PSPR2 Seminar Series: Mass Casualty Impact and Recovery

THE SESSION WILL BEGIN SHORTLY

AGENDA

- Special Introductions
- CISA Overview
- An Introduction to Recovery Preparedness
- An Introduction to Preparedness in the Private Sector
- Q&A
- Session Wrap Up

PSPR2

SEMINARS FOR RESILIENCE

GH INTERNATIONAL

American Red Cross

Albertsons

NEW YORK STATE | Homeland Security and Emergency Services

PSPR2 Seminar Series: Mass Casualty Impact and Recovery

INTRODUCTION TO RECOVERING FROM A MASS CASUALTY EVENT

PSPR2

SEMINARS FOR RESILIENCE

CH INTERNATIONAL

ACCREDITED IACET PROVIDER

Albertsons

American Red Cross

NEW YORK STATE Homeland Security and Emergency Services

PSPR2 SERIES OVERVIEW

The primary goals of the Private Sector Preparedness, Response, and Recovery Seminar (PSPR2) series are to:

- Provide participants with critical infrastructure best practices at the owner and operator level on recovery and continuity resulting from a mass casualty event
- Present and discuss best practices on phases of mass casualty event recovery, and
- Provide partners with planning resources and tools to assist with mass casualty impact and recovery.

PSPR2

SEMINARS FOR RESILIENCE

LEARNING OBJECTIVES

- Explain who CISA is and what they do in relation to mass casualty incidents
- Define recovery and compare short- and long-term recovery
- Discuss recovery recommendations and identify additional recovery resources
- Describe Run – Hide – Fight
- Understand the goals of post-incident management

HOUSEKEEPING

- Cameras and microphones are disabled
- Safari and Chrome users might experience connectivity issues; recommended to use Teams desktop or mobile application (preferred), Edge, or Firefox
- Please use the Q&A chat in the upper right corner
- Captions may not be enabled by your organization
- Session is being recorded; more information to come

IACET CEUs

G&H is accredited by the International Accreditors for Continuing Education and Training (IACET) and offers IACET Continuing Education Units (CEUs) for its learning events that comply with the ANSI/IACET Continuing Education and Training Standard. IACET is recognized internationally as a standard development organization and accrediting body that promotes quality of continuing education and training.

CEUs are earned by attending the entirety of a session and by achieving an 70% or higher score on a post-webinar knowledge assessment. For every 10-hours of, in-person or virtual, classroom time, a learner can earn 1 CEU. Learners are eligible to earn .1 CEU for attendance at each PSPR2 session for a cumulative total of .9 CEU.

For questions about the PSPR2 CEU process, please contact G&H at training@ghinternational.com or +1 202-955-9505.

For additional information about IACET or the ANSI/IACET Continuing Education and Training Standard, please contact IACET directly at info@iacet.org.

G&H Proprietary Interest Policy

It is the policy of G&H that if instructors have a vested interest in any product, instrument, device, or materials that may be used in this learning event, they must disclose this interest.

Further, if any instructors receive any share of the royalties or profits from product promotion or endorsement, the interest must be disclosed to the learner.

If there are any breaches of this policy, please contact G&H at training@ghinternational.com or +1 202-955-9505.

G&H Anti-Discrimination Policy

G&H is committed to providing working and learning environments free of sexual or any form of unlawful harassment or discrimination.

Harassment or unlawful discrimination against individuals on the basis of actual or perceived race, color, creed, religion, national origin, ancestry, citizenship status, age, sex or gender (including pregnancy, childbirth and pregnancy-related conditions), gender identity or expression (including transgender status), sexual orientation, marital status, military service and veteran status, physical or mental disability, genetic information, or any other characteristic protected by applicable federal, state or local laws and ordinances is illegal and prohibited by G&H policy,.

If there are any breaches of this policy, please contact G&H at training@ghinternational.com or +1 202-955-9505.

Susan Schneider
Chief of Active Assailant Security
Cybersecurity and Infrastructure
Security Agency

Matt Garrett
Interim Director
Oregon Department of
Emergency Management

Brad Richy
Director
Idaho Office of
Emergency Management

Susan Schneider
Chief of Active Assailant Security
Cybersecurity and Infrastructure
Security Agency

Matt Garrett
Interim Director
Oregon Department of
Emergency Management

Brad Richy
Director
Idaho Office of
Emergency Management

Susan Schneider
Chief of Active Assailant Security
Cybersecurity and Infrastructure
Security Agency

Matt Garrett
Interim Director
Oregon Department of
Emergency Management

Brad Richy
Director
Idaho Office of
Emergency Management

Susan Schneider
Chief of Active Assailant Security
Cybersecurity and Infrastructure
Security Agency

Matt Garrett
Interim Director
Oregon Department of
Emergency Management

Brad Richy
Director
Idaho Office of
Emergency Management

Jon Hanian
Public Private Partnerships Program Manager
Idaho Office of
Emergency Management

PSPR2
SEMINARS FOR RESILIENCE

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

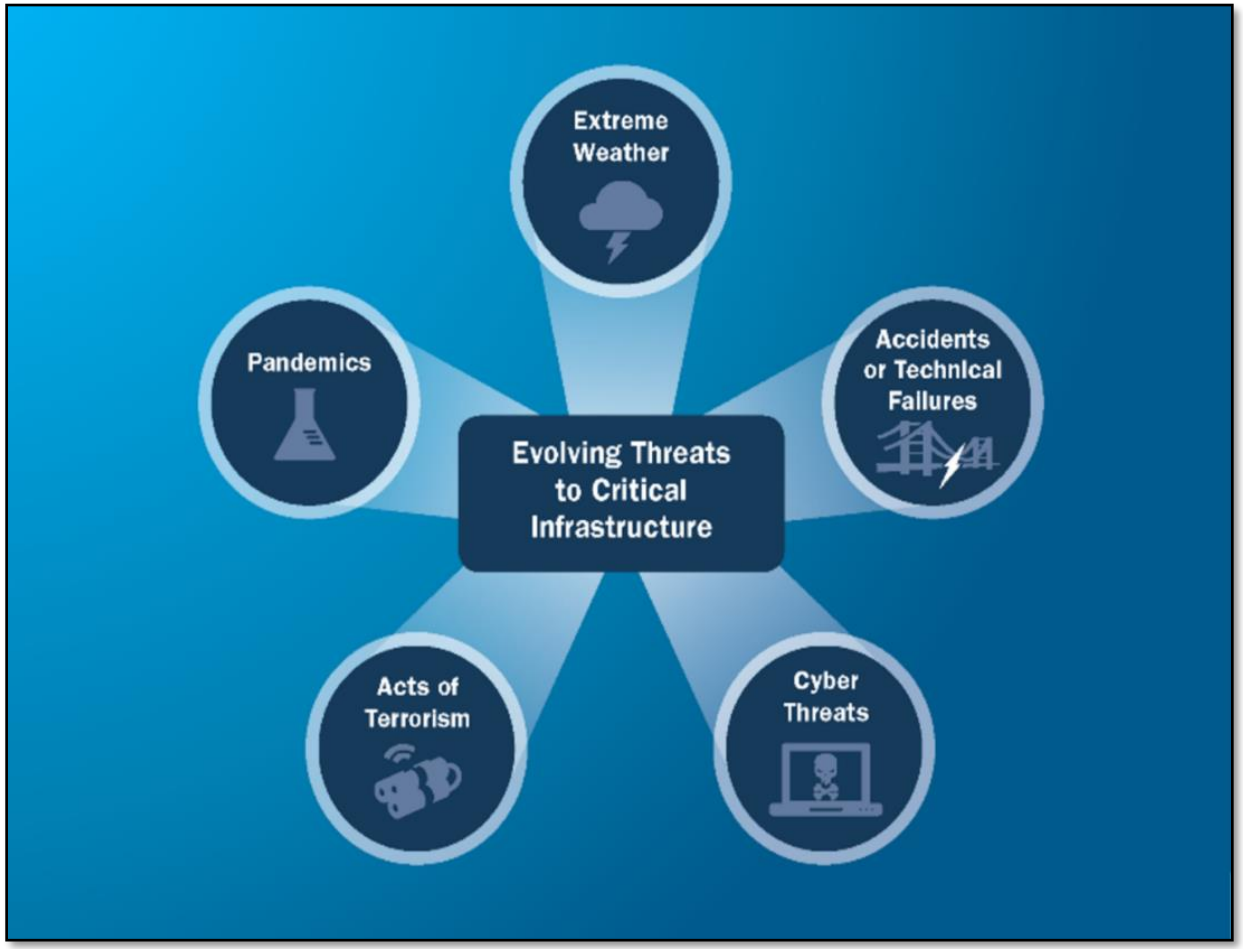
CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed, voluntary decisions and investments.

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.

Threats to Critical Infrastructure

- America remains at risk from a variety of threats including:
  - Acts of Terrorism
  - Cyber Attacks
  - Extreme Weather
  - Pandemics
  - Accidents or Technical Failures



Threats to Critical Infrastructure

- 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

Sector Risk Management Agencies

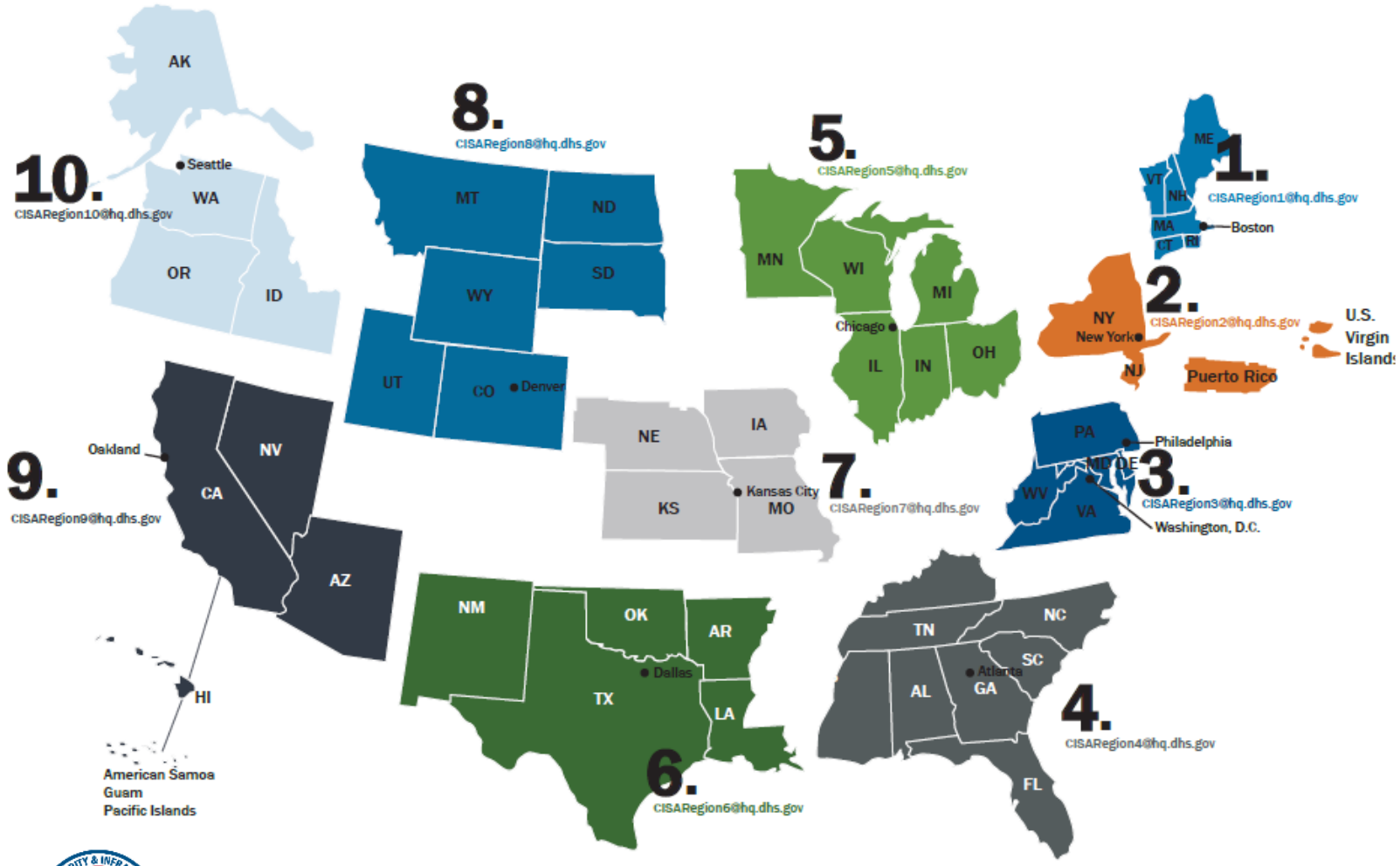
CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	DOT & DHS
WATER	EPA

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:
  - 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

cisa.gov/resources-tools/programs/protective-security-advisor-psa-program

PSA Locations Nationwide



Region 1: Boston, MA

Region 2: New York, NY

Region 3: Philadelphia, PA

Region 4: Atlanta, GA

Region 5: Chicago, IL

Region 6: Dallas, TX

Region 7: Kansas City, MO

Region 8: Denver, CO

Region 9: Oakland, CA

Region 10: Seattle, WA

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

Protected Critical Infrastructure Information

- 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

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.

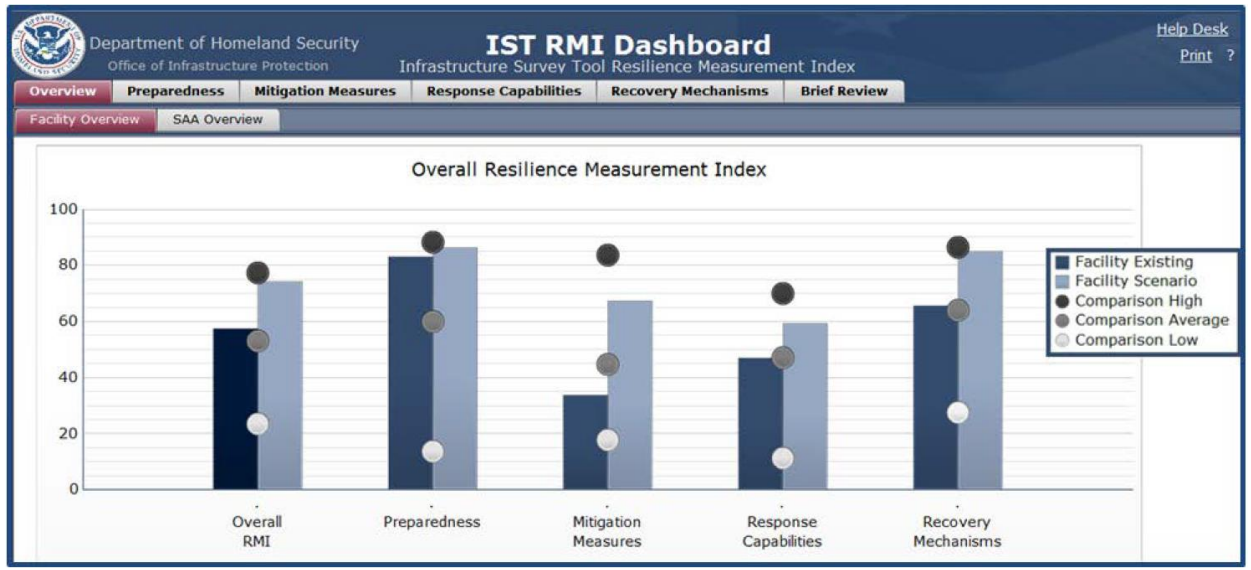
Submission Identification Number:

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program

Infrastructure Survey Tool (IST)

- 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



cisa.gov/resources-tools/services/infrastructure-survey-tool-ist

Security Assessment at First Entry

- 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

cisa.gov/resources-tools/services/security-assessment-first-entry

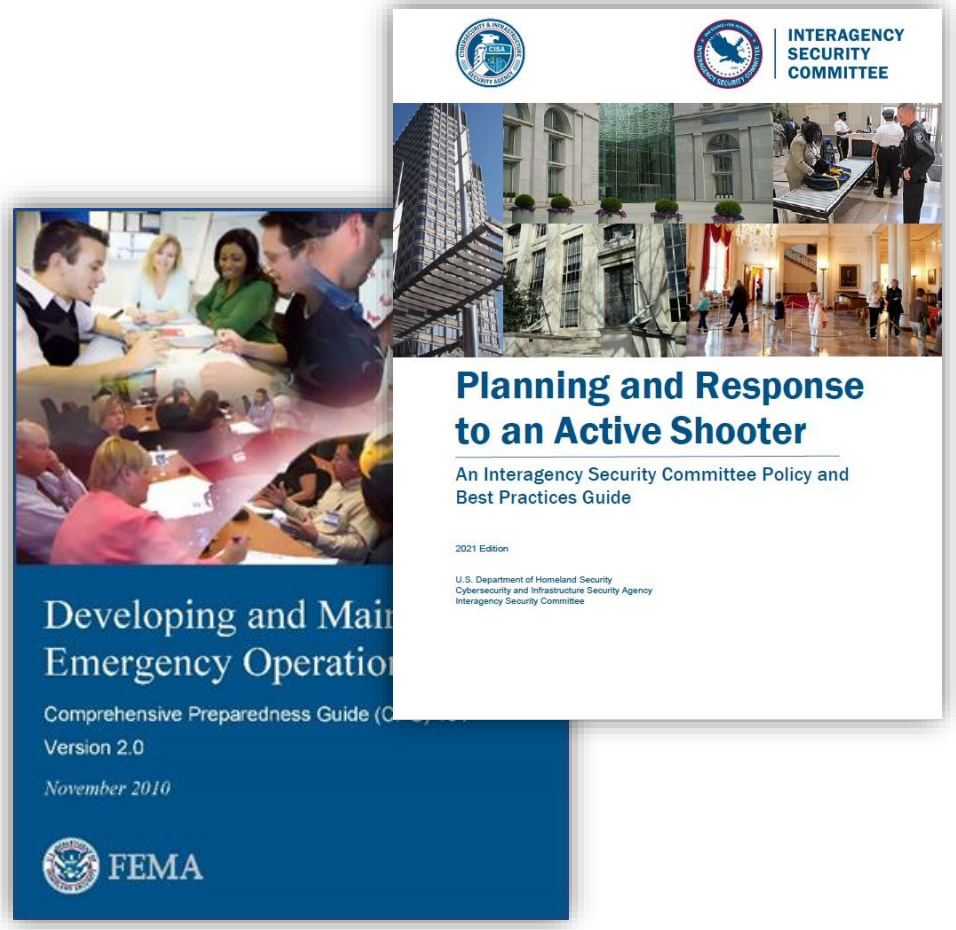
Active Shooter Preparedness Training

cisa.gov/resources-tools/training/active-shooter-preparedness-webinar

Active Shooter Preparedness Plans

A preparedness plan typically will address five areas:

- **Prevention**
- **Protection**
- **Mitigation**
- **Response**
- **Recovery**



cisa.gov/topics/physical-security/active-shooter-preparedness

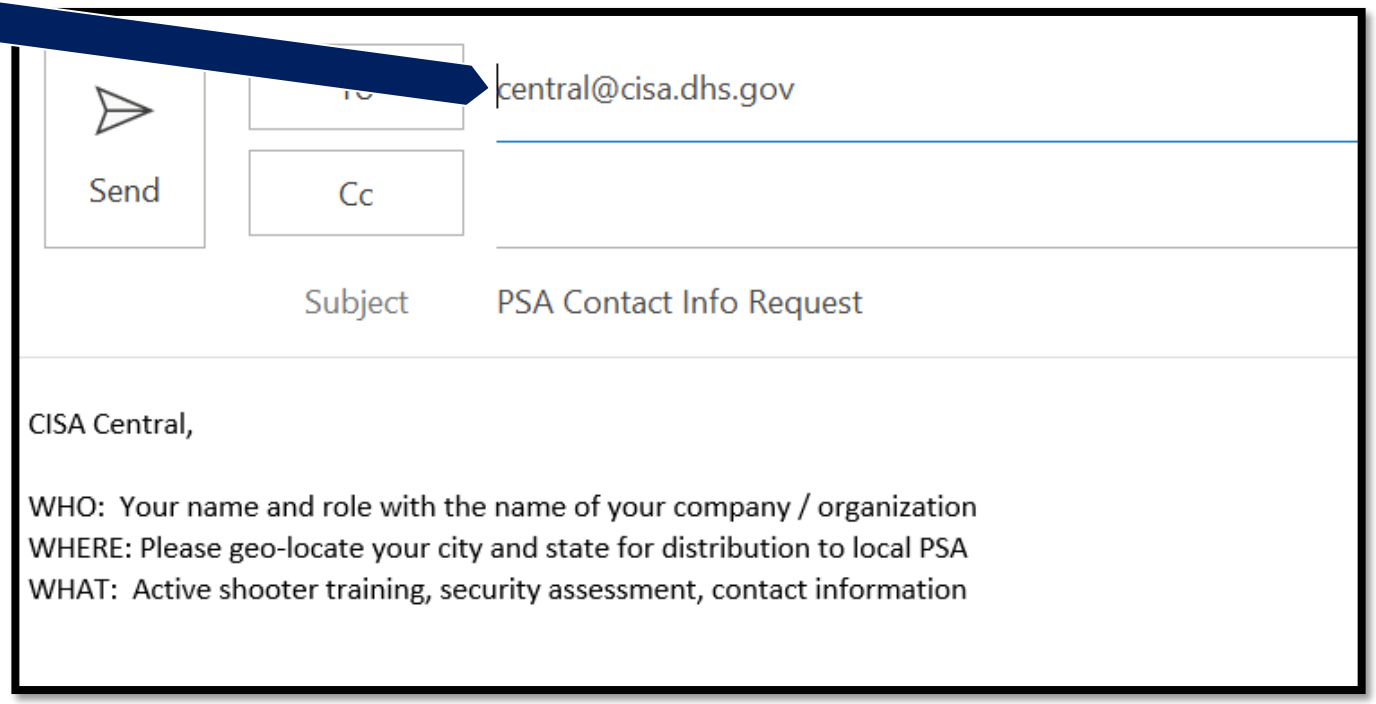
Get in Touch with Your PSA

EMAIL: central@cisa.dhs.gov

WHO: Company Name

WHERE: City, State

WHAT: Requested Service



cisa.gov/resources-tools/programs/protective-security-advisor-psa-program

AN INTRODUCTION TO RECOVERY PREPAREDNESS

What is Recovery?

- Resumption of operations and returning organization or institutions to full functionality
- Occurs over short- and long-term incremental phases for people and organizations
- Progress happens at different rates for your people and the organization as a whole; requires varying degrees of assistance

Recovery Considerations

Short-Term

Address Immediate Needs

- Tend to health and safety
- Enable immediate support
- Establish reunification with families, communities
- Establish a hotline and crisis communications
- Interaction with investigation
- Support funerals and vigils
- Continuity planning

Long-Term

Restoration

- Provide grief counseling
- Resume operations
- Manage donations and volunteers
- Maintain scam and fraud awareness
- Support judicial process
- Establish memorials
- Recovery plan assessment

cisa.gov/resources-tools/resources/active-shooter-recovery-guide

Recovery Planning: Best Practices

- Develop a recovery plan and review it regularly.
- Establish crisis teams and assign duties. Address immediate needs to reestablish safety and long-term restoration considerations.
- Include training on the recovery plan as part of your active shooter preparedness.
- Exercise your recovery plan. Focus on one aspect of the plan and begin a cycle of rotation to address the comprehensive plan.
- Prepare for operational disruption due to an active shooter event, including impacts on personnel, facilities, equipment, and capacity.
- Identify local resources available to support recovery operations and establish relationship with providers in advance.

cisa.gov/resources-tools/resources/active-shooter-recovery-guide

Additional Resources

Active Shooter Preparedness

Products, tools, and resources to help you prepare for, respond to, and recover from an active shooter incident

- Active Shooter Preparedness Webinar
- Active Shooter Recovery Guide
- Recovering from an Active Shooter Incident Fact Sheet

cisa.gov/topics/physical-security/active-shooter-preparedness

Securing Public Gatherings resources

Compendium of resources to help organizations mitigate potential risks in today's dynamic and rapidly evolving threat environment

- Physical Security Considerations for Temporary Facilities
- Personal Security Considerations
- Mass Gathering Security Planning Tool
- Houses of Worship Security Guide and Self-Assessment

cisa.gov/topics/physical-security/securing-public-gatherings

Security Planning Resources

Products, tools, and resources to help you plan and prepare for, an emergency event

- CISA Resources for Critical Infrastructure Owner and Business Partners
- CISA Active Shooter Emergency Action Template and Guide
- DHS Planning Suite

cisa.gov/active-shooter-preparedness-resources-businesses-and-ci-partners

For more information:

cisa.gov/resources-tools/resources/active-shooter-recovery-guide

Subscribe today to receive new products on ***Active Assailant Security***

PSPR2

SEMINARS FOR RESILIENCE

AN INTRODUCTION TO PREPAREDNESS IN THE PRIVATE SECTOR

MASS SHOOTING FACTS

2023: U.S. surpassed 100 mass shootings in only 64 days

The U.S. has surpassed 100 mass shootings in 2023, according to the Gun Violence Archive (GVA), which defines mass shootings as situations in which at least four people are shot and either injured or killed, not including the shooter.

The big picture: The U.S. didn't exceed 100 mass shootings until March 19 in 2022 and March 22 in 2021, according to GVA data.

There were 52 mass shootings in January, 41 in February and 11 so far in March
There were 647 mass shootings in 2022 and another 690 in 2021.

Why it matters: In the first 64 days this year, there have been more mass shootings than days in the U.S. thus far.

FBI & US SECRET SERVICE

According to the Federal Bureau of Investigation:

- Active shooter attacks spiked by 52.5 percent in 2021

The U.S. Secret Service recently released its first-ever report on mass shootings in the United States:

- The report listed key findings and a breakdown of the shooters including that:
  - The most common sites for mass shootings were businesses, restaurants, and retail facilities
- “Today, no industry and no person is immune to these attacks”

GROUND RULES

- This series is not to politically deal with the issues about weapons - guns or otherwise.
- It is to be better prepared – when (and not if) these events happen. Steps to take after an incident has happened.
- Being prepared with Safety, Empathy & Compassion for employees, customers, and the community is our focus
- This can be a very sensitive and difficult topic to discuss.
  - Be sure to take care of yourself

THE OFFICIAL RECORD

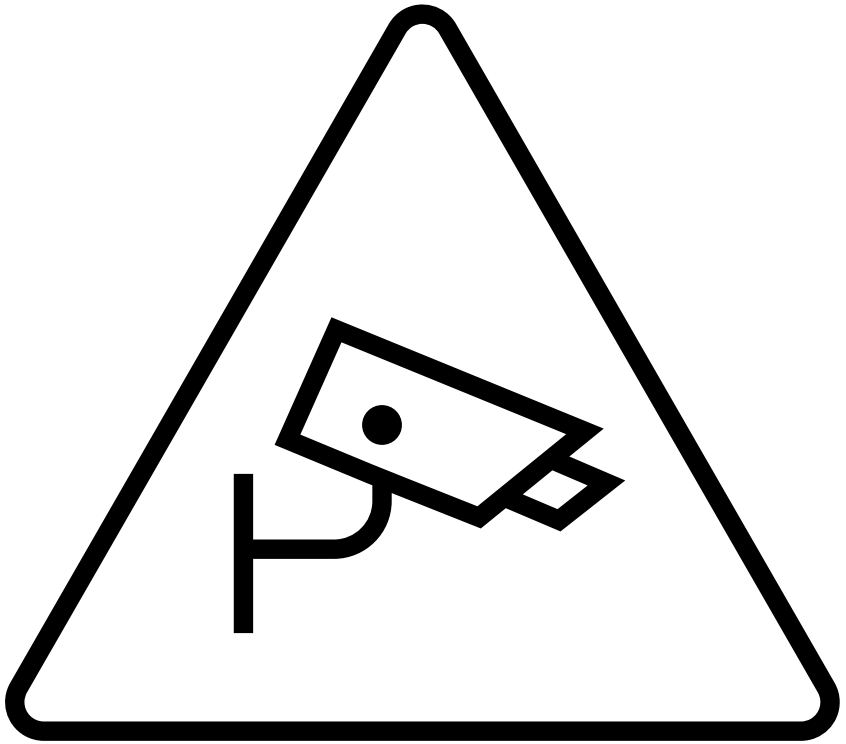
5 MINUTE VIDEO

398 PAGES OF REPORTS

OVER 100 SHOTS FIRED

Yes, your incident will become part of the official record.

SOME CONTEXT



RUN – HIDE – FIGHT

IT WORKS!

- A Run Hide Fight review will become different for the location that goes through an event – be sure to plan for it.
- Part of the training/review needs to include where all the exits are (and secure hiding places) - not just the ones closest to one's immediate work area.
- Be sure you don't have "Timed exits" (doors that remain locked for a period of time when the panic bar is pushed).

RUN – HIDE – FIGHT (CONTINUED)

When you are in the vicinity of an Active Assailant event:

RUN – HIDE – FIGHT

Two other types of actions you must plan for*:

- Shelter in place
- Evacuate – (Leave and Lock)

*Based on what you are told to do by authorities.

PUBLIC-PRIVATE SECTOR RELATIONSHIPS

Sun, Aug 28 at 21:29

Heard about possible active shooter in Bend/Safeway. 🙏🙏😢

Thanks - shooting with one fatality.

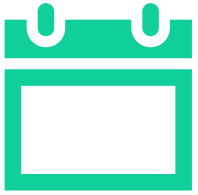
I'm sorry to hear that!

Sketchy details. Glad number is low. Still, not something you want to happen.

DIVIDED TASKS

Immediate – “your” first minutes or hours

Ongoing – then what? What’s next?



Post – next few days, next operational period

GROUPS TO CONSIDER INVOLVING

- Legal
- HR
- Operations
- Asset Protection
- Communications
  - Internal
  - External
- Pharmacy
- Vendors that deliver direct
- Tenants: Banks & Coffee Shops
- Regulatory & Claims

EAP/CID OBSERVATIONS

- Who are you going to call?
- Even if you have a number, what do you need?
- Type of help needed
  - Virtual
  - In-person
  - Group
  - One on One
  - Internal vs External events
- When is help needed
  - Initial need
  - During witness interviews
  - Employee walk-thru prior to re-open
  - Day of re-open
  - On-going

GOALS

- Safe
- Accounted for
- Reunited with their families/friends
- Retrieve their personal possessions
- Proper medical and mental health care, if required
- Re-Open for Business

This Photo by Unknown Author is licensed under CC BY-SA-NC

Q&A

PSPR2

SEMINARS FOR RESILIENCE

Please use the Q&A chat in the top right-hand corner.

NEXT SESSION – REGISTER NOW

REGISTER NOW

PSPR2: It's a Crime Scene—Addressing Immediate Needs

- April 20th, 0900 Pacific/1200 Eastern
- Registration Page:

https://www.eventbrite.com/cc/pspr2-seminar-series-1751269

- Email requests, questions, or comments to training@ghinternational.com

THANK YOU FOR ATTENDING!

We look forward to seeing you at a future session.

PSPR2

SEMINARS FOR RESILIENCE

GH INTERNATIONAL

American Red Cross

Albertsons

NEW YORK STATE | Homeland Security and Emergency Services