[Insert Photo]

K-12 Active Threat Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 7:45 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 9:45 a.m. | Module One: Intelligence and Information Sharing |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module Two: Incident Response |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:05 p.m. | Module Three: Recovery Continuity |
| 12:05 p.m. | 12:30 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | K-12 Active Threat Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a [insert exercise type] planned for [insert exercise duration] and will focus on [insert scope].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas] |
| **Capabilities** | * Health and Social Services
* Infrastructure Systems
* Intelligence and Information Sharing
* Mass Care Services
* On-Scene Security, Protection, and Law Enforcement
* Operational Communication
* Operational Coordination
* Planning
* Public Health, Healthcare, and Emergency Medical Services (EMS)
* Public Information and Warning
* Risk Management for Protection Programs and Activities
* [modify as needed]
 |
| **Objectives** | 1. Examine pre-incident threat intelligence, information sharing, and notification and communication procedures between public and private partners including identifying threat assessment procedures, prevention resources and programs, and discussing pertinent privacy protection concerns.
2. Examine current emergency plans, procedures, and capabilities for incident response to an active shooter threat with a focus on:
* Alert and communication procedures
* Integration and coordination between public and private partners using Incident Command System (ICS) concepts
* Eliminating the threat
* Medical and patient triage
* Training programs
1. Examine public messaging and media relations procedures during and immediately following an incident, including the Public Information Officer (PIO) role.
2. Discuss recovery and continuity plans and procedures following an incident, with a focus on prioritizing health and social services (including behavioral health) in the community and reunification.
3. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Active Shooter |
| **Scenario** | An interactive, discussion-based exercise focused on an active shooter threat at a K-12 school. The scenario consists of three modules: Intelligence and Information Sharing, Incident Response, and Recovery and Continuity. |
| **Sponsor** | [Insert the name of the sponsor organization as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A] |
| **Points of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Core Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| Exercise Objective | Core Capability |
| --- | --- |
| Examine pre-incident threat intelligence, information sharing, and notification and communication procedures between public and private partners including identifying threat assessment procedures, prevention resources and programs, and discussing pertinent privacy protection concerns. | * Intelligence and Information Sharing
* Operational Coordination
* Risk Management for Protection Programs and Activities
 |
| Examine current emergency plans, procedures, and capabilities for incident response to an active shooter threat with a focus on: * Alert and communication procedures
* Integration and coordination between public and private partners using ICS concepts
* Eliminating the threat
* Medical and patient triage
* Training programs
 | * On-Scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
* Public Health, Healthcare, and EMS
 |
| Examine public messaging and media relations procedures during and immediately following an incident, including the PIO role. | * Public Information and Warning
 |
| Discuss recovery and continuity plans and procedures following an incident, with a focus on prioritizing health and social services (including behavioral health) in the community and reunification.  | * Infrastructure Systems
* Health and Social Services
* Mass Care Services
 |
| [Insert additional objectives as necessary.] | * [Insert additional core capabilities as necessary.]
 |

**Table 1.—Exercise Objectives and Associated Core Capabilities**

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Types of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate the discussion. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Evaluators** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Intelligence and Information Sharing
* Module Two: Incident Response
* Module Three: Recovery and Continuity

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

# Scenario Ground Truth

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: [Time]

On [Insert date], a student at [Insert name of school] posted on his social media accounts his membership and allegiance to Universal Adversary (UA), an extremist group that advocates for gun violence and anti-government rhetoric. He posted pictures of himself with semi-automatic rifles, the UA flag, and suspected homemade explosives, which he boasted about learning how to make from websites and social media accounts on the dark web.

He has been bullied his entire life because of a visible facial birth mark. He had been in counseling for the past two years, but because of financial struggles his family has had to cut expenses, so he can no longer attend counseling. His mother is an elementary teacher at a neighboring school. He recently began distancing himself from the few friends he has, and his grades have significantly declined over the past two quarters.

His friends have expressed their concerns to him, but he has convinced them that everything is ok and that he is just going through a rough patch. When his parents received his progress report for the last quarter, they became very upset and grounded him. Because he was grounded, his girlfriend broke up with him by text message. Over the past two weeks, he has become increasingly distant and secretive.

This page is intentionally left blank.

# Module One: Intelligence and Information Sharing

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: [Time]

A student has reported to their teacher that a fellow student has been posting concerning messages on social media. These messages express frustration in the student’s personal and academic life, with several other of the school’s students and faculty mentioned by name. More concerning, the student has expressed some violent intent in the messages, and the reporting student and many others say it makes them fearful of the student in question.

## Discussion Questions

1. What tools and / or methods does your school or school district use to collect information on possible threats to your institution?
2. Do students have a way to report, other than to a teacher, suspicious behavior they find on social media?
	1. Are students aware how to do so?
	2. Is it anonymous?
3. What are the procedures for reporting an incident of this kind?
	1. Who would be notified of this incident?
	2. Would law enforcement be made aware of this incident?
4. Does your school participate in the School Resource Officer program?
5. If so, what information sharing procedures do the officers use with other schools in the district or state?
6. What would school officials be expecting from local, state, and federal government in response to this incident?
7. Does your school or school district have established threat assessment procedures?
8. What threat assessment team has your school or school district implemented?
9. Are your faculty and staff trained on privacy protections such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA)?
10. Are students educated on how to report concerning behavior? If so, how is it conducted?
11. Who within your school or school district is identified to receive reports?
12. What actions would your school or school district take in response to this incident from a security standpoint?
13. Does your school or school district conduct threat-based training, such as for active shooters or other threats?
14. Does your school partner with your state’s education agency for training opportunities?
15. What mental health resources are available within your school for students?
	1. What additional resources are there within the greater school district that can be leveraged for students?
16. What programs or policies does your school have in place to foster an environment of inclusivity and to assist at-risk students?
17. What steps does your school or school district take to mitigate bullying?
18. What about cyberbullying?

# Module Two: Incident Response

## Scenario

## [Insert Location]

### [Insert Previous date + 1 day]: [Time]

It is a normal day at [insert school name applicable to the exercise]. It is mid-day and all students are either in class or at lunch in the cafeteria. The gymnasium is occupied with students for gym class, and the auditorium is currently occupied with students and a teacher who are working on stage preparations and practicing lines for a theatrical play that will be held in a couple weeks.

Meanwhile, the front desk receptionist notices a suspicious individual wearing baggy attire who appears to be favoring his left side entering through the front doors. The individual does not stop by the front office to properly check-in or provide a note for their tardiness. As the individual walks by, it becomes visible the individual is armed with at least one semi-automatic gun and a backpack that seems heavier than normal. The individual briskly walks into the school, heading towards the school cafeteria and gymnasium. A few moments later, shots are fired and screaming follows.

The shooter begins to run further inside the school, towards the cafeteria and sets off the school fire alarm.

## Discussion Questions

1. What types of security measures and / or protocols, including security operations and physical infrastructure, are in place to facilitate school safety?
	1. Do you have surveillance cameras?
	2. Is the camera footage actively monitored and / or shared with law enforcement?
	3. How is access to the school controlled?
	4. What screening systems does your school employ?
	5. Are all doors lockable with an automated system, or by physical means only?
	6. Do you have a security management team, and what are their responsibilities?
2. What are the established alert and notification protocols to alert students, school staff, and visitors of an active shooter threat?
	1. Who is in charge of enacting these protocols?
	2. What communication method(s) is / are used to disseminate the alert (e.g., intercom announcement, email, radios, other information sharing platforms / devices)?
	3. What is the message that would be sent?
	4. Is a code system used?
3. How would a fire alarm activation complicate an active shooter response?
	1. What elements of response would be negatively impacted (e.g., alerting, active shooter procedure implementation, etc.), and how?
	2. Is there redundancy set up in school communications in case the primary communications systems fail?
4. How would response agencies be alerted?
	1. Who is responsible for alerting them?
	2. Does the school remain on the line with dispatch until response agencies are on-site or the threat has been neutralized?
	3. What information is included in the message to these stakeholders (e.g., building, floor, room number, physical description of the shooter, direction of movement, weapons, number of victims and injuries)?
5. What does your school’s active shooter training program entail?
	1. How are school staff trained to respond in an active shooter incident?
	2. How are students trained to respond in an active shooter incident?
	3. Who provides this training?
	4. How often is training conducted?
	5. What type of cross-training is conducted with other local agencies or nearby schools?
6. What level of security / law enforcement is at your school daily, if any?
	1. Are they armed or unarmed?
	2. How do response protocols differ between security and law enforcement?
	3. What type of training and coordination takes place between staff, security, and law enforcement regarding active shooter response?
7. How does your school’s emergency plan address an active shooter?
	1. What are the school’s immediate actions / priorities?
	2. Has this plan been collaborated and shared with appropriate stakeholders, and how is the plan updated?
	3. How do you verify that everyone is clear in understanding his or her role and responsibilities as outlined in the plan?
	4. Aer there any concerns that would inhibit implementing the school’s active shooter plan and procedures based on the scenario and the fire alarm being activated?
8. What are your school’s lockdown procedures?
9. What protocols are in place to alert nearby businesses, neighborhoods, and organizations of an incident?
	1. Who is in charge of enacting them and how are they alerted?

## Scenario Update

## [Insert Location]

### [Insert Incident date]: [Time + 15 minutes]

First responders arrive at the scene and neutralize the subject. Local response agencies arrive and begin to assist the injured. [insert number of injuries and / or fatalities, if any, as the sponsor and emergency planning team see fit] were killed or injured in the attack. EMS are on-scene and conducting triage. Calls from concerned family and loved ones overwhelm both 911 and [insert school name]. The media is arriving on-site trying to get details from anyone they can.

## Discussion Questions

1. How quickly can law enforcement arrive on-scene?
2. Does your jurisdiction have a Rescue Task Force (RTF) capability?
3. How familiar is law enforcement with the school layout?
4. What responder access considerations have been incorporated to facilitate coordinated and effective response?
5. What are law enforcement’s immediate actions and priorities as they arrive on school grounds?
6. How would school security or law enforcement integrate with local response agencies?
7. Would responding agencies establish an incident command structure?
8. How soon would this happen?
9. Who would be in charge?
10. What is the role of your organization in this incident command structure?
11. How would your organization integrate into the command structure?
12. Does your status as a public / private institution shape that role?
13. Are your organizational personnel trained on incident command procedures?
14. Are there other organizational command structures that would be established? Consider elements such as an Emergency Operations Center (EOC), Joint Information Center (JIC), or mass casualty incident (MCI).
15. How and when would that take place?
16. How is the school coordinating with response agencies and other stakeholders?
17. How is training on this conducted?
18. If applicable, how do first responders manage medical and patient triage?
19. Does your community have an MCI management plan?
20. What protocols are in place to allow fire department and EMS personnel to make entry into the school to assist injured individuals?
21. How does the school conduct an accountability check of their staff?
22. Do your plans and procedures outline this?

## Scenario Update

## [Insert Location]

### [Insert Incident date]: [Time + 60 minutes]

The school is still under lockdown as local law enforcement begins its investigation of the scene, and EMS continues its triage and medical assistance to the victims. Students and school staff are prompted to exit the school. Social media has exploded with images and posts about the incident, creating various versions of the story and vastly different estimates of injuries and fatalities. Students’ parents begin arriving at the school looking for their children. A number of off-duty police officers have arrived, two of which have children at the school.

## Discussion Questions

1. How would an evacuation be executed if deemed necessary?
2. Are evacuation procedures incorporated into the school’s emergency operations plan (EOP)?
3. Does the plan address primary and alternate rally locations?
4. Who would be responsible for providing security for those locations?
5. How would accountability be taken for evacuated students and faculty?
6. What training do students and faculty receive on evacuation procedures?
7. What information is being shared with the public at this time and how is it being distributed?
	1. Who is responsible for public messaging?
	2. How are you coordinating this messaging with response agencies and other stakeholders?
	3. Would incident command establish a JIC?
	4. Who would be involved in developing public messaging statements and priorities?
	5. How are these messages being released?
8. Do you have pre-identified PIOs?
9. How are they contacted?
10. Are they trained in this type of incident?
11. How are they integrated into the incident command structure?
12. How will they represent the school immediately following an incident?
13. How does your school handle incoming calls from those searching for loved ones and desperate for updates?
14. Would you establish a call center to assist with answering and fielding inquiries?
15. If so, who would run and staff this center?
16. What resources are available for public messaging during and immediately following an incident?
17. What social media platforms would you use as part of the response and how would you use them?
18. How would you vet information being shared on social media?
19. What measures are taken to counter rumors and misinformation?
20. How would you address inquiries from the media?
21. Is there a specified location for media members to gather?
22. How does the media receive updates?
23. How are media inquiries coordinated with Incident / Unified Command?
24. How does authority differ for public versus private schools regarding restricting access during response operations?
25. Can your school tell people to leave the grounds to go to a specific area?
26. Are there other potential issues or concerns regarding differing authority for public and private schools that may inhibit response efforts?
27. How are off-duty responders handled regarding access to the school?

# Module Three: Recovery and Continuity

## Scenario

## [Insert Location]

### [Insert Incident date]: [Time + 2-8 hours]

There were [insert number of injuries and / or fatalities, if any, as sponsor and emergency planning team see fit] because of the active shooter and the panic that ensued once the shooting started. A number of students, school staff, and first responders are showing signs of stress from being involved in the traumatic incident. Local 911 is being inundated with calls from frantic parents asking about the status of their children and where they can be reunited with them.

## Discussion Questions

1. Do you have comprehensive, established reunification procedures to efficiently and quickly reunite loved ones?
2. How quickly are reunification procedures activated?
3. Have these procedures been trained and / or tested?
4. Do you have a pre-identified reunification center for parents, students, and school staff to reunite with loved ones?
5. If so, has the reunification center already been pre-communicated to parents and other applicable external stakeholders (e.g., through school orientation materials or other school preparedness materials)?
6. Who would you be coordinating with to activate the reunification center?
7. If applicable, do you have existing agreements with other contiguous schools or organizations to assist in providing resources or shelter?
8. If the reunification center is off-site, how are students and school staff transported there?
9. How would you address crowd control and media control, including directing parking?
10. Does your organization have a continuity of operations plan?
11. Does your continuity of operations plan include a crisis communications plan?
12. What mental health services are available for students, employees, and responders?
13. What standard operating procedures (SOPs) are in place for assisting visitors that the incident impacted?
14. How would available services be communicated?
15. How would your organization handle incoming requests for information over the phone?
16. What about through various social media sources?

This page is intentionally left blank.

## Scenario Update

## [Insert Location]

### [Insert Incident date + 1 week]

One week has passed since the active shooter incident at your school, and the community is mourning [insert “the lives lost,” if applicable] and the numerous students remaining in the hospital. A number of students, staff, faculty, and first responders are still showing signs of stress after being involved in the traumatic incident.

The school has started short-term recovery to return to normal operations while simultaneously responding to the media fallout of another active shooter incident in an American school. Many students and school employees are expressing fear in returning to the facility in the wake of the attack, and parents are in constant contact with the administration wanting to know how the school is ensuring student safety.

## Discussion Questions

1. Does your facility have trauma or mental health counseling available to students?
2. Is it provided to visiting students?
3. Do your plans, policies, and procedures outline this?
4. Is participation tracked to ensure outreach is successful?
5. How and what type of messaging will be sent to employees and students?
6. What training do employees receive regarding media relations and the release of sensitive information?
7. What are the priorities at your facility post-incident?
8. Do your plans, policies, or procedures specify these priorities?
9. How are these priorities communicated internally?
10. Are priorities coordinated with county emergency management?
11. Are priorities coordinated with state or federal agencies?
12. How long will it be before impacted buildings are available for use?
13. Will just the affected building(s) be closed, or will the entire campus be closed?
14. Are there plans in place to handle donations management after the incident? Who is responsible for this task?
15. Are there plans to handle memorials after the incident?
	1. Who would be responsible for this task?
16. What local, state, or federal resources are available to assist in recovery?
17. Does your facility have memorandums of understanding (MOUs) with local response agencies or other K-12 organizations?
18. How is information communicated with personnel and families during the days following the incident?
19. If employees are unable to come back to work because of injury or trauma, do you have a plan for additional resources?
20. How would the loss of personnel impact your daily workload?
21. Are there measures used to mitigate the loss of workforce from this type of incident?
22. What information are you communicating to the public?
23. Who in your organization is responsible for making this communication?
24. How is your facility changing its procedures to ensure students and parents still feel safe?
25. Do your plans, policies, and procedures outline this?
26. Do recovery procedures affect nearby education organizations in any way?
27. Is social media being monitored to maintain awareness of information spreading that may not be accurate?
28. Who is responsible for this?
29. What procedures are in place to counter false information?
30. What is the plan to handle the significant media attention from national and / or international outlets?
31. At what point would you consider your organization back to steady-state operations?
32. What actions would be taken to address security concerns at academic institutions following the incident?
33. Are there plans to handle possible protests or demonstrations?

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| **Acronym** | **Definition** |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP**  | CISA Tabletop Exercise Package  |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center  |
| **EOP** | Emergency Operations Plan |
| **EPT** | Exercise Planning Team |
| **FERPA** | Family Educational Rights and Privacy Act  |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **ICS** | Incident Command System |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **MCI** | Mass Casualty Incident |
| **MOU** | Memorandum of Understanding |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **RTF** | Rescue Task Force |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert  |
| **SOP** | Standard Operating Procedure |
| **TTX** | Tabletop Exercise |
| **UA** | Universal Adversary |

