PROTECTIVE SECURITY ADVISOR STAKEHOLDER BRIEFING

David Melby
June 8, 2022

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

CORE COMPETENCIES

Partnership Development

CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed, voluntary decisions and investments.

Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.

Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.

Critical Infrastructure Significance

- Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on national security, the economy, public health or safety, and our way of life

Protective Security Advisors

- Protective Security Advisors (PSA) are field-deployed personnel who serve as critical infrastructure security specialists
- State, local, tribal, territorial (SLTT) and private sector link to DHS infrastructure protection resources
  - Coordinate vulnerability assessments, training, and other DHS products and services
  - Provide a vital link for information sharing in steady state and incident response
  - Assist facility owners and operators with obtaining security clearances

Protective Security Advisors

- Protective Security Advisors (PSA) have five mission areas that directly support the protection of critical infrastructure:
  - Plan, coordinate, and conduct security surveys and assessments
  - Plan and conduct outreach activities
  - Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
  - Respond to incidents
  - Coordinate and support improvised explosive device awareness and risk mitigation training

Protective Security Advisors

- **Plan, coordinate, and conduct security surveys and assessments** – PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions
- **Plan and conduct outreach activities** – PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities

Protective Security Advisors

- **Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events** – PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events
- **Respond to incidents** – PSAs plan for and, when directed, deploy to Unified Area Command Groups, Joint Operations Centers, Federal Emergency Management Agency Regional Response Coordination Centers, and/or State and local Emergency Operations Centers in response to natural or man-made incidents

Protective Security Advisors

- **Coordinate and support improvised explosive device awareness and risk mitigation training** – PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials to SLTT partners to assist them in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats

Homeland Security Starts with Hometown Security

Security starts here.

connect plan train report

For more information, visit
www.cisa.gov/hometown-security

Assist Visits

- Establish and enhance CISA's relationship with critical infrastructure owners and operators; inform them of the importance of their facilities, and reinforce the need for continued vigilance
- During an Assist Visit, PSAs focus on coordination, outreach, training, and education
- Assist Visits are often followed by security surveys using the Infrastructure Survey Tool (IST) or Security Assessment at First Entry (SAFE) or delivery of other CISA services

Infrastructure Survey Tool

- The Infrastructure Survey Tool (IST) is a web-based vulnerability survey tool that applies weighted scores to identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information
  - Physical Security
  - Security Force
  - Security Management
  - Information Sharing
  - Protective Measures
  - Dependencies

IST Data Categories

- Facility Information
- Contacts
- Facility Overview
- Information Sharing*
- Protective Measures Assessment*
- Criticality*
- Security Management Profile*
- Security Areas/Assets

- Physical Security*
  - Building Envelope
  - Vehicle Access Control
  - Parking
  - Site's Security Force
  - Intrusion Detection System (IDS)/Close Circuit Television (CCTV)
  - Access Control
  - Security Lighting

- Additional DHS Products and Services
- Criticality Appendix
- Images
- Security Force*
- Cyber Vulnerability
- Dependencies*

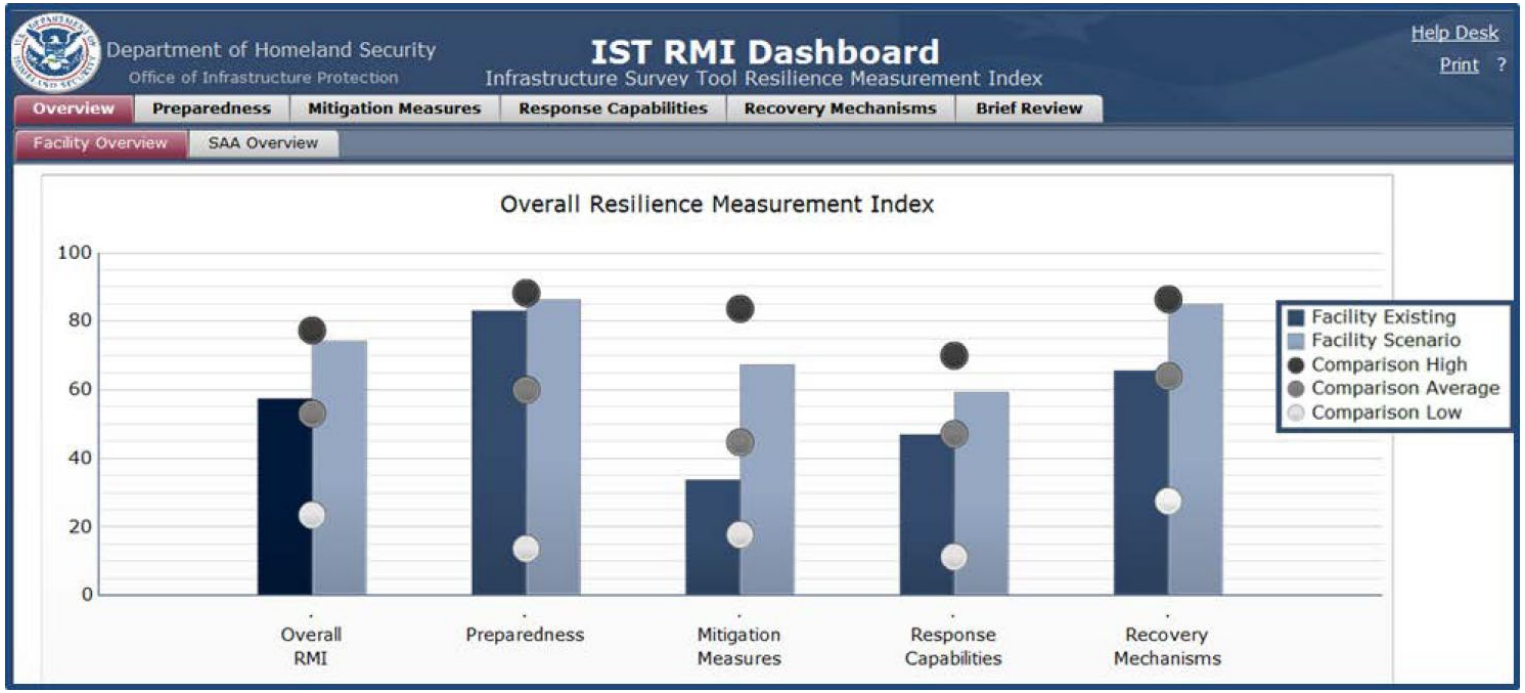
** Comparative analysis provided*

IST Deliverables

- Generates the Protective Measures Index and Resilience Measurement Index
- The tool allows CISA and facility owners and operators to:
  - Identify security gaps
  - Compare a facility's security in relation to similar facilities
  - Track progress toward improving critical infrastructure security

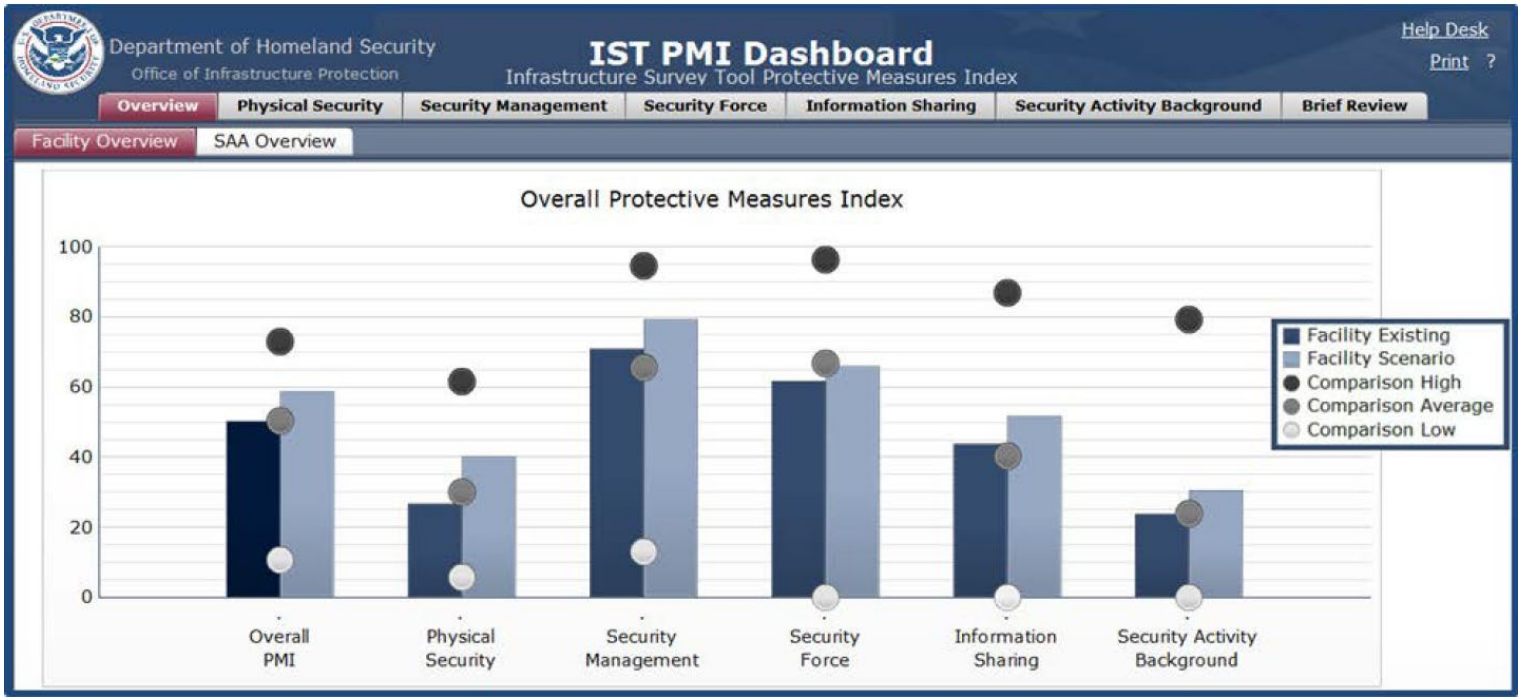
IST Dashboards

- Survey and assessment information is shared with owners and operators through interactive dashboards



IST Dashboards

- Dashboards allow users to explore the impacts of potential improvements to their security and resilience status



SAFE Tool

- The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats
- The SAFE tool is suited for all facilities, including smaller ones such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics

Infrastructure Visualization Platform

- Infrastructure Visualization Platform (IVP) is a data collection and presentation medium
  - Supports critical infrastructure security, special event planning, and response operations
  - Integrates assessment data with immersive video and geospatial and hypermedia data

Protected Critical Infrastructure Information Program

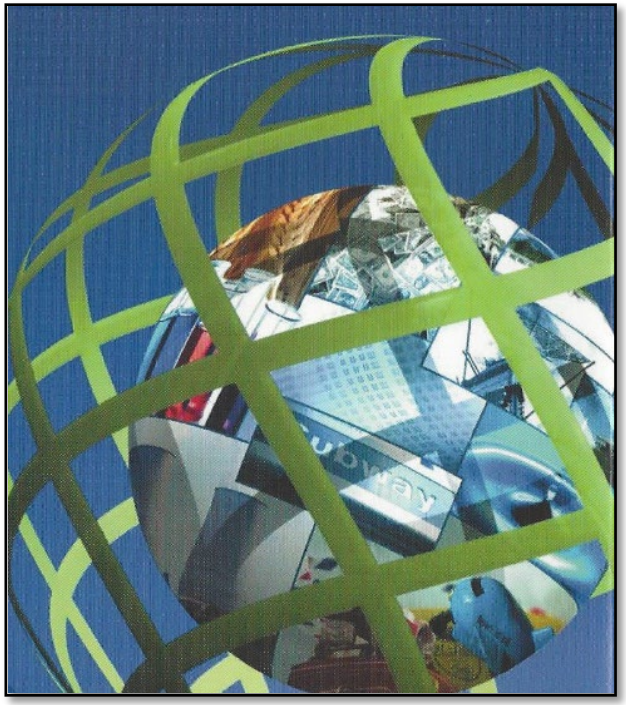
- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes
- PCII protects from release through:
  - Freedom of Information Act disclosure requests
  - State, local, tribal, territorial disclosure laws
  - Use in civil litigation
  - Use for regulatory purposes

Submitters of PCII

- Examples of organizations who submit information for PCII protections are:
  - Critical infrastructure owners and operators
  - State, local, tribal, territorial governments
  - Collaborative homeland security working groups

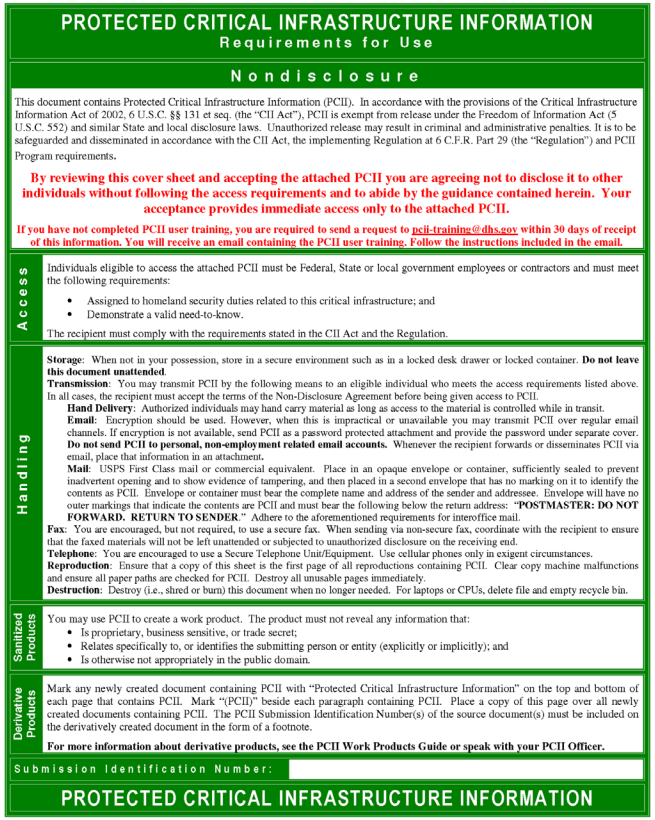
Use of PCII

- Allows CISA and other Federal, SLTT security analysts to use PCII to:
  - Analyze and secure critical infrastructure and protected systems (cyber)
  - Identify vulnerabilities and develop risk assessments
  - Enhance recovery preparedness measures



Qualifications for PCII Protections

- To qualify for PCII protections, information must be related to the security of the critical infrastructure and a submitter must attest the information is:
  - Voluntarily submitted
  - Not customarily found in the public domain
  - Not submitted in lieu of compliance with any regulatory requirement



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION
Requirements for Use

Nondisclosure

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131 et seq. (the "CII Act"), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. 552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. It is to be safeguarded and disseminated in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the "Regulation") and PCII Program requirements.

By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.

If you have not completed PCII user training, you are required to send a request to pcii-training@dhs.gov within 30 days of receipt of this information. You will receive an email containing the PCII user training. Follow the instructions included in the email.

Access

Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:

- Assigned to homeland security duties related to this critical infrastructure; and
- Demonstrate a valid need-to-know.

The recipient must comply with the requirements stated in the CII Act and the Regulation.

Handling

Storage: When not in your possession, store in a secure environment such as in a locked desk drawer or locked container. **Do not leave this document unattended.**

Transmission: You may transmit PCII by the following means to an eligible individual who meets the access requirements listed above. In all cases, the recipient must accept the terms of the Non-Disclosure Agreement before being given access to PCII.

Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.

Email: Encryption should be used. However, when this is impractical or unavailable you may transmit PCII over regular email channels. If encryption is not available, send PCII as a password protected attachment and provide the password under separate cover. **Do not send PCII to personal, non-employment related email accounts.** Whenever the recipient forwards or disseminates PCII via email, place that information in an attachment.

Mail: USPS First Class mail or commercial equivalent. Place in an opaque envelope or container, sufficiently sealed to prevent inadvertent opening and to show evidence of tampering, and then placed in a second envelope that has no marking on it to identify the contents as PCII. Envelope or container must bear the complete name and address of the sender and addressee. Envelope will have no outer markings that indicate the contents are PCII and must bear the following below the return address: "**POSTMASTER: DO NOT FORWARD. RETURN TO SENDER.**" Adhere to the aforementioned requirements for interoffice mail.

Fax: You are encouraged, but not required, to use a secure fax. When sending via non-secure fax, coordinate with the recipient to ensure that the faxed materials will not be left unattended or subjected to unauthorized disclosure on the receiving end.

Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.

Reproduction: Ensure that a copy of this sheet is the first page of all reproductions containing PCII. Clear copy machine malfunctions and ensure all paper paths are checked for PCII. Destroy all unusable pages immediately.

Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.

Sanitized Products

You may use PCII to create a work product. The product must not reveal any information that:

- Is proprietary, business sensitive, or trade secret;
- Relates specifically to, or identifies the submitting person or entity (explicitly or implicitly); and
- Is otherwise not appropriately in the public domain.

Derivative Products

Mark any newly created document containing PCII with "Protected Critical Infrastructure Information" on the top and bottom of each page that contains PCII. Mark "(PCII)" beside each paragraph containing PCII. Place a copy of this page over all newly created documents containing PCII. The PCII Submission Identification Number(s) of the source document(s) must be included on the derivatively created document in the form of a footnote.

For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.

Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Access, Dissemination, & Storage

- To become a PCII Authorized User (AU), one must:
  - Be a government employee or supporting contractor
  - Have specific homeland security duties
  - Have a specific “Need-to-Know”
  - Complete PCII Authorized User training
  - Sign a Non-Disclosure Agreement (except Federal employees)
- PCII protects oral discussions
- PCII Can be Emailed on Government systems
- PCII Can be Stored electronically on approved Government systems
- PCII Can be Stored in controlled spaces in locked containers (GSA safe NOT required)

PCII Myths

- ***PCII is too difficult to share!"***
  - Sanitize the information if possible
  - Share with PCII Authorized Users using derivative products
  - PCII Authorized Users can email PCII with minimal actions on unclassified government networks
  - Exigent circumstances
- "***Marking and handling PCII is like classified information"***
  - PCII is Sensitive But Unclassified (SBU)
  - Can be accessed on UNCLASS network and shared with PCII Authorized Users
- ***"Other protections exist to prevent disclosure/release"***
  - PCII has a specific statutory exemption (CII Act of 2002) from release

Capability Building Framework

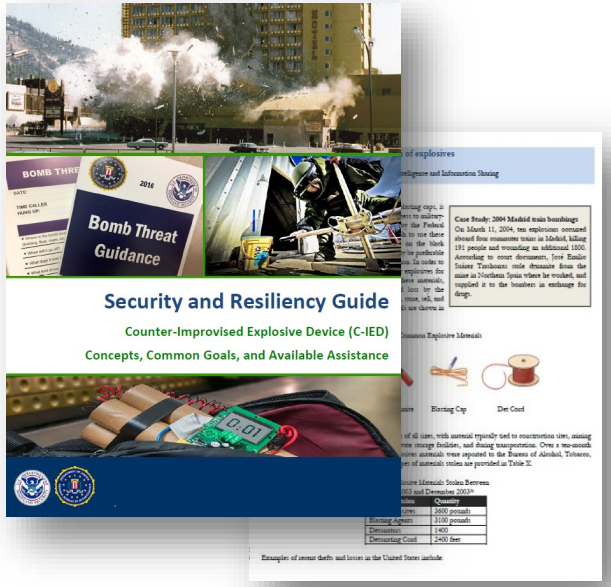
The *Security and Resiliency Guide for Countering IEDs* (SRG C-IED) serves as a foundational resource through which OBP assists stakeholders to build C-IED capabilities.

The SRG C-IED provides stakeholders with access to:

- An overview of IED threats and consequences
- C-IED concepts and a set of common C-IED goals
- Links to Federal Government C-IED tools and resources
- Annexes for high-risk sports venues, public assembly venues, outdoor events, and lodging facilities (Healthcare annex under development).

The SRG C-IED is intended for stakeholders who can play a role in countering IEDs, including:

- State, local, tribal, and territorial governments
- Law enforcement
- Private sector organizations
- Facility owner/operators
- Fire/EMS services
- Emergency management



The SRG C-IED serves as a foundational resource by :

- Distilling complex IED and C-IED concepts into digestible and actionable information
- Helping additional stakeholders understand and play a role in IED security/resilience
- Enhancing nationwide planning and preparedness for IED incidents

SRG C-IED Annexes

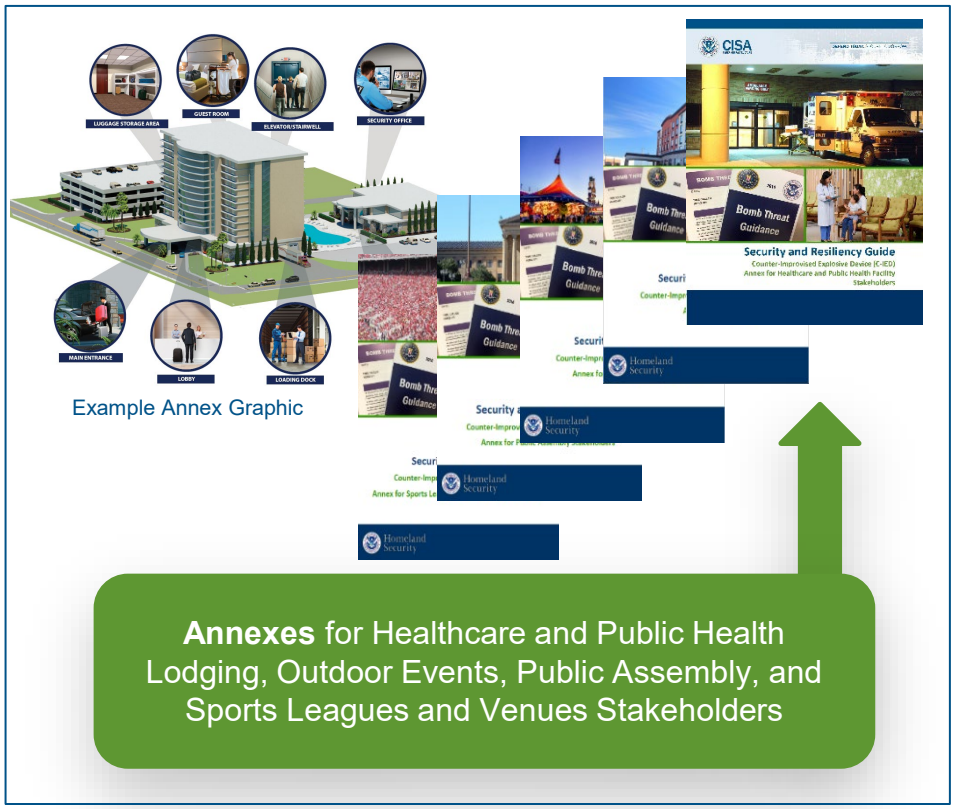
The SRG annexes define tasks and related processes that security managers and staff can use to understand and improve their ability to perform C-IED activities and make decisions as it relates to their specific sectors.

Designed to provide security managers and staff with:

1. A **practical framework** to examine their ability to perform C-IED activities, and
2. Supporting guidance and materials to **strengthen their C-IED preparedness**.

Key Assumption:

The information provided in these guides is meant to **provide suggestions and examples** of what others are doing as options for facilities to consider **to enhance their C-IED preparedness**.



Counter-IED Risk Mitigation Training

CISA's Office for Bombing Prevention delivers a diverse curriculum of accredited training to build nationwide C-IED awareness and capabilities among stakeholders.

OBP is accredited by the International Association for Continuing Education and Training (IACET) to issue the IACET Continuing Education Unit (CEU).

Diverse Curriculum

Diverse curriculum of training designed to build counter-IED core capabilities, such as

- IED Awareness
- VBIED Detection
- Bomb Threats
- Surveillance Detection
- Protective Measures
- Suspicious Items/Activity

Participants

- State and local law enforcement
- Federal agencies
- First responders and First Receivers
- Private sector partners

Access Training

- In-Person Instructor Led Training – 9 courses
- Virtual Instructor-Led Training – 6 courses
- Web-Based Training – 5 courses

Access courses at www.cisa.gov/bombing-prevention-training-courses

TRIPwire

TRIP*wire* is a free information and C-IED resource-sharing website that provides expert analysis and threat information gathered from open-source intelligence, extremist groups, and raw incident data collection.

- **Increases awareness** of evolving IED tactics, techniques, and procedures
- **Shares incident lessons learned** and counter-IED preparedness information with security personnel
- **Integrates open-source information**, including videos and how-to manuals gathered directly from extremist groups, to increase awareness of IED trends and threats
- **Publishes threat, awareness, and training materials** to help first responders and law enforcement anticipate, identify, and prevent bombing incidents

To register for an account, visit https://tripwire.dhs.gov

C-IED Awareness Products

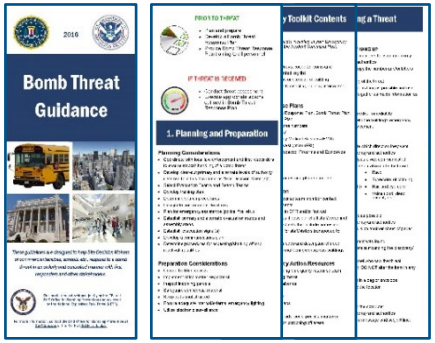
Awareness products provide federal, state, local, and private sector partners on the front-lines with knowledge, tools, resources to protect property and save lives.

Posters

Ex. Common Household Products Advisory

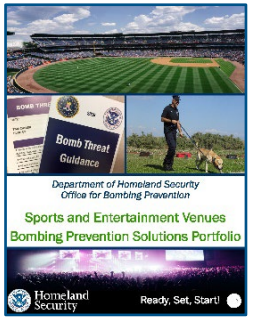
Bomb Threat Guidance Products

Ex. DHS-DOJ Bomb Threat Guidance



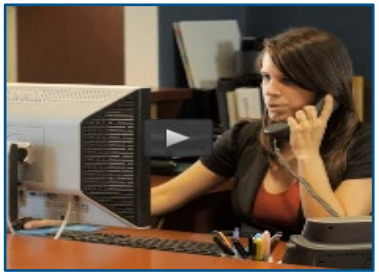
Protection Guides

Ex. Sports and Entertainment Venues Bombing Solutions Portfolio



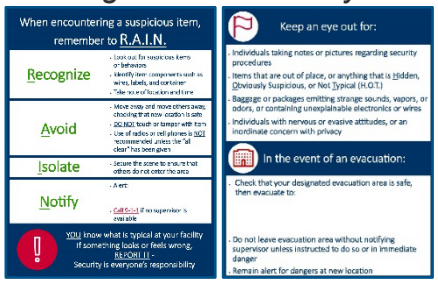
Informational Videos

Ex. What to Do – Bomb Threat



Customized C-IED Products

Ex. Bombing Prevention Lanyard Cards



Awareness Cards

Ex. VBIED Identification Guide

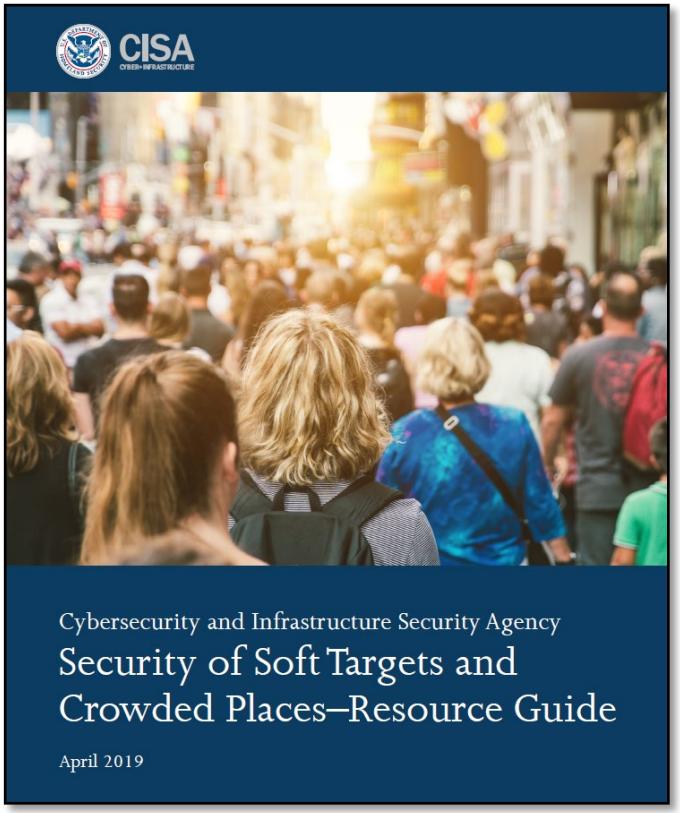
C-IED Awareness Products can be accessed at: https://www.cisa.gov/counter-ied-awareness-products

Security of Soft Targets and Crowded Places

Segments of our society are **inherently open to the general public**, and by nature of their purpose do not incorporate strict security measures

Security of Soft Targets and Crowded Places – Resource Guide

- A catalog of available CISA resources most relevant for soft targets and crowded places
  - High-level overview of CISA resources and programs
  - User-friendly launching point to websites, resources, and programs for more detailed information



Security of Soft Targets and Crowded Places – Resource Guide

Audience

- For **Everyone**
- For **Businesses**
- For **Government**
- For **First Responders**

Types of Resources

- Fact Sheet
- Guide
- Informational Materials
- In-Person Training
- Online Training
- Tool
- Video
- Website

Topic Categories

- Understand the Basics
- Identify Suspicious Behavior
- Protect, Screen, and Allow Access to Facilities
- Protect Against Unmanned Aircraft Systems
- Prepare and Respond to Active Assailants
- Prevent and Respond to Bombings
- Connect with CISA

Homeland Security

Active Shooter Preparedness

Security Awareness for Soft Targets and Crowded Places

- Active Shooter Preparedness materials available from CISA include:
  - “How to Respond” resource materials
  - Preparedness videos and training links
  - Emergency action planning tools and templates
- https://www.cisa.gov/active-shooter-preparedness

Active Shooter Preparedness Brief

Active Shooter Workshops

- These scenario-based workshops feature facilitated discussions to engage private sector professionals and law enforcement representatives from federal, state, and local agencies to learn how to prepare for, and respond to, an active shooter situation
- Through the course of the exercise, participants evaluate current response concepts, plans, and capabilities for coordinated responses to active shooter incidents
- https://www.cisa.gov/active-shooter-workshop-participant

Break time!

- Next up, Bill Nash, Cybersecurity Advisor for Wisconsin