SECURITY PLANNING WORKBOOK

SEPTEMBER 2023

SECURITY PLANNING WORKBOOK

OVERVIEW

The workbook can be used by individuals involved with your organization's security planning efforts; security expertise is not required to complete this workbook. This document can be used by anyone affiliated with your organization, including individuals or groups with varying degrees of security expertise, charged with the safety and security of your facilities and people. The purpose of this security planning workbook is to compile key information that can be used to assist you with building a comprehensive security plan. The process of creating a security plan should not be rushed. The information entered in the workbook can be saved; users should work at their own pace.

CISA's MISSION

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

While some sections and fields within this workbook may not apply to your unique site, every organization should develop and implement a comprehensive security approach to protect its people, property, visitors, and customers. The workbook is flexible and scalable to suit any type of business or organization. The workbook also provides descriptions of critical elements of security planning information, resources, and fillable fields to guide your efforts. As information in this workbook is filled out, your document should be securely saved and stored; follow your organizations information handling requirements.

ORGANIZATION/BUSINESS INFORMATION

Organization/ Business Name:

Address:

State: **Zip Code:**

Phone:

Website:

Description of Organization, Purpose, or Activities:

TABLE OF CONTENTS

1. Forming a Planning Team 4

Security Coordinator Information, Security Planning Team Information 4
Safety Team Information 6
Other Key Contact Information 7

2. Risk Assessment Process 10

Calculating Risk 10
A. Conduct "As-Is Review" 11
B. Evaluate Threats and Hazards 21
C. Assess Your Vulnerability(ies) 23
D. Assess Risk and Prioritize Mitigation 24
Notional Risk Table 26

3. Mitigation Considerations 27

4. Additional Elements of Your Security Plan 29

Training and Exercises 29
Communications 30
Recovery 32

5. Finalizing Your Plan 33

6. Supplemental Planning Options 35

Natural Disaster Contingency Planning 36
Emergency Preparedness 37
Emergency Action Plan (EAP) 38
Business Continuity Planning (BCP) 39
Community Resilience 39

8. Resources 41

1. FORMING A PLANNING TEAM

The Security Coordinator, Security Planning Team, and Safety Team

Establish clears roles, responsibilities, and expectations for those involved with your security planning team. Your team could be composed of a designated Security Coordinator along with Security Planning Team members who will develop plans and implement the identified security practices. Smaller organizations with limited personnel and resources may have a single person responsible for developing the organization's security plan(s). The process and considerations offered in this workbook can be used by organizations of all sizes.

Security Coordinator Information

The Security Coordinator will be the leader of the security planning team responsible for security-related questions. Ideally, the Security Coordinator is a full-or part-time staff member or engaged volunteer. Larger organizations may have a Chief Security Officer (CSO) responsible for these functions. The Security Coordinator is typically responsible for:

- Directing all security operations for all aspects of the organization's safety and security
- Developing and implementing security policies and practices, and evaluating their effectiveness
- Coordinate security decisions with senior leadership
- Reviewing current safety training to recommend updates and improvements

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Security Planning Team Information

The Security Planning Team supports the Security Coordinator by conducting research, evaluating needs, providing recommendations, and assisting with plan development. This should be a diverse group of delegates from within the organization representing all functional, accessibility, and business operational needs. Individuals with knowledge and expertise in security, law enforcement, facility operations and maintenance, mental health, emergency preparedness, incident management, public relations, special needs, childcare, and functional access can bolster your efforts and help build formal partnerships. Other valuable skill sets include policy development, strategic planning, finance and accounting, and training. The Security Planning Team can serve a variety of purposes and should help carry the burden of planning and implementation. Larger organizations with staff aligned to a CSO – or similar function – should coordinate across the organization to understand the unique security risks and planning needs of each group. Smaller organizations with limited personnel and resources, for example, may have a single person responsible for developing the organization's security plan(s). In this case, it becomes even more critical for smaller organizations to reach out to local law enforcement and emergency managers to solicit planning input and coordination

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Additional Security Planning Team Information:

Aim to create an environment that is welcoming and secure.

Safety Team Information

All organizations and businesses should account for the safety and security considerations of the wider range of people that may be impacted by an incident of any kind, such as patrons, customers, volunteers, and maintenance staff. For smaller community-oriented organizations like Faith-Based Organizations (FBO) and Houses of Worship (HoW), some members of this group can constitute a larger Safety Team to help carry out the safety and security program. The Security Planning Team or your organization's primary security planner will determine the activities of your Safety Team during security incidents. Smaller organizations with limited personnel and resources may require individual(s) to be dual-hatted as Security Coordinator, Planner, and member of Safety Team. Members of the Safety Team can include anyone with relevant skills, such as nurses and electricians.

Consider the needs of the organization and what skills may be the most beneficial. Are there any personnel trained in basic first aid, occupational safety and health, cybersecurity, weather emergency response, or any other relevant skills? Safety Team members may be required to treat wounds, seal doorways, operate a power generator, guide staff and customers to a designated assembly point, etc.

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Title:		**First & Last Name:**	
Phone:		**Alternate Phone:**	
Email:			

Additional Safety Team Information:

Other Key Contact Information

Local Law Enforcement Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Local Emergency Manager Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Local Fire Department Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Local Emergency Medical Services Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Hospital Information (Primary or nearest hospital)

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Alternate Hospital Information (For mass casualty events or with a relevant offering like a burn unit or Level 1-4 trauma center.)

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

CISA Protective Security Advisor (PSA)

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

CISA Cybersecurity Advisor (CSA)

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Poison Control Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Other Key Contact Information

Insurance Company Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Insurance Agent Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Contract Security Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Neighbor Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

Additional Neighbor Information

Name:					
Address:				**County:**	
City:		**State:**		**Zip Code:**	
Email:		**Phone:**		**Alternate Phone:**	

2. RISK ASSESSMENT PROCESS

Risk assessment is a process that allows organizations to identify potential threats and hazards and analyze their impact. This process involves interviewing personnel and stakeholders, performing on-site inspections, and examining public records like local crime statistics. Risk assessments have an element of subjectivity as willingness to accept or interpret risk will differ for each organization.

CALCULATING RISK

RISK = THREAT × VULNERABILITY × CONSEQUENCE

The Department of Homeland Security Risk Lexicon frames risk as a function of **Risk = Threat × Vulnerability × Consequence**. The DHS Risk Lexicon specifically defines these terms as follows:

THREATS AND HAZARDS: Man-made (threats) or natural (hazards) occurrence, individual, entity, or action that has or indicates the capability or intent to harm life, information, operations, the environment, and/or property.

VULNERABILITY: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

RISK: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.
Risk is a function of threat, vulnerability, and consequence.

CONSEQUENCE: Effect of an event, incident, or occurrence. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.

USING THE RISK ASSESSMENT PROCESS

By evaluating the combined threats/hazards, vulnerabilities, and consequences, organizations can identify risk. The table at right shows an example of these elements:

Risk Element	Example
Threat/Hazard →	Active shooter
Vulnerability →	Broken lock on door to facility
Consequence →	Damage to facility and/or people are harmed
Risk →	Low probability, high impact event

A CONDUCT "AS IS" REVIEW

Identify your significant assets and their value, which could include:

- Security policies, procedures, protocols, operations
- Employees, members, staff, customers, volunteers
- Physical security technology and equipment

B EVALUATE THREATS & HAZARDS

Consider the impact from:

- Man-made threats / natural hazards
- Facility location and social environment (e.g., demographics, crime rates, etc.)
- Ideological or identity-based threats
- Cyber incidents

C ASSESS YOUR VULNERABILITY(IES)

Determine vulnerabilities to your assets:

- What threats/hazards has your organization experienced in the past?
- How does your organization's location and proximity to threats/hazards impact your security?
- Verify that available security/safety assets are in working order.

D ASSESS RISK AND PRIORITIZE MITIGATION

- Estimate likelihood of threat/hazard to occur (e.g. probability)
- Consider cost/consequence of loss, damage, or harm
- Determine most critical risk(s)
- Establish risk tolerance
- Identify initial risk solution(s) / methods to mitigate risk(s)

A CONDUCT "AS-IS REVIEW"

This step begins with conducting an "as-is review" of the enterprise to document information about the facility, property, personnel, staff, volunteers, contractors, community, valuable assets, and other information about the organization's branding, reputation, and credibility.

Facility Identification and Description:

- Identify each building on your property, such as the main building, visitor center, administrative building, school, playground, community center, and parking.

- Describe the number, physical design, and construction of buildings, including year and type of construction, and geographic footprint.

- Define the type and number of events or activities held, as well as the schedule and number of individuals who might be present in each building at any given time. Be sure to address whether crowds gather inside, outside, or both.

- List any distinguishing features that might help identify the organization's property, especially for first responders including door numbers, vehicle entrance locations, facility maps and floor plans.

A CONDUCT "AS-IS REVIEW"

Identify elements of your outer, middle and inner perimeter.

Security-in-depth (also referred to as **layered security**) is an industry-accepted concept in asset protection. This approach helps to slow or dissuade potential criminals from gaining unauthorized access to your facility. The security "**layers**" of your facility can be further described as your outer, middle, and inner perimeters.

Outer perimeter area: could include the parking facility and lots, exterior common grounds, walkways, playgrounds, and a fence line or gate at the outer edge of your property

Middle perimeter area: a fluid area that generally includes anything that is "on campus" but outside of the main buildings (could include but not limited to exterior features such as walkways, doors, walls, and power generators).

Inner perimeter area: includes anything that is inside the facility or facilities on your property. Could include lobby, offices, seating balcony, worship area(s), community room(s), auditorium, classrooms; as well as, secure spaces such as offices, server rooms, file rooms, and building systems.

A CONDUCT "AS-IS REVIEW"

Identify Additional Security Assets and their Functions

Identify your electronic security systems, CCTV systems, intrusion detection / alarm systems.

Identify exterior lighting (type and location).

Identify mechanisms for systems used to control access to your facility such as locks and key cards.

Identify how your facility enables access for those with access and functional needs.

Describe how emergency responders would gain access to your facility.

Identify any paid and unpaid security staff, along with their responsibilities.

A CONDUCT "AS-IS REVIEW"

Evaluation of Significant Areas and Assets

Evaluate Significant Areas and Assets that Require Protection and their Potential Replacement Costs.

Assets are both tangible — like people, property, and things — and intangible — like reputation and sense of well-being. Consider consulting an insurance adjuster or other assessor to determine the actual replacement cost for all assets, which can be evaluated as simply "high," "moderate," or "low." Also consider the challenges of replacing key personnel, re-establishing reputation, and mitigating other potential losses. CISA developed The Business Case for Security to guide organizations in understanding their security posture and understanding the costs associated with security.

Identify valuables, such as artwork and irreplaceable artifacts. Also identify sensitive and proprietary information, hazardous material, and weapons, if applicable.

IDENTIFY VALUABLES	COST ESTIMATE (high, moderate, or low)	$ VALUE

A CONDUCT "AS-IS REVIEW"

Review day-to-day operations, administrative procedures, cybersecurity safeguards, and physical security-related protocols:

- What are your practices around visitor access?
- What are your hours of operation for your patrons and staff?
- Note which spaces in which areas are routinely kept locked, as well as those routinely unlocked? Should any locks be reassessed?
- Describe the protocol for greeting and screening visitors during events. How does this protocol differ during regular business hours?
- How do you assess compliance with your security policy and procedures? How often do you review and update them?
- Identify how first responders gain access to your facility during an emergency (such as - during a lockdown situation).

A CONDUCT "AS-IS REVIEW"

- Consider how to report incidents: Do people call an internal operations center or 9-1-1? What is the process for notifying facility occupants and first responders of an incident?

- Do you have recovery plans to return to normal operations after an incident? Identify written plans or describe short- and long-term recovery procedures here.

- Identify your documented administrative processes, procedures, policies, directives, and operational manuals. Where are these administrative documents stored? When were your organization's policies last updated?

Review day-to-day operations, administrative procedures, cybersecurity safeguards, and physical security-related protocols:

A CONDUCT "AS-IS REVIEW"

Evaluate human resources practices:

- Does your organization use contract security personnel, either armed or unarmed, to support standard activities and events? Are security personnel aware of and trained to mitigate the threats to the organization and the surrounding community?

- Do you have formalized relationships and partnerships with local law enforcement and/or first responders who have authority in your jurisdiction? Do you meet with them regularly to exchange information and collaborate around security and risk mitigation priorities? Do they have floor plan information and building keys on hand for all buildings on your campus? Do local law enforcement have an ability to remotely activate any on-site Closed-Circuit-Television (CCTV) technology in the event of an armed or hostage-taking incident?

A CONDUCT "AS-IS REVIEW"

- What pre-employment screening protocols do you follow? Are employees and volunteers subject to background investigations? How often are employees rescreened or reinvestigated?

- How does your organization receive reports of concerning employee behavior or insider threat information?

Evaluate human resources practices.

A CONDUCT "AS-IS REVIEW"

People and Organizational Culture;

Consider your organization's attitude toward security procedures:

- What potential security threats have your employees expressed concern about?

- How do organizational values and initiatives, such as supporting vulnerable populations and providing food, shelter, and social support in the community, increase possible security vulnerabilities?

- What is your organizations process for recognizing, reporting, adjudicating, and sharing reports of concerning behavior and/or suspicious activity?

- How does your organization's leader(s) regularly communicate with staff about security and safety?

A CONDUCT "AS-IS REVIEW"

- List security and emergency preparedness training you have conducted. Include the date, audience, and a brief description.

- Do you have a public relations manager to control communication with media during an event?

- What future security enhancements are planned as part of the organization's overall security strategy?

People and Organizational Culture

B EVALUATE THREATS AND HAZARDS

The Security Planning Team or individual planner should document the threats (man-made) and hazards (natural) that the organization/business and surrounding community previously encountered or may encounter in the future. Work with CISA PSAs (Protective Security Advisors) and CSAs (Cybersecurity Advisors), local law enforcement, your local emergency management agency, or other non-profits to obtain a relevant assessment detailing the potential threats and hazards to your organization.

THREATS AND HAZARDS: man-made (threats) or natural (hazards) occurrences, persons, entities, or actions that have or indicate the capability or intent to harm life, information, operations, the environment, and/or property.

Consider the threats and hazards to your organization to better understand how your organization may be harmed.

- What man-made or external threats could hurt your organization, facility, staff, and/or customers?

  This could include:
  - Cyberattacks, such as ransomware, malware, phishing, or network intrusions
  - Physical attacks such as an active shooter or active assailant, vehicle ramming, drone incursion, arson, improvised incendiary devices (IID), improvised explosive devices (IED), or insider threat; and
  - Hybrid attacks where a cyberattack results in a physical outcome like an inability to operate or industrial control system failure.

- What natural hazards could impact your organization's ability to operate? This could include: Floods, wildfires, tornadoes, hurricanes, and other natural hazards specific to your area or location.

- Who could cause harm to your facility, personnel, customers, or volunteers? This could include: A disgruntled former or current employee, an ideologically motivated attacker, a volatile domestic partner, a dissatisfied customer, or criminal.

B EVALUATE THREATS AND HAZARDS

- Consider factors such as your organization's public profile and visibility in the community and region. For example, understand whether ideological, social, or political opinions or beliefs linked to the organization and its leaders could incur a high level of attention and risk.

- Threat is a function of intent, capability and opportunity. Evaluate the probability of occurrence of each threat you identified above. Consider factors such as the historic frequency of such threats in your neighborhood and environments similar to yours.

- Consider how location and proximity might influence your threat environment. For example, degree of risk may increase if an organization is located near another group that is regularly the focus of public attention or targeted for violence or vandalism.

Consider reviewing the following resources to discover more about threat/hazards local to you:

- State Fusion Centers
- DHS Center for Prevention Programs and Partnerships (CP3)
- NCTC Joint Counterterrorism Assessment Team (JCAT)

C ASSESS YOUR VULNERABILITY(IES)

A vulnerability assessment is an analysis performed to determine security countermeasures necessary to mitigate specific threats to personnel, facilities and/or events. Your findings can inform security decisions and help prioritize security actions by looking at feasibility, complexity, expected benefits, cost, and resource availability. Vulnerability assessments should collect data and information through interviews with key personnel and stakeholders, perform on-site inspections and observations, review relevant policies and procedures, and examine public records such as local crime statistics.

VULNERABILITY:
a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

The most important aspect of a vulnerability assessment is documenting your process and findings so the data can help develop a security strategy. The assessment should be revised regularly.

Have you conducted a vulnerability assessment in the past?

If so, has it been updated recently? Date, if available:

State or local law enforcement, a PSA, or other consultants can conduct a vulnerability assessment or provide additional guidance on how to conduct a self-assessment. CISA offers several free vulnerability assessment tools, services, and resources:

PSAs can conduct Vulnerability Assessments

- Security Assessment at First Entry (SAFE)
- Infrastructure Survey Tool (IST)
- Houses of Worship Security Self-Assessment
- School Security Assessment Tool (SSAT)
- Vehicle Ramming Self-Assessment Tool

This **Security Self-Assessment Tool** is a useful resource even if your organization is not a House of Worship

While performing your vulnerability assessment, a key question to consider is - How likely are your people / processes / security systems to deter, detect, delay, or defend against a potential threat?

The field below can be used to enter your findings, outputs, and results of the vulnerability assessment:

D ASSESS RISK AND PRIORITIZE MITIGATION

The culmination of the risk assessment process is a consolidation of the information collected. The table below provides your organization with a consolidated, prioritized list of risks you face and shows how and where to boost investments to mitigate the consequences of an event. Use the prompts below to guide the process of assessing your organization's risk.

RISK: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Risk is a function of threat, vulnerability, and consequence.

CONSEQUENCE: The effect of an event, incident, or occurrence.

Ensure your risk assessment clearly identifies consequences associated with identified risks, which can include:

- Tangible losses, such as money, property, and valuables.
- Social, emotional, interpersonal, and psychological damages that may disrupt the organization's operations and business continuity.
- Impact to the organization's brand, credibility, or reputation among stakeholders and throughout the community.

Consider the threats and hazards previously identified and list each type of threat or risk. Every risk should be rated and ranked based on probability of occurrence and impact (e.g., low probability/high impact).

- What are the most likely threats to your organization?
  - Refer to the Identify Threats and Hazards section when completing the risk table below.
- Which vulnerabilities should be prioritized ahead of others?
  - Refer to your Vulnerability Assessment when considering this section in the risk table.
- What is the likelihood of any given threat to occur?
  - In the risk table below, consider using a range of likelihood: Very Unlikely, Unlikely, Neutral, Likely, Very Likely
- What are the consequences if such threats occur? Which threats / hazards present the greatest danger(s) to your organization?
- What is your organization's willingness to accept the associated consequences of each risk?
- What is your organization's attitude toward security practices?
- What personnel resources do you have to direct, manage, and oversee security operations?
- What is your budget to support security initiatives, both immediate and long-term?
  - Consider prioritizing security initiatives according to the identified likelihood.
- Consider your organization's risk tolerance by having candid discussions for each identified risk.

D ASSESS RISK AND PRIORITIZE MITIGATION

- Risk factors, tolerance, and mitigation views can change over time, especially with mitigations in place. Keep a flexible process for assessing risk within your organization, and ensure the Risk Table is reviewed on a regular basis by the Security Planning Team or primary planner.

Estimate the likelihood of a threat/hazard happening to your organization and weigh it against the estimated cost and impact if it were to occur. This information will factor into your risk calculation (see table on next page).

- Other more complex systems exist to determine the impact a threat can pose to your organization and facility. Rating risks and calculating your total risk scores, however, will assist you with prioritizing security planning strategy options regardless of the complexity of the chosen measurement system.

Use the following formula to fill in the ratings for **Threat**, **Vulnerability**, and **Consequence** (done below). Next, multiply these three numbers **(TxVxC)** to obtain the "**Total Risk Score**" for that particular risk. Use the table on the following page to capture each of your risk ratings and total risk score.

CALCULATING RISKS

T

THREAT: Rate the **severity** of threat incident (*scale 1-5*) with the **probability** or likelihood of the threat occurring (*scale 1-5*). Add these two numbers together (**Severity + Probability**) to get your Threat Rating (*scale 1-10*).

V

VULNERABILITY: A numerical score (*on a scale of 1-10, with 1 being the least vulnerable and 10 being the most vulnerable*) based on your determination of **how susceptible** your organization/facility is to the identified threat.

x C

CONSEQUENCE: Rate the **impact** the incident/event would have on your organization (*scale 1-10*). Consider monetary value (*see pg. 13 for additional information on **value***), importance of assets harmed in the incident, disruption of operations, and/or estimated recovery time.

TOTAL RISK SCORE

NOTIONAL RISK TABLE

Use the **Calculating Risks** graphic on the previous page and the worksheet below to assist with capturing and determining the level of risk(s) to your facility or organization. Use the **Risk Priority Level** to the right to determine if your risk score equates to a low, medium, or high priority. The risks which are rated as "High" would be the ones to consider mitigating first. **For additional information on risk mitigation, see** **Chapter 3 (Mitigation Considerations) beginning on the next page.**

RISK PRIORITY LEVEL

Once the **Total Risk Score** has been calculated, determine if the Total Risk Score should be prioritized as **Low**, **Medium**, or **High**.

1-60 = LOW	*61-175 = MEDIUM*	*176-Above = HIGH*

RISK NO.	BRIEF RISK DESCRIPTION	THREAT RATING (T)	VULNERABILITY RATING (V)	CONSEQUENCE RATING (C)	TOTAL RISK SCORE (T x V x C)	PRIORITY OF RISK (HIGH MEDIUM LOW)
Ex.	*Active Shooter Attack*	*6*	*6*	*7*	*252*	*HIGH*
		-	-	-		-
		-	-	-		-
		-	-	-		-
		-	-	-		-
		-	-	-		-
		-	-	-		-
		-	-	-		-
		-	-	-		-

3. MITIGATION CONSIDERATIONS

Now that your risk assessment is complete, organizations should look to bolster their security posture and implement methods to mitigate identified risk(s). Decisions to accept and mitigate risk are unique to each organization and should be based on the organization's goals, objectives, and available resources. Your goals and objectives are key to determining your priorities and the resources required to mitigate risk(s). Mitigation considerations can include training and exercising, building, or enhancing situational awareness, investing in physical security measures, and strengthening relationships and partnerships.

The information identified during your security risk-assessment and the information gathered during the planning process can inform your decisions to implement measures to mitigate risk, reduce or eliminate potential hazards, and protect your organization from potential existing or future threats.

Mitigation is the capability necessary to eliminate or reduce the loss of life and property damage by lessening the impact of an event or emergency.

Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide, November 2015

PHYSICAL SECURITY

Physical security mitigation may include:

- Installing bollards, barriers, fencing, or landscaping
- Implementing access control systems such as an employee key card system
- Protecting essential equipment from the elements

CYBERSECURITY

Cybersecurity mitigations options may include:

- Training employees to identify phishing emails
- Backing up and protecting data regularly
- Implementing multi-factor authentication
- Setting strong password requirements

Consider reviewing the following references for low or no cost mitigation options:

- CISA PSAs - Proactively engage with government partners and the private sector to protect critical infrastructure
- CISA Houses of Worship Security Self-Assessment Tool - The information in this resource can be applied by all organizations
- CISA Vehicle Ramming Self-Assessment Tool
- Low Cost/No Cost Immediately Implementable School Safety Tactics
- CISA School Security Assessment Tool (SSAT) - The information in this resource can be applied by all organizations
- Ready.gov - Provides additional insight into mitigation of natural disasters
- CISA Shields Up - Guidance for organizations on cybersecurity mitigations
- CISA Cyber Essentials - Develops an actionable understanding of how to implement organizational cybersecurity practices
- CISA Stop Ransomware - Tips and guidance to keep your network healthy

Consider applying for DHS and FEMA grants to address organizational resource requirements

To address the acquisition of resources to enhance your organization's physical security, for eligible organizations, consider exploring DHS and FEMA grant programs that can potentially assist with mitigation needs. DHS and FEMA provide grants that can be used for training, exercises, planning, personnel, and equipment to prepare for many threats and hazards.

- Preparedness (Non-Disaster) Grants: FEMA provides program funding in the form of non-disaster grants to enhance the capacity to prevent, respond to, and recover from various emergencies.
- FEMA Grants: FEMA provides grant funding to state, local, tribal, and territorial governments in the form of non-disaster grants.
- Continuing Training Grants: Offered through FEMA, the Homeland Security National Training Program (HSNTP) Continuing Training Grants (CTG) provides funding via cooperative agreements to partners to develop and deliver training to prepare communities to prevent, protect against, mitigate, respond to, and recover from acts of terrorism and natural, man-made, and technological hazards.

Organizations can search for additional preparedness grants through DHS.

More detailed information and specific free and low-cost resources for training, physical security, cybersecurity, and more are included in Chapter 4.

For additional resources, click here.

Enter information or the document location for **Mitigation Considerations** below**:**

4. ADDITIONAL ELEMENTS OF YOUR SECURITY PLAN

TRAINING AND EXERCISES

Creating and regularly practicing effective training and exercise programs builds proficiency and can help personnel understand what to expect in the event of an emergency. Training and exercises are critical components of security plans. Training should be completed for each planned incident or emergency event, such as natural disasters, active assailant incidents, and cyber-attacks. Training activities may take several forms, ranging from online learning to conducting a tabletop or full-scale exercise.

- Online-based learning should be integrated as part of the employee onboarding process and be completed at least annually.

- Exercises that help prepare for physical security incidents, such as active assailant training, should be conducted at least annually.

Practice, Practice, Practice. CISA conducts cyber and physical security exercises with organizations to evaluate readiness, as well as identify areas for improvement and lessons learned. These exercises can be tailored to accommodate organizations of all sizes with unique operating environments. CISA also offers Tabletop Exercise Packages designed to assist stakeholders in conducting their own exercises and to facilitate discussions internally to address a variety of threat scenarios.

Online training is available to stakeholders on Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) for a variety of threat vectors.

Some recommended DHS training includes the following:

- IS-906: Workplace Security Awareness
- IS-907: Active Shooter: What You Can Do
- IS-915: Protecting Critical Infrastructure Against Insider Threats
- Stop the Bleed | Homeland Security (dhs.gov)
- DHS Tactical Emergency Casualty Care Program

For additional resources, click here.

Enter information or the document location for **Training and Exercises** below:

COMMUNICATIONS

Organizations must be ready to respond promptly, accurately, and confidently during an emergency in the hours and days that follow, as they will need to reach many different audiences with information specific to their interests and needs. Emergency incidents can develop quickly, and effective communication with victims, staff and their families, customers, emergency responders, press, and other members of the community is essential to manage the situation. Security plans should account for communications both within (internal) and outside (external) the organization, as appropriate.

ELEMENTS OF SUCCESSFUL COMMUNICATION

The communications element of a plan should outline the specific roles individuals will have in responding to different emergency scenarios. Communication planning considerations could include:

- Method to communicate the initial notification of an emergency
- Method to provide updates to personnel
- Guidance on messaging the public when incidents occur

INITIAL NOTIFICATION OF AN EMERGENCY

Organizations must be able to quickly identify who to contact when an emergency occurs. For most emergencies, contacting 9-1-1 may be the most appropriate response; everyone should have the ability to do this. In some emergencies, there may be a need to contact additional specific individuals. For example:

- In the event of an active assailant incident, after 9-1-1 has been contacted, notifying your organization's leadership or security staff may be appropriate because they might oversee communications with emergency responders and account for injured and missing personnel.
- Prior to a hurricane or significant weather event, you may notify your organization's leadership, security staff or other designated team member(s) to enable effective communication and preparedness.

Enter information or the document location for **Initial Notification of an Emergency** below**:**

METHODS FOR PERSONNEL UPDATES

The goal for effective communications should describe how organizational personnel will maintain internal and external communications before, during, and after an emergency incident.

- Organizations may rely on an internal communications system or may use organizational or personal cell phone numbers to communicate with personnel.
- Organizations should consider how emergency communications will be sent to external staff, members, and others (e.g. vendors, remote employees, etc.)
- Organizations should be able to provide emergency alerts, real-time updates, and follow-up notifications that are relevant to the specific emergency event to enable informed decisions. If an organization relies on a web-based application or other internet-based system to communicate with personnel, consider developing a back-up plan in case access to systems is unavailable
- If your organization uses a mass notification system or application, consider coordinating with local law enforcement or emergency response officials to identify suitable solutions.

Enter information or the document location for **Personnel Updates** below**:**

GUIDANCE ON PUBLIC MESSAGING

Communication planning should consider how to provide updates to the public. In larger organizations, public messages may need to be coordinated with several internal teams before being published and should outline the approval processes. Messages should be tailored to the specific event. For example:

- Communications with the community should include initial notification of the incident and be coordinated with public safety.
- Communications with the public could address service disruptions and restoral timelines.
- Communications with the media or law enforcement should be assigned to a designated group or individual within your organization to ensure clarity and consistency of message, as well as deconflict information prior to public release.

Ready.gov outlines additional guidance for creating and implementing communication elements into Emergency Action Plans (EAPs).

For additional resources, click here.

Enter information or the document location for **Guidance on Public Messaging** below**:**

RECOVERY

Recovery requires focused preparation and planning to meet the recovery needs of those impacted by an event. This preparation and planning, sets the foundation for successful recovery. Each EAP should address short-term and long-term recovery efforts and they should be tailored to the incident.

The goals in **short-term recovery** are to re-establish safety and mitigate the physical, psychological, and emotional impacts from the incident. **Long-term recovery** goals should help those impacted resume operations and return to a sense of normality in their daily interactions and professional life. The aim is to address both the immediate care of impacted personnel and return to full operations.

SHORT-TERM

Address Immediate Concerns

- Tend to health and safety
- Enable immediate crisis support
- Establish reunification with families, communities
- Establish a hotline and crisis communication
- Work with law enforcement
- Support funerals and vigils
- Work on 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

The psychological and emotional impact from an incident is different for each affected individual. Some may require limited support, while others may need much more. Organizations should identify local resources available to support recovery and establish relationships with providers well in advance of an event. Refer to the resources to assist with your recovery planning efforts:

- CISA Active Shooter Recovery Guide – Active Shooter Preparedness
- DOJ's Office for Victims of Crime; Helping Victims of Mass Violence and Terrorism – Planning, Response, Recovery, and Resources
- "I Love U Guys" Foundation – Standard Reunification Method
- Ready.gov Business Continuity Plan

There is no set timeline for short and long-term recovery efforts, and actions will depend on each unique situation. Short and long-term recovery efforts may look different for each threat vector and should be incorporated into EAPs accordingly.

For additional resources, click here.

Enter information or the document location for **Short-term and Long-term Recovery** below**:**

5. FINALIZING YOUR PLAN

DRAFTING THE PLAN

Now that you have compiled the key elements necessary for developing a security plan, you are ready to write your plan, draft it, review it, obtain approval from organizational leadership, and finally publish your security plan. Federal Emergency Management Agency's (FEMA) Comprehensive Planning Guides provide additional guidance to assist with finalizing your plan.

Keep the following in mind when drafting your plan:

- Use simple language and short sentences in active voice.
- Summarize important information with checklists and visual aids (maps and flow charts).
- Avoid using jargon and minimize the use of acronyms.
- Give enough detail to ensure your plan is easily understandable and actionable.
- Format the plan and organize its contents so readers can quickly find solutions and options.
- Focus on providing mission guidance (e.g., insight into intent and vision, rather than discussing policy and regulations).
- The plan should be reviewed for compliance with regulatory standards (e.g., Industry, Local, State, and Federal etc.), including Americans with Disabilities Act (ADA) mandates.
- The Security Planning Team or primary planner should consult with leadership to determine the review cycle for the plan.
- Ensure accessibility by developing alternate formats (e.g., print, electronic, video).

VALIDATE THE PLAN AND PREPARE FOR APPROVAL

Once your security plan has been drafted, re-confirm the plan supports your organization's goals and objectives which have been identified earlier in the planning process. Consider having key members of your organization review the draft plan to ensure the plan is adequate, feasible, acceptable, and complete.

Revisions are common in the process to finalizing your plan. Feedback from key stakeholders will ultimately strengthen your security plan.

APPROVE AND DISSEMINATE THE PLAN

Now that the plan has been validated, the planning team or primary planner should present it to the senior official(s) and obtain approval of the plan. Once the plan has been approved, distribute it to applicable members of your organization. Consider holding an organizational meeting during which members can ask questions or seek clarification to confirm that the plan is known and understood.

After your plan is approved and disseminated, organizations should train their personnel to ensure they have the necessary knowledge, are proficient with the required skills, and capable of performing the tasks identified in the plan. Training can be accomplished through a variety of ways, including new employee orientation, "All Hands" meetings, conferences, workshops, newsletters and internal broadcasts, and online courses. For additional information on training and exercises, see Chapter 4 *Additional Elements of Your Security Plan*.

REVIEW THE PLAN

Planning teams or an organization's primary planner should establish a process to review and revise the plan on a recurring basis. Plans should be reviewed and updated after the following events:

- A major incident
- Changes in organizational resources (e.g., key personnel, organizational structure, management processes, facilities, equipment)
- A formal update of planning guidance, policies, management processes, or standards
- Changes to the threat environment
- Significant improvements to your organizations' security and safety elements, including improvement or changes to items such as facilities and equipment
- Incorporating feedback from exercise after action reviews

Enter information for **Finalizing Your Plan** below**:**

6. SUPPLEMENTAL PLANNING OPTIONS

This section offers resources, products, and practical knowledge to inform the development of certain functional security plans. Users are encouraged to build their plans and store them in a location where those with a need to know can access the plans. Each section provides an overview of the topic, options for consideration when building the plan, and additional resources for further learning. The following pages will address the following topics:

- Additional Cybersecurity Planning Considerations
- Natural Disaster Contingency Planning
- Emergency Preparedness
- Emergency Action Plan
- Business Continuity Plan
- Community Resilience

Additional Cybersecurity Planning Considerations

Use a comprehensive approach to reduce your organization's cyber risk exposure. Cyber threats can harm an organization's operations, proprietary and sensitive information, reputation, intellectual property, and — especially — its personnel. Employees are the first line of defense against social engineering cyber tactics, and they must have the skills to maintain their guard against cybersecurity risks. Use basic cybersecurity training to broaden exposure to cybersecurity concepts and terminology.

Develop a secondary data repository or cloud resources to ensure all data is backed up and accessible in the event of an incident. Implementing this step before a breach will significantly help to reduce or eliminate any downtime during an emergency and allow for better business continuity. Alternative data backup options can be found in CISA's Data Backup Options resources.

Ensure only those who belong to an organization have access to its network and digital infrastructure. Supervisors should approve access privileges only as employee duties require and control employee access as the workforce evolves. IT teams should maintain inventories of hardware and software assets to know what is in use and at-risk for attack. Consider employing Identity Access Management (IAM) as legal parameters permit.

To learn more about CISA cyber preparedness resources, visit Shields Up.

For additional resources, click here.

Enter additional information or the document location for your organization's **Cybersecurity Plans** below:

Natural Disaster Contingency Planning

Having a contingency plan for natural disasters involves personnel safety, communication, business continuity, and can also include recovery of systems, networks, and data. Ensure all staff are familiar with how to prepare for natural disaster events, such as hurricanes, tornadoes, and flooding.

Your security plan should include or address the following elements:

- Communication - Account for the safety of all personnel, both as the weather event approaches, and after it passes.
- Data Backup - Ensure data is backed up and systems are tested on a regular schedule.
- Power - Ensure emergency generators and back-up batteries are available during power outages.
- Recovery - After the natural disaster has ended, have a plan to determine losses and assess damage.

FEMA's mobile app provides alerts in real-time from the National Weather Service, and the Emergency Alert System and Wireless Emergency Alert automatically provide severe weather updates without a required sign up.

For more information, refer to the following resources:

- Ready.gov IT Disaster Recovery Plan
- Ready.gov Hurricane Page
- FEMA Protecting Business Operations Second Report on Costs and Benefits of Natural Hazard Mitigation

For additional resources, click here.

Enter information or the document location for **Natural Disaster Contingency Planning** below**:**

Emergency Preparedness

Preparing and planning for emergency incidents will help significantly in mitigating their potential impacts on employees and facilities. Before creating an Emergency Action Plan (EAP) and Business Continuity Plan (BCP), organizations need to understand the threat landscape and know what kind of disasters and emergencies are most relevant to their unique environment. It is important for organizations to have a practical crisis communications plan so that all individuals within the organizations should contact their state/territory Office of Emergency Management to learn more about resources available to support your emergency preparedness planning efforts. Train employees to understand what they should do in the event of an emergency. CISA offers an Active Shooter Emergency Action Plan template, guide, and video to help users get started. Additionally, FEMA offers a Basic Preparedness Guide to assist organizations and individuals with emergency preparedness planning.

Organizations should prepare basic emergency supply kits. These supplies can help organizations treat minor injuries and continue operating at a baseline level of operations.

Some basic supplies include:

Battery-powered radio	Extra batteries	Flashlights
First aid kit	Dust masks	Plastic sheeting
Duct tape and scissors	Garbage bags	Local maps
Emergency phone with charger	Blankets	Over the counter medication (i.e. pain relievers, etc.)
Water	Copies of important documentation	Fire extinguishers
Generator	Gasoline	Bleach

Emergency supply kits should be stored in cool, dry places that can be easily accessed. Check supplies regularly for expiration and replace as needed. Ready.gov offers guidance on building an emergency supply kit. Ready.gov also offers extensive resources for emergency preparedness, including no cost preparedness strategies.

For additional resources, click here.

Enter information or the document location for **Emergency Preparedness** below**:**

Emergency Action Plan (EAP)

An EAP is a detailed plan designed to enhance an organizations' ability to respond to and recover from a specific incident or crisis event. Organizations should consider developing an individual EAP for each of the threats or hazards they have determined they are most likely to face. EAPs can help ensure personnel are familiar with required actions to take during each type of emergency. Without an EAP, an organization may struggle with responding to an emergency which may result in a disorganized response, miscommunication, frustration amongst your members, families or customers and possibly additional loss of life.

Examples of specific emergency situations EAPs can address include but are not limited to active shooter incidents, vehicle ramming attacks, bomb threats, hazardous material events (HAZMAT), weather incidents, and incidents of fire and arson.

When developing an EAP, consider addressing:

A designated assembly point or points	A detailed list of emergency supplies and their location
Shelter-in-place guidance	Emergency communications
Emergency evacuation routes	Contact information for emergency responders

As you develop your EAP, refer to your risk assessment (see Chapter 2 Risk Assessment Process) to understand what risks your organization may face and the impacts each risk could have on your organization, should it occur. Ready.gov provides resources and information on conducting a risk assessment. Understanding the most prominent threats facing your organization will enable you to determine resource requirements needed to prepare and protect your organization.

Organizations should also consider including staff in the development of an EAP to help identify the specific actions staff should take during an emergency. Once your EAP has been developed, review it with your staff and members to maximize awareness of your emergency response procedures. Keep a copy of your EAP in a convenient location where it can be accessed; or physically provide a copy to all relevant staff. If your organization has fewer than ten employees, the Occupational Safety and Health Administration (OSHA) suggests communicating your EAP orally to your staff or members; ensure your EAP is not posted on a public facing website.

OSHA provides further information on developing an EAP. Ready.gov also offers more information on emergency preparedness.

For additional resources, click here.

Enter information or the document location for **Emergency Action Plan** below**:**

Business Continuity Planning (BCP)

Business Continuity Plans (BCPs) are closely tied to your EAPs and recovery efforts. An effective BCP should identify key personnel and guide organizations to restore essential functions after an incident occurs. This process is unique to organizations of differing sizes, industries, and capabilities.

A BCP provides information on how personnel will communicate during and after an incident. The BCP may include work and personal cell phone numbers for key staff, email addresses, and other means of electronic communication. Some organizations may have an internal system or proprietary application to enable staff member communications during an emergency or weather event. The BCP should also list key staff members and identify their roles and responsibilities during recovery efforts.

In summary, when drafting a BCP consider the following:

- How will you sustain the most essential business functions?
- How will you maintain lines of communication during an emergency incident and recovery efforts?
- How will you protect critical information, records, and IT systems?
- How will you ensure employee/staff/member safety?

DHS offers several resources to help organizations develop a BCP, including:

- Ready.gov Business Continuity Plan
- Ready.gov Business Continuity Planning Suite which includes videos and detailed walkthroughs to help develop the plan

Community Resilience

Community resilience is an organization's ability to withstand and recover from an incident. DHS encourages collaboration within communities to mitigate risk and enhance the security and resilience of the public. Key community preparedness activities include: a plan for operations continuity, compiling resources, building relationships with key partners, and information sharing.

For more information on implementing protective measures, refer to the following resources:

- CISA Tabletop Exercise Package (CTEP) offers ready-to-use exercise packages that can be tailored to an organization's threats or objectives.
- CISA Personal Security Considerations fact sheet which encourages critical infrastructure owners and their personnel to remain vigilant and report suspicious behavior that individuals may exhibit in order to thwart an attack.
- CISA Pathway to Violence – Warning Signs and What You Can Do product that explains warning signs that may lead to violence and what individuals can do to mitigate a potential incident.
- CISA "What to Do" Training Video Series provides guidance to security officials, the public, and many other stakeholders about the steps they should take to protect themselves and others from bomb incidents.

CISA Securing Public Gatherings resources provide further resources for organizations in all sectors on building community resilience and cooperation.

For additional resources, click here.

Enter information or the document location for **Business Continuity Planning and Community Resilience** below**:**

Community resilience is an organization's ability to withstand and recover from an incident.

RESOURCES

CISA provides the Security Planning Workbook tools and resources without endorsing any specific company or entity. The tools and resources identified are a starting point for an organization's security plan and do not encompass all resources that are available.

Security Planning Resources

CISA Active Shooter Emergency Action Plan
cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

CISA Active Shooter Recovery Guide
cisa.gov/resources-tools/resources/active-shooter-recovery-guide

CISA Making a Business Case for Security
cisa.gov/resources-tools/resources/isc-best-practices-making-business-case-security

CISA Mass Gathering Security Planning Tool
cisa.gov/resources-tools/resources/mass-gathering-security-planning-tool

CISA Personal Security Considerations Fact Sheet
cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

CISA Physical Security Considerations for Temporary Facilities Fact Sheet
cisa.gov/resources-tools/resources/physical-security-considerations-temporary-facilities-fact-sheet

Department of Justice Office for Victims of Crime; Mass Violence & Terrorism: Planning, Response, Recovery and Resources Toolkit
ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv

FEMA Basic Preparedness Guide
fema.gov/pdf/areyouready/basic_preparedness.pdf

FEMA Comprehensive Planning Guides
fema.gov/emergency-managers/national-preparedness

FEMA Mobile Products
fema.gov/about/news-multimedia/mobile-products

FEMA Protecting Business Operations: Second Report on Costs and Benefits of Natural Hazard Mitigation
fema.gov/sites/default/files/documents/fema_fema-331-protecting-business-operations.pdf

"I Love U Guys" Foundation
iloveuguys.org

OSHA Developing an EAP
osha.gov/etools/evacuation-plans-procedures/eap

Ready.gov

Are You Ready? Guide
ready.gov/collection/are-you-ready

Business Continuity Plan
ready.gov/business-continuity-plan

Building an Emergency Supply Kit
ready.gov/kit

Crisis Communications Plan
ready.gov/crisis-communications-plan

Emergency Response Plan
ready.gov/business/implementation/emergency

Hurricanes
ready.gov/hurricanes

IT Disaster Recovery Plan
ready.gov/it-disaster-recovery-plan

Low and No Cost Strategies
ready.gov/low-and-no-cost

RESOURCES

Risk Assessment Process

CISA ChemLock On-Site Assessments and Assistance
cisa.gov/resources-tools/programs/chemlock/chemlock-assessments

CISA Houses of Worship Security Self-Assessment
cisa.gov/topics/physical-security/protecting-houses-worship

CISA Infrastructure Survey Tool
cisa.gov/resources-tools/services/infrastructure-survey-tool-ist

CISA ISC Standard: Risk Management Process
cisa.gov/resources-tools/resources/isc-standard-risk-management-process

CISA School Security Assessment Tool
cisa.gov/school-security-assessment-tool

CISA Security Assessment at First Entry
cisa.gov/resources-tools/services/security-assessment-first-entry

CISA Vehicle Ramming Self-Assessment tool
cisa.gov/topics/physical-security/vehicle-ramming-mitigation/resources

DHS Risk Lexicon
dhs.gov/publication/dhs-lexicon

Ready.gov

Risk Assessment
ready.gov/risk-assessment

RESOURCES

Threats and Hazard Assessment Resources

CISA Chemical Security
cisa.gov/topics/critical-infrastructure-security-and-resilience/chemical-security

CISA Insider Threat Mitigation
cisa.gov/topics/physical-security/insider-threat-mitigation

CISA Office for Bombing Prevention
cisa.gov/topics/physical-security/bombing-prevention

CISA Protective Security Advisor Program
cisa.gov/resources-tools/programs/protective-security-advisor-psa-program

Department of Labor Workplace Violence Program
dol.gov/agencies/oasam/centers-offices/human-resources-center/policies/workplace-violence-program

DHS Center for Prevention Programs and Partnerships
dhs.gov/CP3

DHS "If You See Something Say Something" ®
dhs.gov/see-something-say-something

DHS Prevention Resource Finder
dhs.gov/prevention

DHS State Fusion Centers and Locations
dhs.gov/fusion-center-locations-and-contact-information

Federal Bureau of Investigation Field Offices
fbijobs.gov/locations

FEMA Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide
fema.gov/emergency-managers/national-preparedness/plan#considerations

The National Counterterrorism Center (NCTC) Joint Counterterrorism Assessment Team
dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team

The Defense Personnel and Security Research Center (PERSEREC), Enhancing Supervisor Reporting of Behaviors of Concern
https://www.dhra.mil/PERSEREC/Selected-Reports/

The United States Secret Service, Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted Violence
secretservice.gov/protection/ntac/reports

RESOURCES

Cybersecurity Resources

CISA Cyber Essentials
cisa.gov/resources-tools/resources/cyber-essentials

CISA Data Backup Options
cisa.gov/sites/default/files/publications/data_backup_options.pdf

CISA and NSA Guidance on Identity and Access Management (IAM)
cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management

CISA Mitigating the Impacts of Doxing on Critical Infrastructure
cisa.gov/resources-tools/resources/cisa-insights-mitigating-impacts-doxing-critical-infrastructure

CISA Shields Up
cisa.gov/shields-up

CISA Stop Ransomware
cisa.gov/stopransomware

Ready.gov

IT Disaster Recovery Plan
ready.gov/it-disaster-recovery-plan

Preparedness Grant Resources

Continuing Training Grants
federalgrants.com/Homeland-Security-National-Training-Program-HSNTP-14672.html

DHS Grants
dhs.gov/find-and-apply-grants

DHS — Targeted Violence and Terrorism Prevention Grant Program (TVTP)
dhs.gov/tvtpgrants

Federal Grants Guidance
grants.gov

FEMA Grants
fema.gov/grants

SchoolSafety.gov, *Grants Finder Tool*
schoolsafety.gov/grants-finder-tool

RESOURCES

Training and Exercise Resources

CISA ChemLock Exercises
cisa.gov/resources-tools/programs/chemlock

CISA Office of Bombing Prevention Training
cisa.gov/topics/physical-security/bombing-prevention/office-bombing-prevention-obp-training

CISA Pathway to Violence: Warning Signs and What You Can Do
cisa.gov/resources-tools/resources/pathway-violence

CISA Tabletop Exercise Packages

dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team

DHS Tactical Emergency Casualty Care Program
emtsinc.com/tactical-emergency-casualty-care-tecc

FEMA Emergency Management Institute
training.fema.gov/empp

FEMA Homeland Security Exercise and Evaluation Program (HSEEP)
fema.gov/emergency-managers/national-preparedness/exercises/hseep

DEFEND TODAY,
SECURE TOMORROW

ACRONYM LIST

The list below defines the acronyms used in this resource:

ACRONYM	DEFINITION
BCP	Business Continuity Plan
CCTV	Closed-Circuit Television
CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cybersecurity Advisor
CSO	Chief Security Officer
CTEP	CISA Training and Exercise Package
CTG	Continuing Training Grants
DHS	Department of Homeland Security
EAP	Emergency Action Plan
EMI	Emergency Management Institute
FBI	Federal Bureau of Investigation
FBO	Faith-Based Organizations
FEMA	Federal Emergency Management Agency
HoW	Houses of Worship
HSNTP	Homeland Security National Training Program
IAM	Identity Access Management
IED	Improvised Explosive Devices
IID	Improvised Incendiary Devices
IST	Infrastructure Survey Tool
IT	Information Technology
NICE	National Initiative for Cybersecurity Education
NSA	National Security Agency
OSHA	Occupational Safety and Health Administration
PSA	Protective Security Advisor
SAFE	Security Assessment at First Entry
SAR	Suspicious Activity Reporting
SSAT	School Security Assessment Tool
START	Study of Terrorism and Responses to Terrorism
TECC	Tactical Emergency Casualty Care
VBIED	Vehicle Borne Improvised Explosive Device