

U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) SERVICES

Greater Cincinnati Safety Council
10 May 2023



Gregory A. Howard
September 11, 2023

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

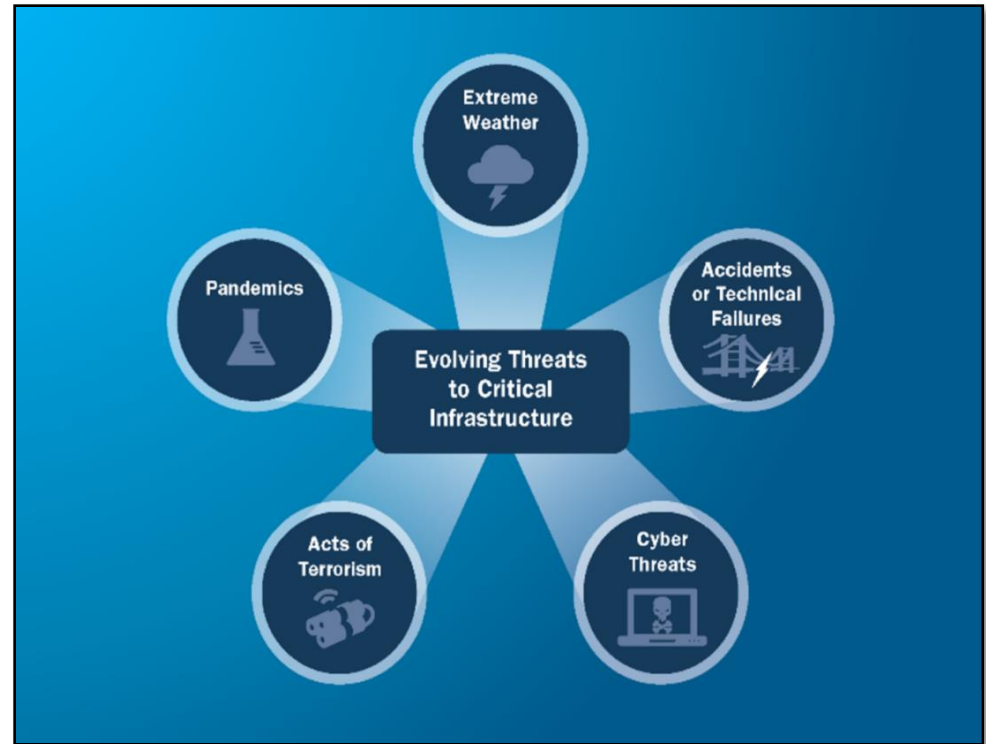
Secure and resilient critical infrastructure for the American people.

MISSION

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

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



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



16 Sectors & Sector Risk Management Agencies

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



SURVEYS AND ASSESSMENTS

PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.



OUTREACH ACTIVITIES

PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities.



SPECIAL EVENT SUPPORT

PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.



INCIDENT RESPONSE

PSAs plan for and, when directed, deploy in response to natural or man-made incidents.



BOMBING PREVENTION AND AWARENESS

PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials for partners to assist in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.



Security Approach

Layered

- Think in terms of “rings of security” – a Layered Defense (to Deter, Detect, Delay, Defend/Respond)
- Physical – Think equipment & people (e.g., locks, cameras, lighting, security force, etc.)
- Procedural – Think plans, operating procedures, training, and exercises
- Intelligence – Awareness of what can be elicited about the facility from publically available sources (e.g., internet, observation, etc.)

Assess Risk

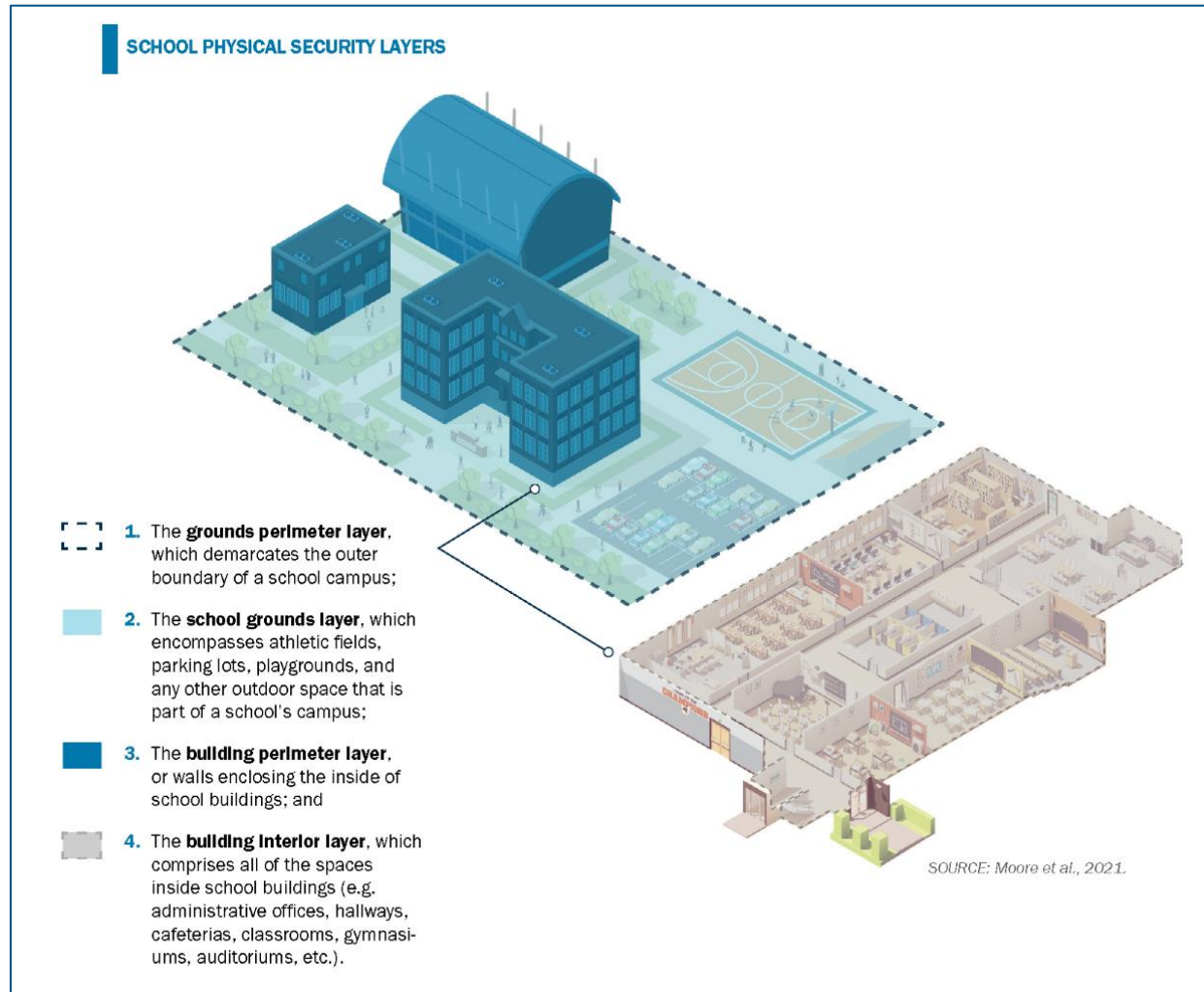
- Risk = Consequence X Vulnerability X Threat
- Make Decision = Avoid, Reduce, Transfer, or Accept

Goal

- Reduce risk (“buy it down”) to the greatest degree possible with the resources you have available



Physical Security Across Layers



Physical Security Assessments

- Infrastructure Survey Tool (IST) = CISA (PSA)
- Security Assessment at First Entry (SAFE) = CISA (PSA)
- Self Assessments (Web Based Available to All) =
 - School Security Assessment Tool (SSAT)
 - House of Worship Security Self-Assessment (HOWSSA)
 - Mass Gatherings Security Planning Tool (MGSPPT)
 - Vehicle Ramming Self-Assessment Tool (VRSAT)



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*



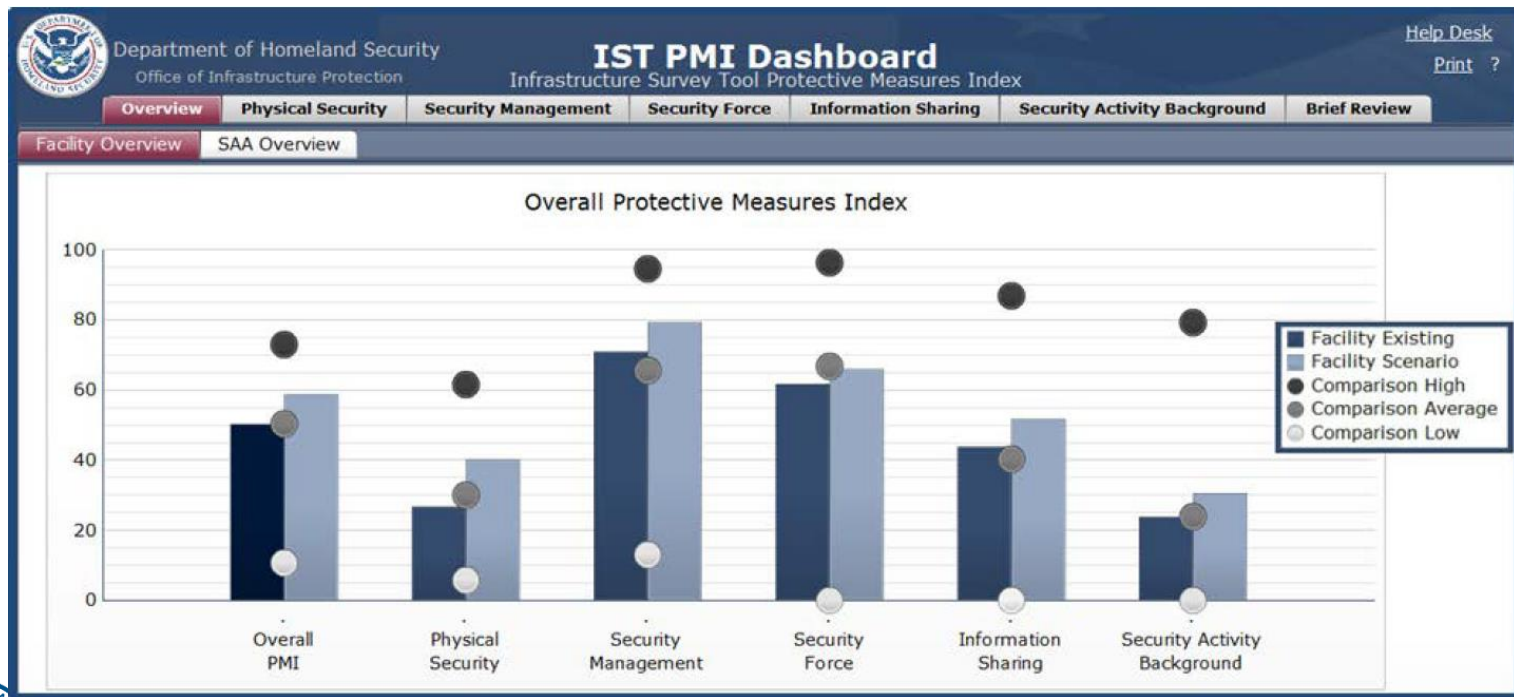
IST Deliverables

- 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
- 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
- SAFE may be better suited for facilities such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics



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



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 | |
| <p>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.</p> <p>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.</p> <p>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.</p> | |
| Access | <p>Individuals eligible to access the attached PCII must be Federal, State or local government employees or contractors and must meet the following requirements:</p> <ul style="list-style-type: none"> Assigned to homeland security duties related to this critical infrastructure; and Demonstrate a valid need-to-know. <p>The recipient must comply with the requirements stated in the CII Act and the Regulation.</p> |
| Handling | <p>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.</p> <p>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.</p> <p>Hand Delivery: Authorized individuals may hand carry material as long as access to the material is controlled while in transit.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Telephone: You are encouraged to use a Secure Telephone Unit/Equipment. Use cellular phones only in exigent circumstances.</p> <p>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.</p> <p>Destruction: Destroy (i.e., shred or burn) this document when no longer needed. For laptops or CPUs, delete file and empty recycle bin.</p> |
| Sanitized Products | <p>You may use PCII to create a work product. The product must not reveal any information that:</p> <ul style="list-style-type: none"> 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 | <p>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.</p> <p>For more information about derivative products, see the PCII Work Products Guide or speak with your PCII Officer.</p> |
| Submission Identification Number: <input type="text"/> | |
| PROTECTED CRITICAL INFRASTRUCTURE INFORMATION | |



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



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.

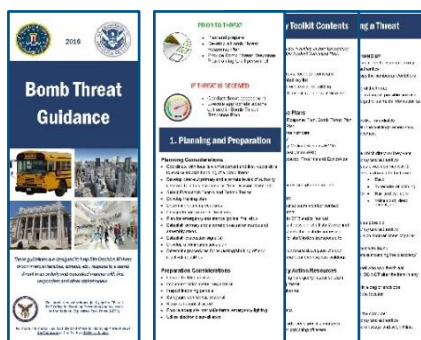
Posters

Ex. Common Household Products Advisory



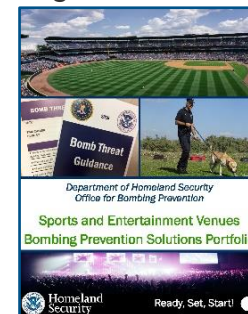
Bomb Threat Guidance Products

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>



Gregory A. Howard
September 11, 2023

Bomb Threat Resources

DHS-DOJ Bomb Threat Guidance



Bomb Threat Procedures & Checklist

BOMB THREAT PROCEDURES

The bomb threat procedures are designed to help employees and decision makers of commercial facilities, schools, etc., respond to a bomb threat in an orderly and controlled manner with the first responders and other stakeholders. Most bomb threats are received by phone. Bomb threats are serious and require attention. Act quickly, but remain calm and obtain information with the individual on the receipt of the call.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to draw more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone is ringing, keep the number and/or notes on the window display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of call, DO NOT HANG UP, but from a different phone, contact authorities immediately with information and exact instructions.

If a bomb threat is received by handwritten note:

- Handle note as minimally as possible.
- If a bomb threat is received by a mail:
- Call:
- Do not disseminate the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Strange odor
- Strange sounds
- Unexplained delivery
- Plainly handwritten
- Misplaced words
- Insected titles
- Strange postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone. Radio signals have the potential to detonate a bomb.
- Touch or move a suspicious package.

WHO TO CONTACT (Select One)

- 911
- Follow your local guidelines

For more information about this form contact the Office for Bombing Prevention at: OBP@cisa.dhs.gov

BOMB THREAT CHECKLIST

DATE: _____ TIME: _____

TIME CALLED: _____ PHONE NUMBER WHERE CALL RECEIVED: _____

Ask Caller:

- Where is the bomb located? (Building, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of device is it?
- What will make it explode?
- OR (If possible) YES/NO
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (Building, room, etc.)
- Estimated age
- Is voice familiar? If yes, who does it sound like?
- Other points:

| Caller Name | Redacted Name | Threat Name |
|-------------|---------------|-------------|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |
| 16 | | |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | | |
| 21 | | |
| 22 | | |
| 23 | | |
| 24 | | |
| 25 | | |
| 26 | | |
| 27 | | |
| 28 | | |
| 29 | | |
| 30 | | |
| 31 | | |
| 32 | | |
| 33 | | |
| 34 | | |
| 35 | | |
| 36 | | |
| 37 | | |
| 38 | | |
| 39 | | |
| 40 | | |
| 41 | | |
| 42 | | |
| 43 | | |
| 44 | | |
| 45 | | |
| 46 | | |
| 47 | | |
| 48 | | |
| 49 | | |
| 50 | | |

DHS-DOJ Bomb Threat Stand-Off Card

| BOMB THREAT STAND-OFF CARD | | | | | |
|-------------------------------|---------------------|-------------------------------|-----------------------|-------------------------------|--|
| OFFICE FOR BOMBING PREVENTION | | | | | |
| Threat Description | Explosives Capacity | Mandatory Evacuation Distance | Shelter-In-Place Zone | Preferred Evacuation Distance | |
| Pipe Bomb | 5 lbs | 75 ft | 75-119 ft | +1200 ft | |
| Suicide Bomber | 25 lbs | 110 ft | 111-169 ft | +1700 ft | |
| Briefcase/Suitcase | 50 lbs | 150 ft | 151-199 ft | +1800 ft | |
| Car | 500 lbs | 320 ft | 321-1099 ft | +1900 ft | |
| SUV/Van | 1,000 lbs | 400 ft | 401-2299 ft | +2400 ft | |
| Small Delivery Truck | 4,000 lbs | 640 ft | 641-2799 ft | +3000 ft | |
| Container/Water Truck | 10,000 lbs | 960 ft | 961-3599 ft | +3100 ft | |
| Semi-Trailer | 60,000 lbs | 1575 ft | 1576-9299 ft | +3300 ft | |

DEFEND TODAY, SECURE TOMORROW

CAUTION!

Do not touch suspicious item

- Notify proper Authorities - Call 911
- Ensure all witnesses are available to brief 1st responders
- Recommended stand-off data should be used in conjunction with your emergency evacuation plan

Shelter-In-Place Zone

Move to Further Distance if possible, and when safe, evacuate from building to safe area.

Mandatory Evacuation Distance

Increase to Preferred Evacuation Distance

Source: Department of Homeland Security, Office for Bombing Prevention, Arlington, VA
 FBI, Bomb Data Center, Quantico, VA
 National Security Group, Arlington, VA

Suspicious vs. Unattended Card

Suspicious or Unattended?

Criminals or terrorists sometimes conceal improvised explosive devices (IEDs) in backpacks, suitcases, or common items.

Use this process to safely determine if an item is a serious threat or just unattended.

Is it HOT?

YES

• Do not touch

• Notify proper authorities

• Do not move

NO

• Do not touch

• Notify proper authorities

• Do not move

If an item is suspicious you should:

R Recognize the Indicators of a Suspected Explosive Device

A Avoid the Area

I Isolate the Suspected Item

N Notify Appropriate Emergency Services

Indicators can be related to the characteristics, sounds, location, or time, including what the item is, where it is, and how it is used.

Do not touch the suspected item, remove, relocate, move and direct others to move away immediately.

Establish a perimeter to prevent the area and restrict to avoid people nearby. Use barriers and personnel (if available) to establish a secure perimeter (per OBP guidance).

Check the location, time and person, the person's status, the location of the item, the time of placement and discovery, and how the item is used.

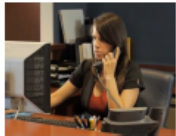
If you see something, say something!

REPORT SUSPICIOUS ITEMS. Contact local law enforcement or 911 in case of emergency.

Available at: www.cisa.gov/what-to-do-bomb-threat



Training Video Series



What to Do: Bomb Threat – Although a bomb threat may seem rare, they happen every day across the nation. Reacting quickly and safely to a bomb threat could save lives, including your own. This video demonstrates the procedures you should follow during a bomb threat and will help you prepare and react appropriately.



What to Do: Suspicious or Unattended Item – Demonstrates how you can determine whether an item is suspicious (potential bomb) or simply unattended and will help you prepare and react appropriately.



What to Do: Bomb Searches – Set in a school, this video describes basic bomb search procedures to use once the determination has been made that a search is warranted, and authorities have been notified. This video demonstrates in detail, the room, route, and area search techniques that can be applied to any type of facility.

What to know OBP Training Video Series:

- Short 5 - 7-minute training videos
- Individual or group viewing
- Mobile device friendly – view on your smartphone
- Accessible anywhere, any time

To view any of the Instructional Videos, please visit www.cisa.gov/bombing-prevention-training



Homeland Security Information Network

- The Homeland Security Information Network (HSIN) is DHS's primary technology tool for trusted information sharing



“If You See Something, Say Something”



“If You See Something, Say Something™” is a national anti-terrorism campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well the importance of reporting suspicious activity to state and local law enforcement

To become a partner, send an email to:
seesay@hq.dhs.gov

For more information visit:
www.dhs.gov/see-something-say-something





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>



Gregory A. Howard
September 11, 2023

Active Shooter Preparedness Brief



Active Shooter Preparedness Webinar

- Two-hour, virtual webinars conducted periodically.
- Focus on:
 - Discussing the elements of active shooter incident response planning with guidance from expert instructors;
 - Describing common behaviors, conditions, and situations associated with active shooter events;
 - Discussing how to recognize potential workplace violence indicators; and
 - Providing information about best practices, communications protocols, and resources that will assist stakeholders to develop or enhance their emergency planning, preparedness, and response to active shooter incidents.
- Modules from the pre-COVID day-long workshops can be downloaded from DHS. (See <https://www.cisa.gov/active-shooter-workshop-participant>.)
- Check with PSA for offerings.



Power of Hello

Employee Vigilance through the **Power of Hello**

Alert employees can spot suspicious activity and report it



Used effectively, the right words can be a powerful tool. Simply saying “Hello” can prompt a casual conversation with unknown individuals and help you determine why they are there. **The OHNO approach – Observe, Initiate a Hello, Navigate the Risk, and Obtain Help** – helps employees observe and evaluate suspicious behaviors, empowers them to mitigate potential risk, and obtain help when necessary.

The **OHNO** approach to risk prevention relies on reasonable persons to make these observations to properly detect and report terrorism/criminal-related suspicious behavior.



For additional **Power of Hello** resources please visit [cisa.gov/employee-vigilance-power-hello](https://www.cisa.gov/employee-vigilance-power-hello).

DHS’ “If You See Something, Say Something®” campaign provides additional information on how to recognize and report the indicators of terrorism-related suspicious activity.



<https://www.cisa.gov/employee-vigilance-power-hello>

Gregory A. Howard
September 11, 2023

Employee Vigilance and De-Escalation

- Recognize
- Assess
- De-escalate
- Report

CYBERSECURITY INFRASTRUCTURE SECURITY EMERGENCY COMMUNICATIONS NATIONAL RISK MANAGEMENT ABOUT CISA MEDIA

Infrastructure Security > Hometown Security > Active Shooter Preparedness > Employee Vigilance and De-escalation

Employee Vigilance

De-Escalation Series - Translated Resources

Active Shooter Preparedness

Active Shooter Workshop Participant

Employee Vigilance ▾

First Responder

Products/Resources

Human Resources or Security Professional

Private Citizen

Active Shooter Workshop Participant

Translated Active Shooter Resources

Insider Threat Mitigation Resources

EMPLOYEE VIGILANCE AND DE-ESCALATION

First Responders and Security Professionals

Private Citizens

Critical Infrastructures and Businesses

Active Shooter Preparedness Workshop/Webinar

Employee Vigilance and De-escalation

Products/Resources

Industries face a variety of threats, both internal and external, from hostile governments, terrorist groups, disgruntled employees and malicious introducers. Alert employees can spot suspicious activity and report it. The power is in the employee, citizen, patron, or any person who can observe and report.

[Expand All Sections](#)

Power of Hello +

Insider Threat Mitigation +

De-escalation +



<https://www.cisa.gov/employee-vigilance-and-de-escalation>

Gregory A. Howard
September 11, 2023

Insider Threat Mitigation

- Develop Insider Threat Program
 - Define
 - Detect
 - Assess
 - Manage

Infrastructure Security

- Infrastructure Security Month
- Securing Public Gatherings
- Infrastructure Dependency Primer
- 2015 Sector Specific Plans
- Autonomous Vehicle Security
- Critical Infrastructure Exercises -
- Cybersecurity and Physical Security Convergence
- IDT
- Interagency Security Committee
- Chemical Security
- Critical Infrastructure Sector Partnerships
- Critical Infrastructure Training
- Critical Infrastructure Vulnerability Assessments
- Dams Sector Resources
- IDR Program
- Information Sharing: A Vital Resource
- Insider Threat Mitigation -

INSIDER THREAT MITIGATION



Insider Threat Mitigation

Insider threat incidents are possible in any sector or organization. An insider threat is typically a current or former employee, third-party contractor, or business partner. In their present or former role, the person has or had access to an organization's network systems, data, or premises, and uses their access (sometimes unwittingly). To combat the insider threat, organizations can implement a proactive, prevention-focused mitigation program to detect and identify threats, assess risk, and manage that risk - before an incident occurs.

The information and resources available from the Cybersecurity and Infrastructure Security Agency (CISA) will help individuals, organizations, and communities create or improve an existing insider threat mitigation program. Organizations putting such a program into practice must remain adaptable. As infrastructure communities work internally at protecting against insider threat and share lessons learned, they can protect the Nation. And if insider threat disruptions should occur, organizations with mature programs can prove resilient.

The key steps to mitigate insider threat are Define, Detect and Identify, Assess, and Manage. Click on the icons below to learn more about each step.



Define Detect & Identify Assess Manage

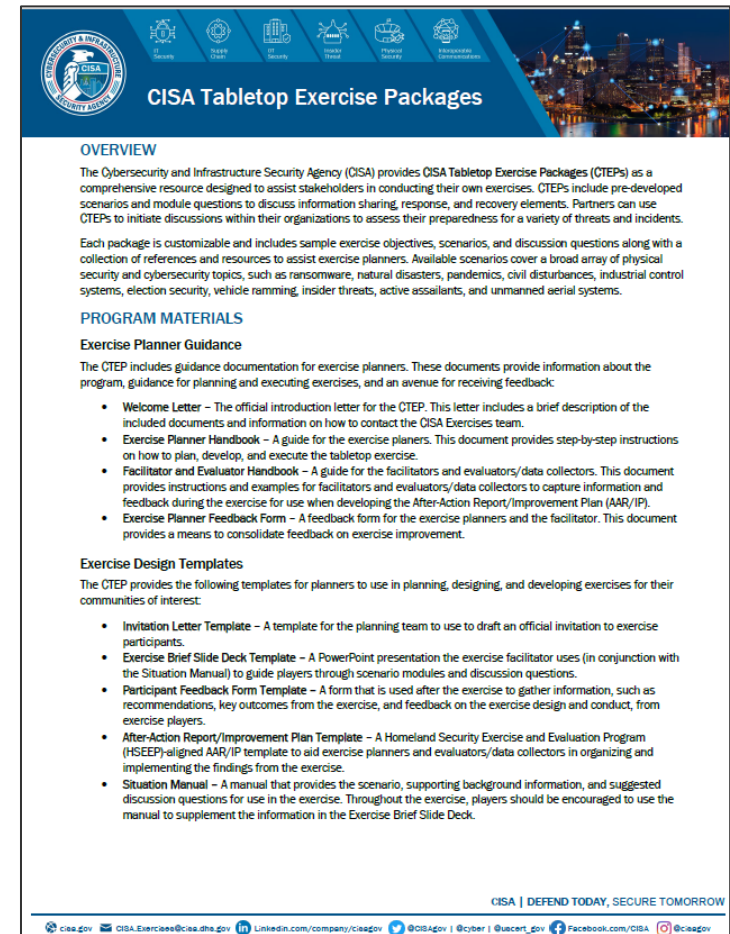


<https://www.cisa.gov/insider-threat-mitigation-resources-and-tools>

Gregory A. Howard
September 11, 2023

CISA Tabletop Exercise Packages (CTEP)

- “Tabletop Exercise (TTX) in a Box”
 - Exercise Planner Guidance
 - Welcome Letter
 - Exercise Planner Handbook
 - Facilitator and Evaluator Handbook
 - Exercise Planner Feedback Form
 - Exercise Design Templates
 - Invitation Letter
 - Exercise Brief Slide Deck
 - Situation Manual
 - Participant Feedback Form
 - After-Action Report
 - Exercise Scenarios
 - Cyber/Active Shooter/Vehicle Ramming
 - Complex Coordinated Attack (Active Shooter & IED)



The image shows a screenshot of the CISA Tabletop Exercise Packages (CTEP) Overview document. The header features the CISA logo and a navigation bar with icons for various security domains. The main content is divided into sections: Overview, Program Materials, and Exercise Design Templates. The Overview section describes the CTEPs as a comprehensive resource for stakeholders. The Program Materials section lists the Exercise Planner Guidance documents. The Exercise Design Templates section lists the templates for planning, designing, and developing exercises.

CISA Tabletop Exercise Packages

OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) provides CISA Tabletop Exercise Packages (CTEPs) as a comprehensive resource designed to assist stakeholders in conducting their own exercises. CTEPs include pre-developed scenarios and module questions to discuss information sharing, response, and recovery elements. Partners can use CTEPs to initiate discussions within their organizations to assess their preparedness for a variety of threats and incidents.

Each package is customizable and includes sample exercise objectives, scenarios, and discussion questions along with a collection of references and resources to assist exercise planners. Available scenarios cover a broad array of physical security and cybersecurity topics, such as ransomware, natural disasters, pandemics, civil disturbances, industrial control systems, election security, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.

PROGRAM MATERIALS

Exercise Planner Guidance

The CTEP includes guidance documentation for exercise planners. These documents provide information about the program, guidance for planning and executing exercises, and an avenue for receiving feedback:

- **Welcome Letter** – The official introduction letter for the CTEP. This letter includes a brief description of the included documents and information on how to contact the CISA Exercises team.
- **Exercise Planner Handbook** – A guide for the exercise planners. This document provides step-by-step instructions on how to plan, develop, and execute the tabletop exercise.
- **Facilitator and Evaluator Handbook** – A guide for the facilitators and evaluators/data collectors. This document provides instructions and examples for facilitators and evaluators/data collectors to capture information and feedback during the exercise for use when developing the After-Action Report/Improvement Plan (AAR/IP).
- **Exercise Planner Feedback Form** – A feedback form for the exercise planners and the facilitator. This document provides a means to consolidate feedback on exercise improvement.

Exercise Design Templates

The CTEP provides the following templates for planners to use in planning, designing, and developing exercises for their communities of interest:

- **Invitation Letter Template** – A template for the planning team to use to draft an official invitation to exercise participants.
- **Exercise Brief Slide Deck Template** – A PowerPoint presentation the exercise facilitator uses (in conjunction with the Situation Manual) to guide players through scenario modules and discussion questions.
- **Participant Feedback Form Template** – A form that is used after the exercise to gather information, such as recommendations, key outcomes from the exercise, and feedback on the exercise design and conduct, from exercise players.
- **After-Action Report/Improvement Plan Template** – A Homeland Security Exercise and Evaluation Program (HSEEP)-aligned AAR/IP template to aid exercise planners and evaluators/data collectors in organizing and implementing the findings from the exercise.
- **Situation Manual** – A manual that provides the scenario, supporting background information, and suggested discussion questions for use in the exercise. Throughout the exercise, players should be encouraged to use the manual to supplement the information in the Exercise Brief Slide Deck.

CISA | DEFEND TODAY, SECURE TOMORROW

[cisa.gov](https://www.cisa.gov) CISA.Exercises@cisa.dhs.gov [LinkedIn.com/company/cisa.gov](https://www.linkedin.com/company/cisa.gov) [@CISAGov](https://twitter.com/CISAGov) [Facebook.com/CISA](https://www.facebook.com/CISA) [@cisa.gov](https://www.instagram.com/cisa.gov)



<https://www.cisa.gov/cisa-tabletop-exercise-packages>

Gregory A. Howard
September 11, 2023

Cybersecurity Resources

- Cybersecurity Advisor Program
- Cybersecurity Assessments
- Response Assistance

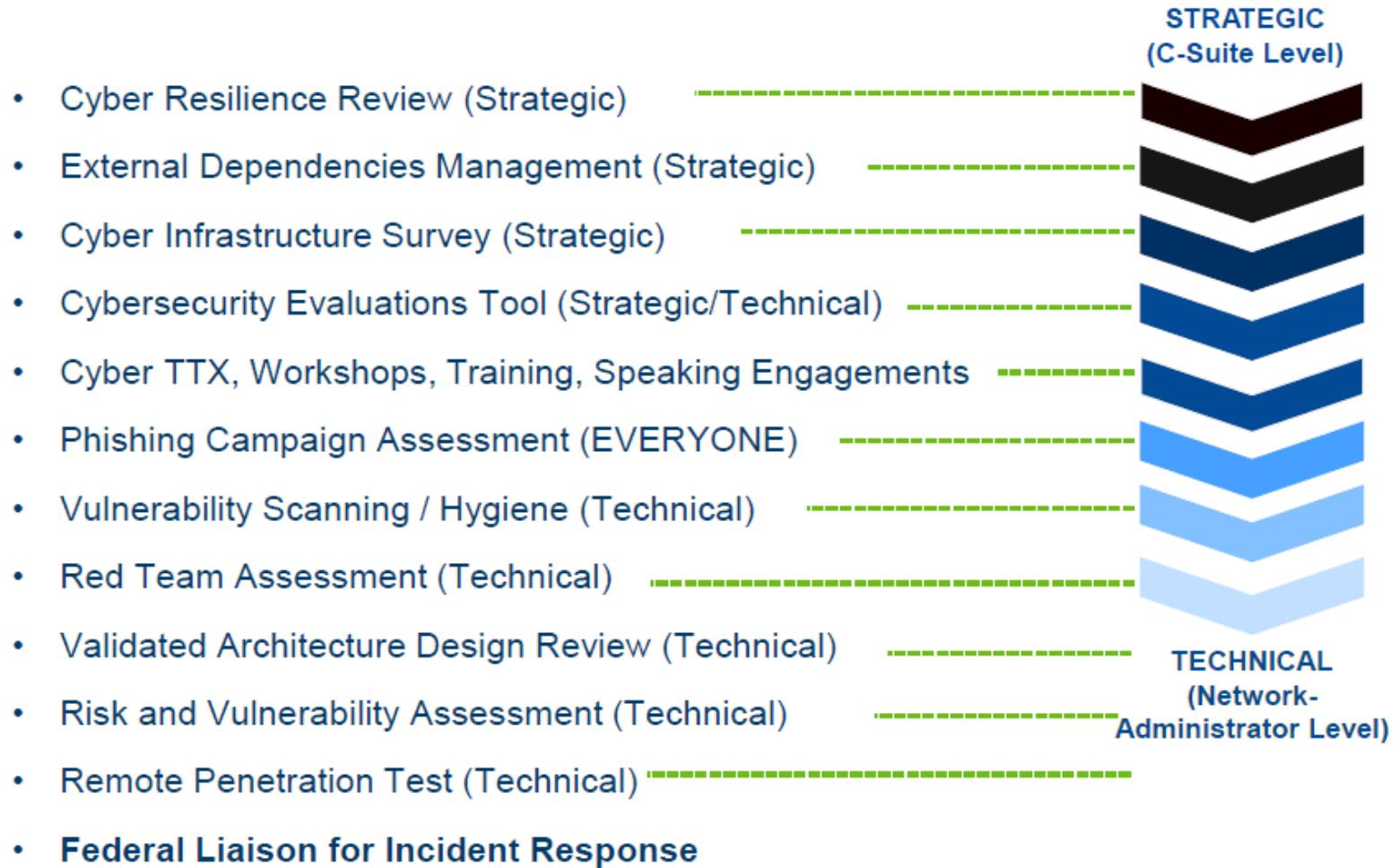


Cybersecurity Advisor Program

- Cybersecurity Advisors (CSA) offer assistance to help prepare and protect private sector entities and governments from cybersecurity threats
 - **Assess:** Evaluate critical infrastructure cyber risk
 - **Promote:** Encourage best practices and risk mitigation strategies
 - **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups
 - **Educate:** Inform and raise awareness
 - **Listen:** Collect stakeholder requirements
 - **Coordinate:** Bring together incident support and lessons learned



CISA Cybersecurity Services (No Fee)



Response Assistance

- Remote and on-site assistance
- Malware analysis (www.malware.us-cert.gov)
- Incident coordination



Cyber Incident Reporting

- CISA Watch provides real-time threat analysis and incident reporting capabilities
- To report an incident or find out more about the CISA Cyber Service Offerings, contact the service desk at CISAServiceDesk@cisa.dhs.gov
- You should report all suspected or confirmed cyber attacks or incidents that:
 - Affect core critical infrastructure functions
 - Result in the loss of data, system availability, or system control
 - Indicate malicious software is present on critical systems



PSA/CSA Ohio Contact Info

PSAs

- **Cleveland**
(Yellow) -
PSA Jon
Richeson
- **Columbus**
(White) -
SPSA Patrick
Shaw
- **Cincinnati**
(Green) –
PSA Gregory
Howard

➤ (202) 495-9082
Jonathan.Richeson@cisa.dhs.gov

➤ (216) 410-3718
patrick.shaw@hq.dhs.gov

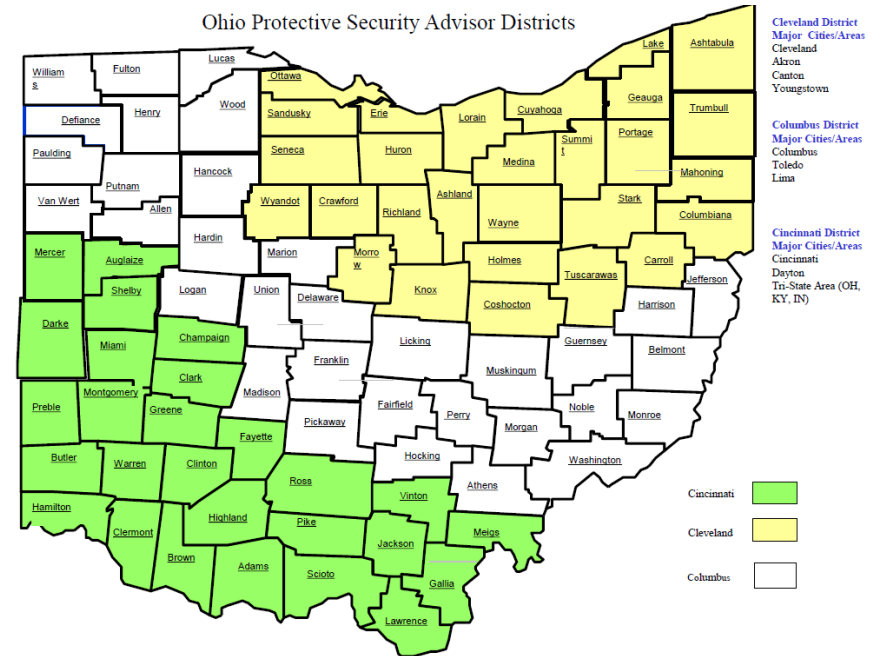
➤ (513) 526-1018
gregory.howard@hq.dhs.gov

CSAs

- **Ohio –**
Terin Williams terin.williams@cisa.dhs.gov

Spencer Wood ➤ (202) 793-4498

Spencer.wood@cisa.dhs.gov



Gregory A. Howard
September 11, 2023



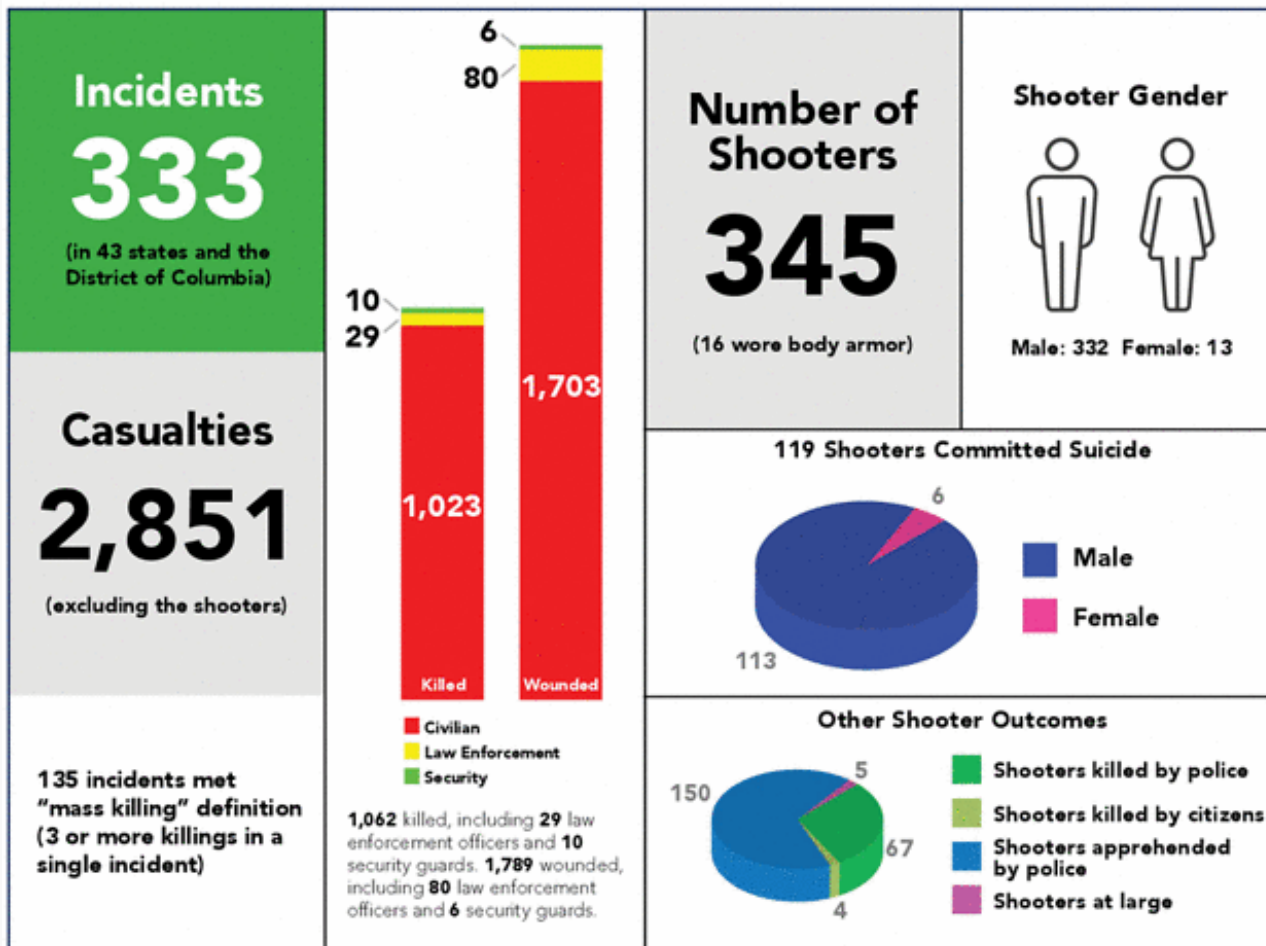
Questions?

For more information:
cisa.gov

Gregory Howard
Protective Security Advisor
513-526-1018
Gregory.howard@hq.dhs.gov



Active Shooter Incidents (2000 – 2019)



FBI - Active Shooter Incidents 20-Year Review from 2000 to 2019

<https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>



Active Shooter Incidents (2021 vs. 2022)

| 2021 | 2022 | |
|--|--|---|
| 61 in 30 states | 50 in 25 states +DC* | Total Incidents |
| 243 103 killed 140 wounded | 313 100 killed 213 wounded | Casualties (Excluding Shooters) |
| 2 | 1 | Law Enforcement Officers Killed |
| 5 | 21 | Law Enforcement Officers Wounded |
| 12 | 13 | Met "Mass Killing" Definition |
| 17 | 9 | Incidents Where Law Enforcement Engaged Shooters |
| 60 male 1 female | 47 male 1 female 1 nonbinary 1 unidentified | Shooter Gender |
| 2 | 4 | Shooters Wore Body Armor |
| 11 | 9 | Shooters Committed Suicide |
| 14 | 7 | Shooters Killed by Law Enforcement |
| 4 | 2 | Shooters Killed by Citizen |
| 30 1 at large | 29** 3 at large | Shooters Apprehended by Law Enforcement |
| * Two incidents occurred in two states. ** Three shooters were restrained by citizens prior to law enforcement arrival. | | <div>Decreased metrics</div> <div>Increased metrics</div> |



Active Shooter Incidents – U.S. (2000 - 2019)



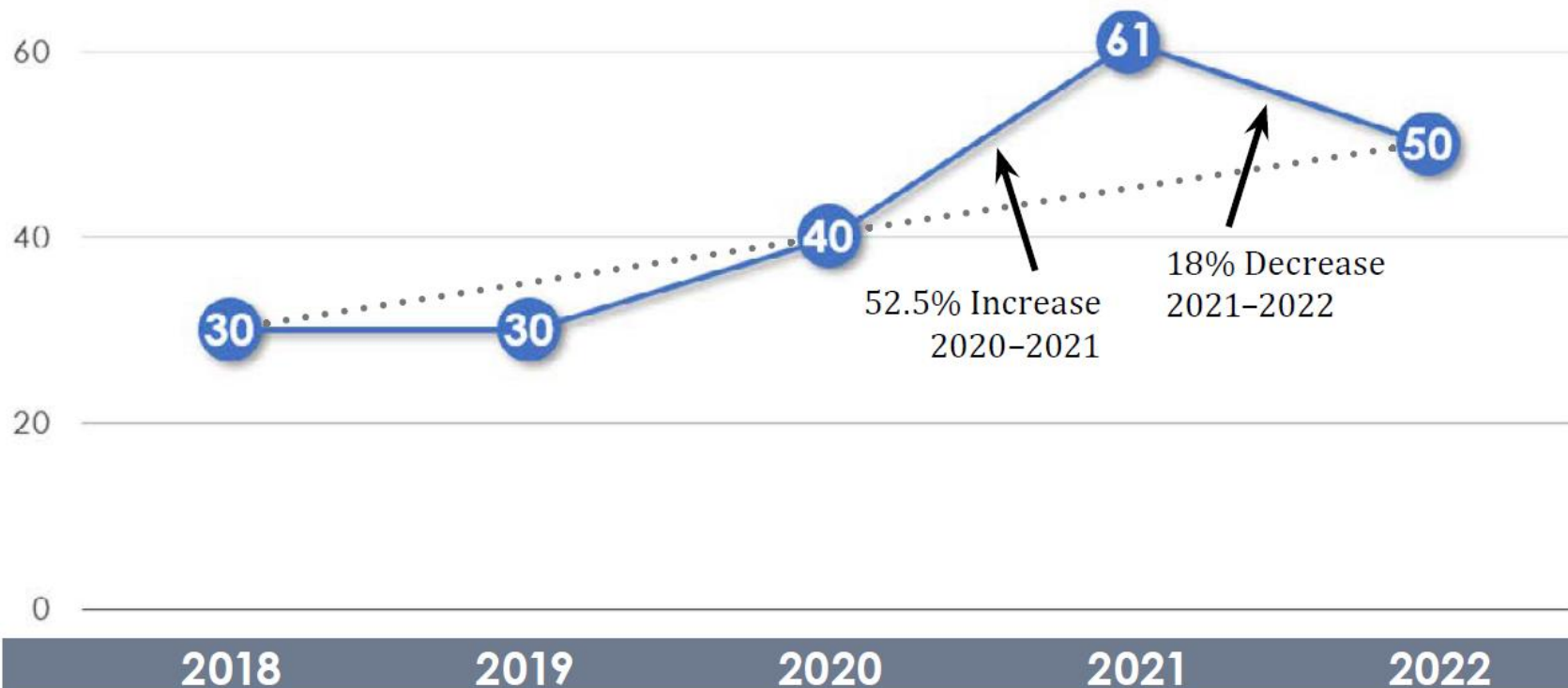
FBI - Active Shooter Incidents 20-Year Review from 2000 to 2019

<https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>

Active Shooter Incidents (2018 – 2022)

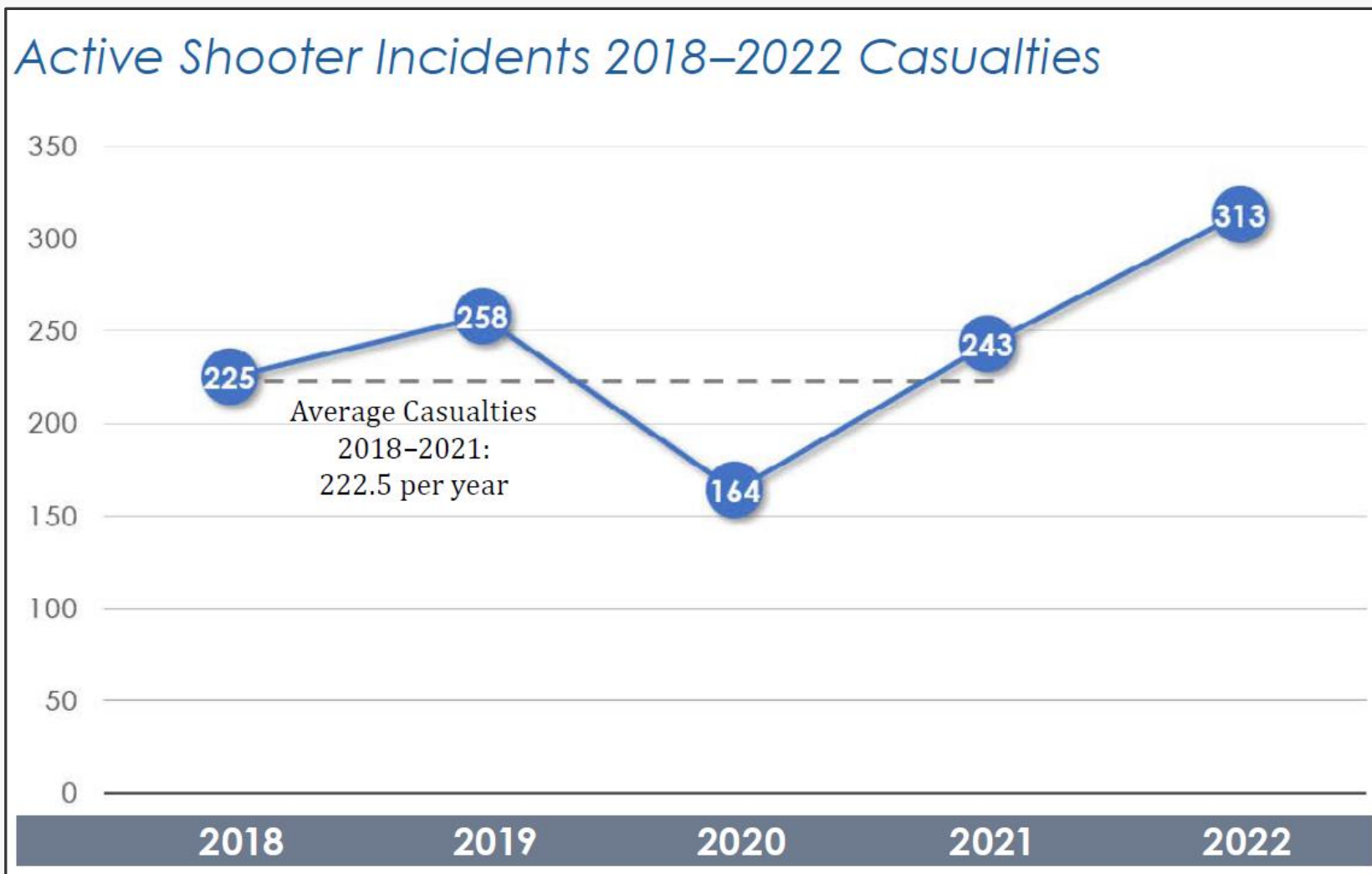
Incident Statistics

Active Shooter Incidents 2018–2022

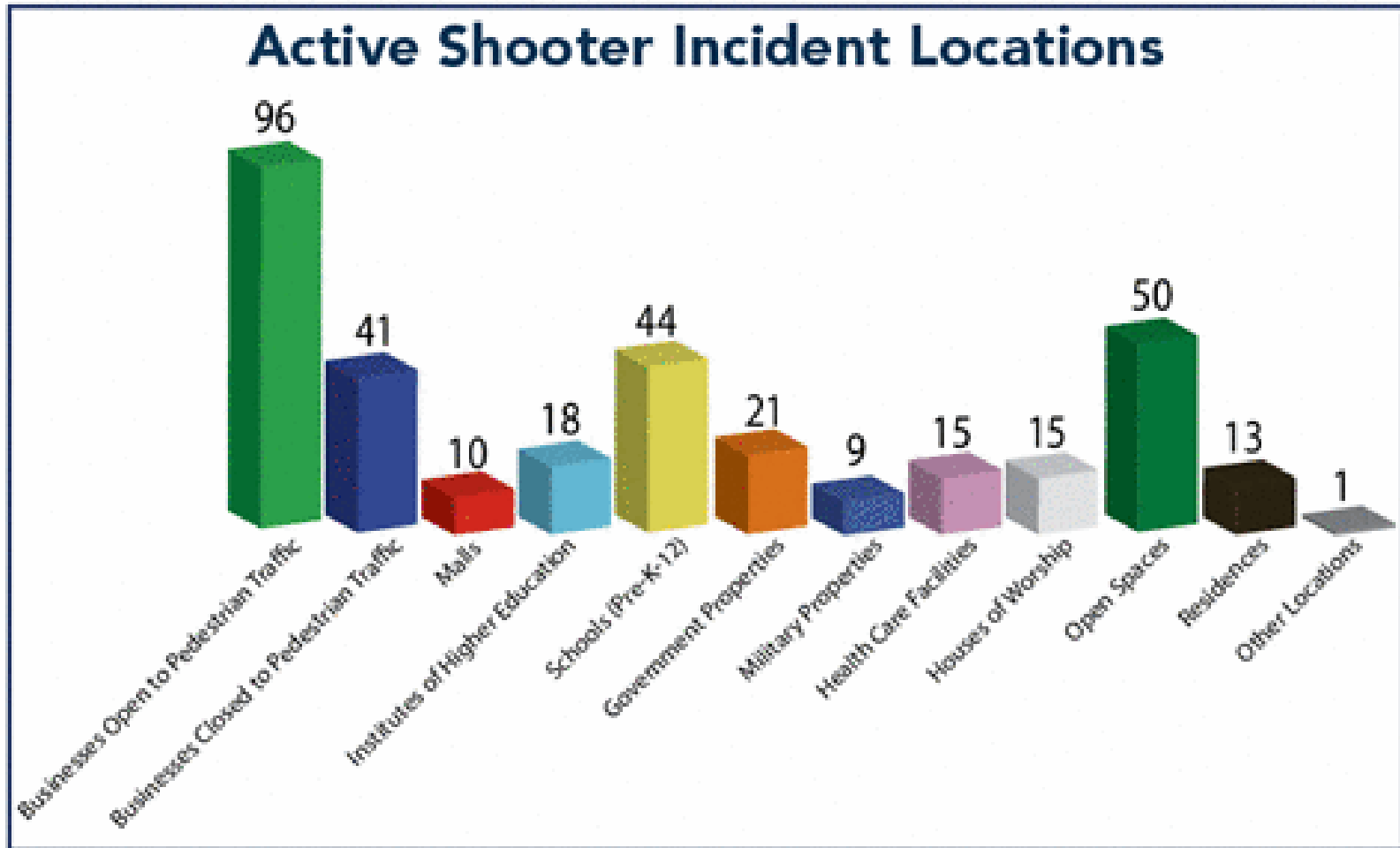


FBI Report. *Active Shooter Incidents in the United States in 2022* (Apr 2023)

Active Shooter Incidents – Casualties (2018 - 2022)



Active Shooter Incidents (2000 – 2019)



FBI - Active Shooter Incidents 20-Year Review from 2000 to 2019

<https://www.fbi.gov/file-repository/active-shooter-incidents-20-year-review-2000-2019-060121.pdf/view>



Active Shooter Incidents - Locations (2022)

Locations



Twenty-three³⁴ of the 50 incidents occurred in **open space** locations, resulting in 29 people killed (including one law enforcement officer)³⁵ and 76 people wounded (including six law enforcement officers).



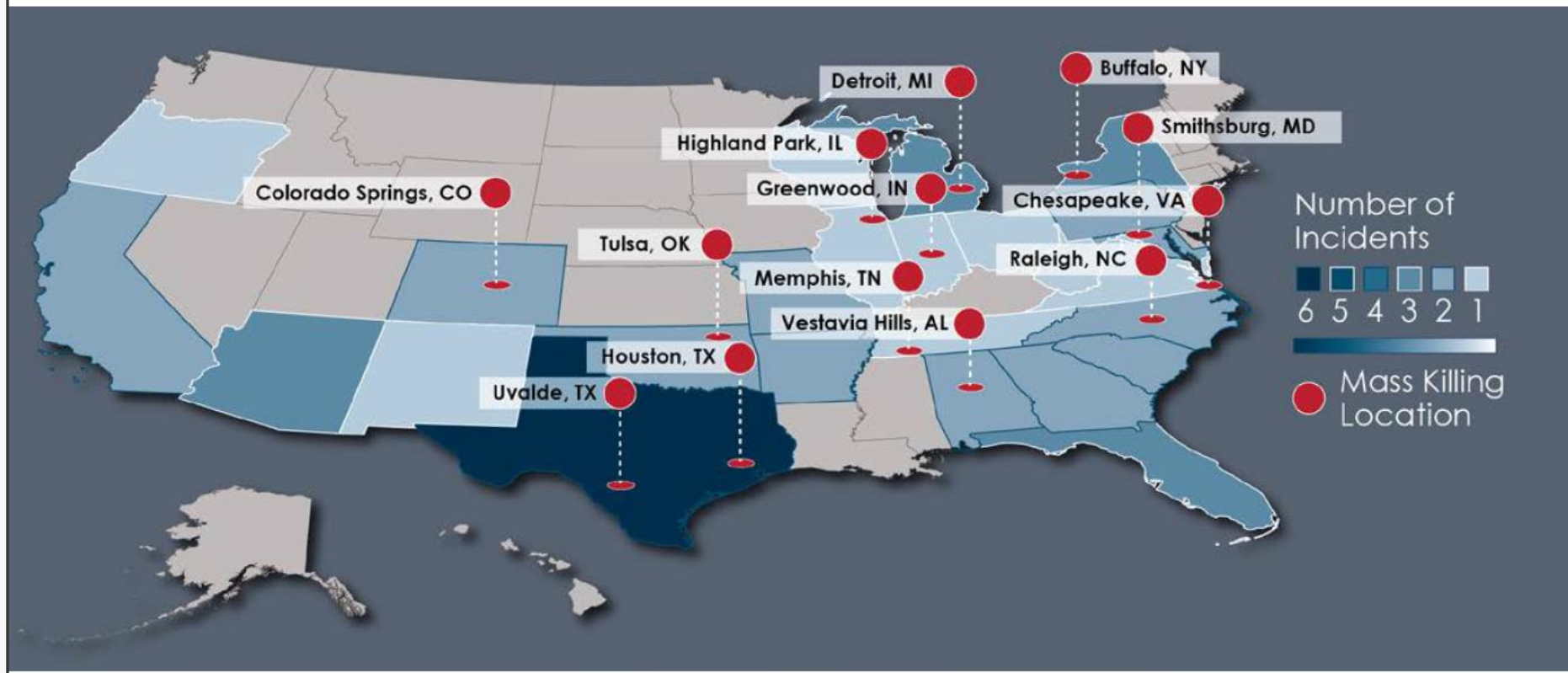
Fourteen³⁸ of the 50 incidents occurred in areas of **commerce**, resulting in 32 killed (including 10 employees) and 60 wounded (including 12 employees and three law enforcement officers).

Twelve incidents occurred in **commerce** environments **open to pedestrian traffic**, resulting in 28 killed (including six employees and one security officer). Fifty-seven were wounded (including 10 employees, two law enforcement officers, and one security officer).



Active Shooter Incidents – Geographic Locations (2022)

2022 Active Shooter Incidents by Location, Including Mass Killings



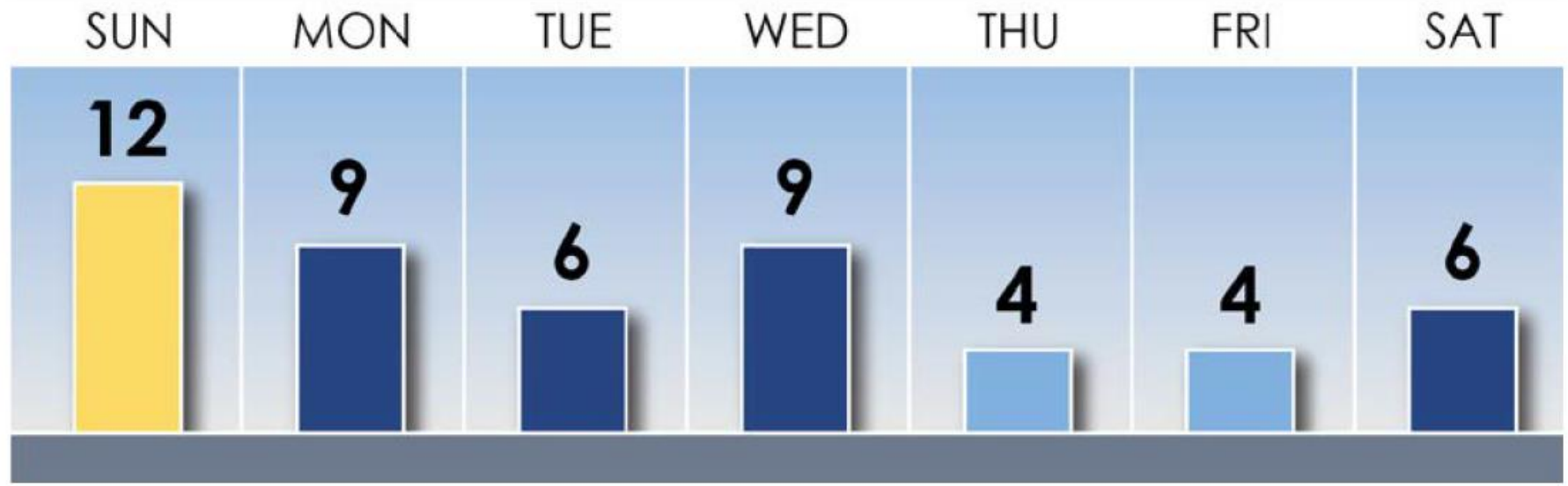
Active Shooter Incidents – Highest Casualties (2022)

2022 Active Shooter Locations with Five Highest Casualty Counts



Active Shooter Incidents – Day of the Week (2022)

2022 Active Shooter Incidents by Day of the Week



FBI Report. *Active Shooter Incidents in the United States in 2022 (Apr 2023)*

USSS Mass Attacks in Public Spaces (2016 - 2020)

| COMPONENTS TO MOTIVE* | 2016 | 2017 | 2018 | 2019 | 2020 | TOTAL |
|---|------|------|------|------|------|-------|
| Grievances | 40% | 50% | 68% | 35% | 60% | 51% |
| <i>Personal</i> | 5 | 9 | 11 | 8 | 13 | 46 |
| <i>Domestic</i> | 6 | 6 | 8 | 1 | 8 | 29 |
| <i>Workplace</i> | 2 | 6 | 3 | 4 | 3 | 18 |
| Ideological, bias-related, or political beliefs | 30% | 24% | 10% | 21% | 10% | 18% |
| Psychotic symptoms | 13% | 26% | 10% | 15% | 8% | 14% |
| Desire to kill | 13% | 8% | 3% | 9% | 3% | 7% |
| Fame or notoriety | 7% | 8% | 3% | 6% | 5% | 6% |
| Other | 3% | 3% | 10% | 9% | 8% | 6% |
| Undetermined | 20% | 8% | 10% | 29% | 23% | 18% |

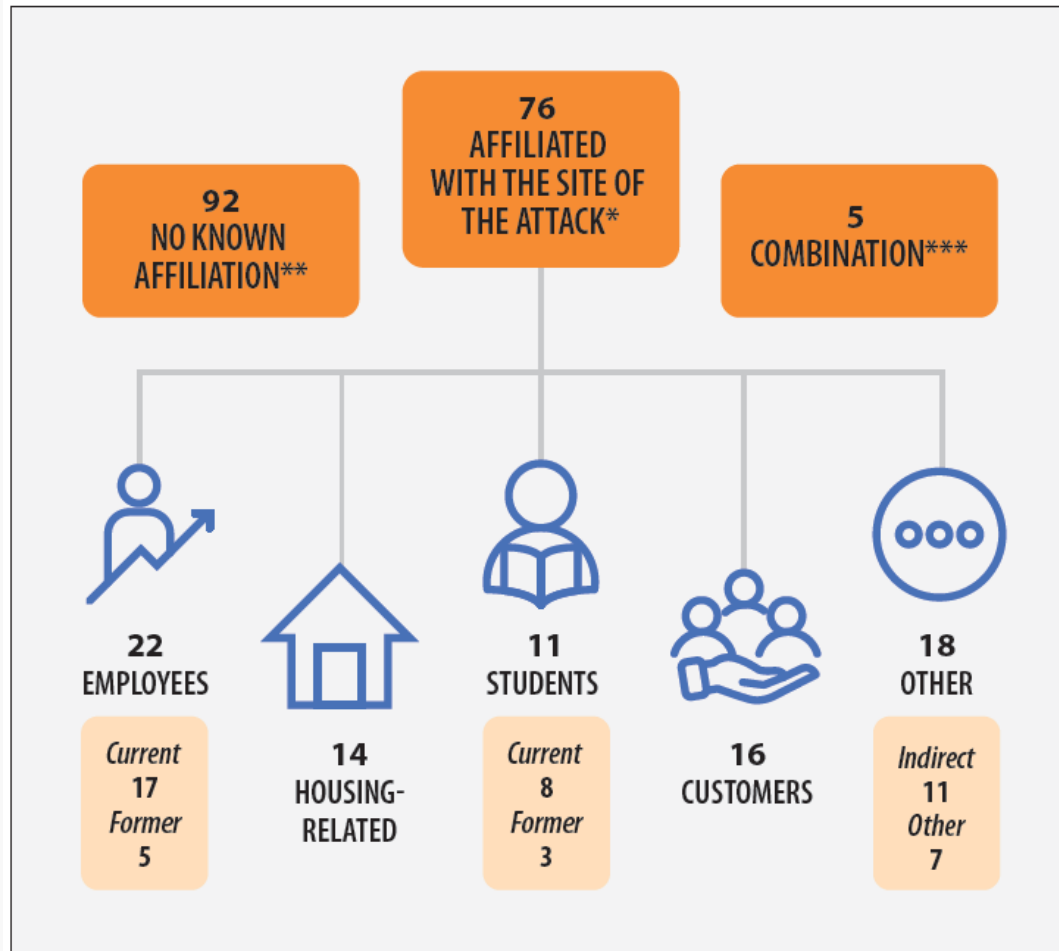
USSS National Threat Assessment Center Mass Attacks in Public Spaces: 2016-2020

[Mass Attacks in Public Spaces: 2016 - 2020](#)



USSS Mass Attacks in Public Spaces (2016 - 2020)

- Total of 173
 - 92
No Known Affiliation
 - 76
Affiliated w/Site
 - 5
Combination of the two



USSS National Threat Assessment Center Mass Attacks in Public Spaces: 2016-2020
[Mass Attacks in Public Spaces: 2016 - 2020](#)

FEMA Nonprofit Security Grant Program

- Notice of Funding Opportunity (NOFO) - 27 Feb 2023
- Deadline to Ohio EMA = 13 Apr 2023
- Max = \$150,000

FEMA Grants

- Preparedness Grants
 - Nonprofit Security Grant Program**
 - How to Apply
 - About Preparedness Grants
 - Assistance to Firefighters Grants Program
 - Emergency Management Performance Grant
 - Homeland Security Grant Program
 - Tribal Homeland Security Grant Program
 - Emergency Operations Center Grant Program
 - Intercity Bus Security Grant Program
 - Intercity Passenger Rail
 - Port Security Grant Program
 - Presidential Residence Protection Assistance

Nonprofit Security Grant Program

[Webinars](#)[Funding Totals](#)[NOFOs & Documents](#)

This grant provides funding support for target hardening and other physical security enhancements and activities to nonprofit organizations that are at high risk of terrorist attack. The intent is to integrate nonprofit preparedness activities with broader state and local preparedness efforts. It is also designed to promote coordination and collaboration in emergency preparedness activities among public and private community representatives, as well as state and local government agencies.

Resources



Preparedness Grants Manual
Recipients seeking guidance on policies and procedures for managing preparedness grants should reference this manual for program-specific information as well as overall guidance on rules and regulations.



How to Apply
Follow the [step-by-step process for applying](#) with tips in each stage.



Sign Up for Emails
If you would like more information about NSGP or to be added to an electronic mailing list for future webinars/technical assistance, [you may sign up](#) by providing your contact information.



<https://www.fema.gov/grants/preparedness/nonprofit-security>

Presenter's Name
September 11, 2023

State of Ohio Security Grant (OSG)

- Notice of Funding Opportunity (NOFO) - 14 Sep 2022
- Deadline to Ohio EMA = 12:00 PM; 4 Nov 2022
- Max = \$100,000

State of Ohio Security Grant (OSG)

Overview

House Bill 110 of the 134th General Assembly and House Bill 338 authorize the Department of Public Safety and Ohio Emergency Management Agency to provide grant funding to nonprofit organizations, houses of worship, chartered nonpublic schools, and licensed preschools for eligible security improvements that assist the organization in preventing, preparing for, or responding to acts of terrorism.

The SFY23 Ohio Security Grant (OSG) application period is now OPEN.

Applications are due no later than noon on November 4, 2022.

SFY23 OSG Application Documents:

- [Notice of Funding Opportunity](#)
- [Funding Application Instructions & Checklist](#)
- [Investment Justification Form](#)
- [Authorized Representative Signature Page](#)

Please send questions regarding this grant program to OSG@dps.ohio.gov

SFY23 OSG Application Information Webinars:

- 10:00am, Monday, September 19, 2022 - [Click here to join the meeting](#)
- 10:00am, Wednesday, October 19, 2022 - [Click here to join the meeting](#)

Participation is **not** mandatory and no registration is required. If you have any questions about the application process, please send your questions to OSG@dps.ohio.gov in advance of the webinar.



https://ema.ohio.gov/PreparednessGrants_OSG.aspx

Presenter's Name
September 11, 2023