[Insert Cover Picture]

Higher Education Active Threat Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

This Situation Manual (SitMan) provides exercise participants with all the 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 |
| --- | --- | --- |
| 7:30 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 and 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** | Higher Education Active Threat Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] at [insert exercise location]. Exercise play is limited to [insert exercise parameters].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** | Economic Recovery; Health and Social Services; Intelligence and Information Sharing; Mass Care Services; Operational Communication; Operational Coordination; Planning; Public Health; Healthcare and Emergency Medical Services (EMS); Public Information and Warning; and Situational Assessment. |
| **Objectives** | 1. Examine threat and incident information sharing, notification, and communication procedures between public and private partners, with a focus on intelligence community partners and higher education facilities.
2. Examine multi-agency coordination using Incident Command System (ICS) concepts during a complex coordinated attack, including collaboration with higher education facilities.
3. Examine public and private organization response procedures, interaction, and public relations collaborations during an active threat.
4. Discuss recovery and continuity plans and procedures following a complex coordinated attack.
5. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Complex Coordinated Attack |
| **Scenario** | An interactive, discussion-based exercise focused on a complex coordinated attack involving a vehicle-ramming and active shooter incident. 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 utilized, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The following 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, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine threat and incident information sharing, notification, and communication procedures between public and private partners, with a focus on intelligence community partners and higher education facilities. | * Planning
* Intelligence and Information Sharing
* Operational Communications
 |
| Examine multi-agency coordination using Incident Command System (ICS) concepts during a complex coordinated attack, including collaboration with higher education facilities. | * Planning
* Operational Coordination
* Operational Communications
* Public Information and Warning
* Situational Assessment
 |
| Examine public and private organization response procedures, interaction, and public relations collaboration during an active threat. | * Planning
* Mass Care Services
* Operational Coordination
* Operational Communications
* Public Information and Warning
* Public Health, Healthcare, and Emergency Medical Services
 |
| Discuss recovery and continuity plans and procedures following a complex coordinated attack. | * Economic Recovery
* Health and Social Services
* Public Information and Warning
 |
| [Insert additional objectives as necessary] | * [Insert additional capabilities as necessary]
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

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

* **Players:** Personnel who 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.
* **Facilitator:** Provides situation updates and moderate discussions. 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:** 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 evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

# Module One: Intelligence and Information Sharing

## Scenario

## General Threat

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

Based on the number of protests taking place recently in the United States and internationally and increased chatter calling for attacks on said protests, the Secretary of Homeland Security, in coordination with other Federal entities, issues an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against the United States. There is no specific information at this time that would warrant the release of an “Imminent” Threat Alert.

The alert states that the threat is from domestic terrorist groups in the United States with ties to international terrorist organizations that are focused on protest groups, particularly in or around higher education facilities. The alert is to remain in place for three months, ending on [insert date].

## Discussion Questions

1. What do college / university stakeholders expect from the federal government and intelligence community at this time? How will you receive this information?
	1. Does your college / university receive NTAS bulletins?
2. What methods of intelligence gathering and information sharing do you have in place within your college or university?
3. How does your agency or organization triage the information you receive (formal reporting, hearsay, and social media)?
4. What security recommendations, if any, are local, state, and federal law enforcement making to college / university stakeholders at this time?
5. What plans are in place describing the required protective measure that need to be taken?
6. What actions are local, state, and federal law enforcement agencies taking at this point?
7. How would your agency or organization expect to receive information about a general threat?
8. What steps does your organization take once they receive notice of a general threat?
9. Does your organization participate in Suspicious Activity Reporting (SAR) efforts?
	1. Does your organization conduct any specific training based on SAR? If so, what kind of training?
10. What key stakeholders outside of your organization would you need to notify based on this information?
11. What kind of messaging would be released regarding general threats?

## Scenario Update: Credible Threat

### [Insert Month, Day, Year]

Following an altercation at a recent protest on campus, a number of counter-protestors were apprehended by law enforcement. Among the counter-protestors were several local college students, a couple of whom were ultimately suspended for violent conduct.

One of the suspended students used social media to rail against the university and claims that he was unlawfully discriminated against for his political beliefs. As his posts go viral, he boasts about his weapons and explosive experience, stating that he could attack campus without law enforcement being able to stop him.

Furthermore, he begins sending angry messages to facility staff, particularly those in higher positions whom he deems most responsible for his suspension. A friend of his reports that he has been talking about attacking your facility in retribution.

[Optional Additional Text Below: Use if law enforcement / fusion center is not participating.]

The state / local fusion center provides information concerning this incident to their registered members via their weekly reports process as well as to law enforcement, public safety partners, and private sector stakeholders. Local and federal law enforcement attempt to question the student but have few leads as he was expelled from his dormitory and released from employment by the administration in conjunction with his suspension.

## Discussion Questions

What do private sector stakeholders expect from the federal government and intelligence community at this time?

What products or information would the intelligence community produce regarding this incident and the ensuing threats?

What security recommendations, if any, are local, state, and federal law enforcement making to private sector stakeholders at this time?

How would this information be shared with partners in the higher education community?

What security measures, if any, will private sector stakeholders employ when a previous employee or student begins making threats on social media or otherwise?

What kind of information would your organization share with law enforcement about this incident and the ensuing threats?

Would state or federal resources, such as the fusion center, be alerted to protests or disgruntled students?

If so, what would their role be?

What actions are local, state, and federal law enforcement agencies taking at this point?

How would your agency or organization expect to receive information about a specific credible threat?

Does your facility or organization monitor social media for potential threats?

What steps does your facility take once they receive notice of a credible threat?

Does your agency or organization conduct any specific training based on credible threats?

Are there additional notifications that need to be made outside of your organization?

Would other higher education facilities in the area be alerted to this situation?

What kind of messaging would be released to the public regarding this threat?

Does the fact that these threats occur via social media require a response via social media, as opposed to traditional forms of communication (i.e., press release or formal statements)?

How would questions from patrons and news organization be handled?

Does your agency or organization conduct any specific training based on credible threats?

# Module Two: Incident Response

## Scenario

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

### [Insert Facility Name and Location]

It is a calm, clear day at your facility with the semester in full swing. Today is one of your busier days, with multiple visitors and many off-campus students on-site for various activities.

Suddenly, a large truck comes careening down the road leading to your main building and crashes into students entering and exiting the front entrance. An individual jumps out and begins firing randomly at people in the area, quickly making his way toward the classrooms as he shoots.

## Discussion Questions

1. Are there protocols in place at your organization to alert students and visitors of an emergency?
	1. Who is responsible for enacting them?
	2. What is the message that would be sent?
2. Are there protocols in place to alert nearby businesses and organization of an emergency?
	1. If so, who is responsible for enacting them?
3. How are employees trained to respond in an incident such as this?
	1. Is training conducted on a regular basis?
4. What level of security / law enforcement is at your facility / campus on a daily basis, if any?
	1. Are they armed?
	2. How do permissions differ between security and law enforcement?
	3. How are they trained to respond to these types of incidents?
5. Does your organization have a dispatch center?
	1. If so, how would they interact with law enforcement dispatch?
	2. Do you have capabilities to integrate with law enforcement and / or provide assistance?
	3. Are you able to provide access to facility cameras or other resources?
6. What public and private stakeholders would be notified about an incident?
	1. Would other higher education organization be included in those notifications?
	2. How are they alerted?
	3. Who is responsible for this communication?
7. How would response agencies and elected officials be alerted?
	1. Who is responsible for alerting them?
8. Do local agencies or higher education organizations cross-train on this type of incident?
9. How would law enforcement work to locate the shooter?
	1. How would facility / campus security or law enforcement integrate with local response agencies?
	2. How would private security integrate with law enforcement?
		1. Does this differ from how campus law enforcement integrates?
10. Does your organization have any type of organizational command structure in response to an emergency?
	1. How and when is it stood up?
11. What type of incident command structure would the responders establish?
	1. Who would be in charge?
12. What is the role of your organization in this incident command structure?
	1. How would your organization integrate into this command structure?
	2. Does your status as a public / private institution shape that role?
	3. Are they trained on incident command procedures?
	4. Is there cross-training?
13. What information is being shared with the public and how is it being distributed?
	1. Who is responsible for public messaging?
	2. How are you coordinating messaging with response agencies and other stakeholders?
	3. How are these messages being released?

## Scenario Update

### Time: [Insert time]

The active shooter was neutralized, and local response agencies are assisting injured people. The building(s) is / are still under lockdown as local law enforcement continue to search and clear the facility. Calls from concerned family and loved ones overwhelm both the campus and 911, and the media is on-site attempting to get details from anyone. Individuals post several images and statuses concerning the incidents on social media, creating various versions of the story and vastly different estimates of injuries and fatalities.

## Discussion Questions

How does your facility handle incoming calls from people searching for loved ones?

Are you familiar with available public sector and non-profit resources that can assist with establishing and operating a phone bank?

Do you have pre-identified Public Information Officers (PIOs)?

How are they contacted?

Are they trained for incidents such as these?

How are they integrated into the command structure?

How will they represent the school immediately following an incident?

What resources are available for public messaging during and immediately following an incident?

What social media platforms would you use and how would you use them?

How would you vet information being shared on social media?

What measures are taken to counter rumors and misinformation?

How would you address inquiries from the media?

Is there a specified location for on-site media?

How does media receive updates?

How is this coordinated with Incident / Unified Command?

Is there a specified location for any persons coming to the campus in person to check on loved ones?

What plans, policies, or procedures are in place for providing services, such as family assistance centers?

How would you address crowd control, including directing parking, if an inordinate amount of people showed up?

How do authorities differ for public versus private campuses regarding restricting access during response operations?

Can your facility tell people to leave the grounds or to go to a specified area?

Does the facility conduct an accountability check of their employees?

Is this outlined in your plans and procedures?

Would other higher education facilities be able to assist in any way?

Do you have any existing agreements with other facilities to assist in providing resources or shelter?

How are separated families reunited?

How quickly are reunification procedures put in place?

Who would you be coordinating with to establish a family reunification center?

Is there a specified location for walk-ins looking for loved ones?

Is this outlined in your plans, policies, or procedures?

# Module Three: Recovery and Continuity

## Scenario

### [Insert Month, Day, Year]

### [Insert Facility Name and Location]

There were multiple fatalities and injuries as a result of the vehicle ramming and active shooter, as well as the panic that ensued once the shooting started. A number of students, university employees, and first responders are showing signs of stress from being involved in the traumatic incident.

Following the initial response, the facility and local community have started short-term recovery procedures. A damage assessment is under way to determine whether the building incurred structural damage. The campus and surrounding businesses / organizations are working on continuity plans, while media continues to contact a variety of organizations looking for any additional information.

## Discussion Questions

1. How do you determine the status of your facilities before, during, and after an incident?
2. Based on the scenario, how does the damage to your facility impact operations?
	1. Are classroom location backups in place so classes can continue?
	2. What about support facilities (libraries, labs, etc.)?
3. Does your organization have a business continuity or continuity of operations plan?
	1. Does your continuity or operations plan include a crisis communications plan?
4. How and what type of messaging will be sent to employees and students?
	1. What training do employees receive regarding media relations and the release of sensitive information?
5. What are the priorities at your facility or organization post-incident?
	1. Are these priorities specified in your plans, policies, or procedures?
	2. How is this communicated internally?
	3. Are priorities coordinated with county emergency management?
	4. Are priorities coordinated with state or federal agencies?
6. What mental health services are available for students, employees, and responders?
	1. What standard operating procedures (SOPs) are in place for assisting visitors that were impacted by the incidents?
	2. How would available services be communicated?
7. Does your facility have trauma or mental health counseling available to students?
	1. Is it provided to visiting students?
	2. Is it outlined in your plans, policies, and procedures?
8. How long will it be before impacted buildings are released for use?
	1. Will just the affected building(s) be closed, or will the entire campus be closed?
	2. Who will make the decision to release the building(s)?
9. What would the financial impact be on your organization if it was closed because of such an incident?
	1. What are the implications of being unable to open your facilities to the public for a period of time?
	2. Can your organization relocate to another facility? If so, how long would this take?
	3. Would other nearby higher education organizations be able to assist in any way?
10. Are there plans in place to handle donations management after the incident? Who is responsible for this task?
11. Are there plans in place to handle memorials after the incident? Who is responsible for this task?
12. What local, state, or federal resources are available to assist in recovery or business continuity?
	1. Does your facility have memorandums of understanding (MOUs) with local response agencies or other higher education organizations?
13. How is this information communicated with personnel and families during the days following the incident?
14. If employees are unable to return to work because of injury or trauma, do you have a plan for additional resources?
	1. How would the loss of personnel impact your operations? What steps would be taken to adjust for or mitigate this?
15. What information are you communicating with the public?
	1. Who in your organization is responsible for making this communication?
	2. How is your facility changing its narrative to ensure students and parents still feel safe?
		1. Is this outlined in your plans, policies, and procedures?
16. Do recovery procedures affect nearby higher education organizations in any way?
17. Is social media being monitored to maintain awareness of information spreading that may not be accurate?
	1. Who is responsible for this?
	2. What procedures are in place to counter false information?
18. What is the plan to handle the significant media attention from national and international outlets?
19. At what point would you consider your organization back to steady-state operations?
20. What actions would be taken to address security concerns at academic institutions following the incident?

This page is intentionally left blank.

# 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 was 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 | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Services |
| **EPT** | Exercise Planning Team |
| **ICS** | Incident Command System |
| **IP** | Improvement Plan |
| **MOU** | Memorandum of Understanding |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SAR** | Suspicious Activity Reporting |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **TTX** | Tabletop Exercise  |

