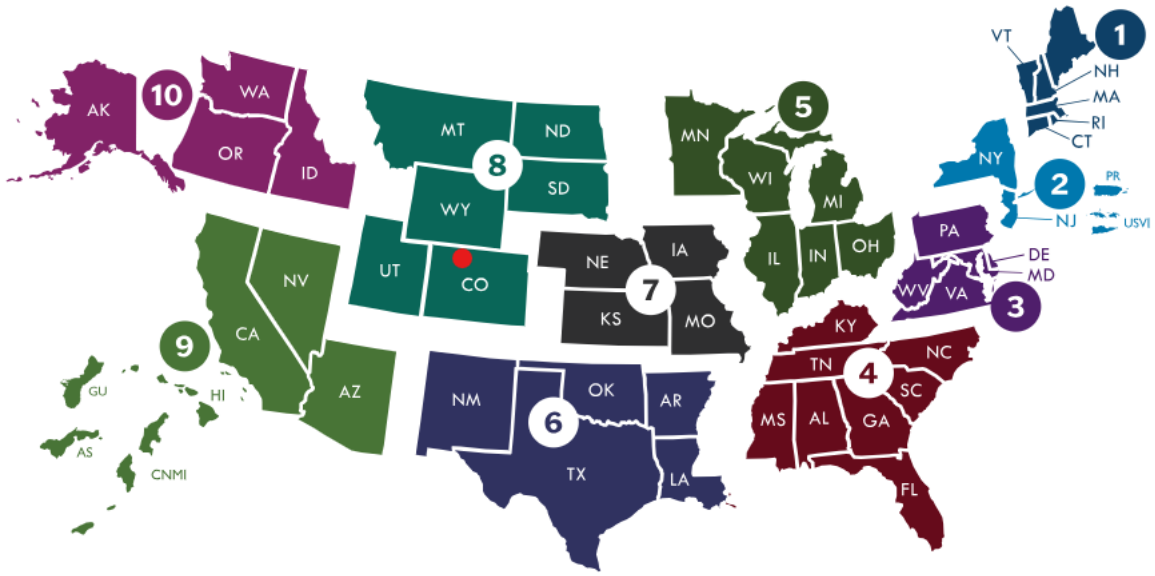

Figure 1: CISA Regions