[Insert Cover Picture]

Higher Education Improvised Explosive Device 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 Improvised Explosive Device (IED) 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
* Healthcare and Emergency Medical Services (EMS)
* Intelligence and Information Sharing
* Mass Care Services
* Operational Communication
* Operational Coordination
* Planning and Public Health
* Public Information and Warning
* Situational Assessment.
* [Insert additional Capabilities as necessary]
 |
| **Objectives** | 1. Examine threat and incident information sharing, notification, and communication procedures between [insert college or university] 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 between higher education facilities and public sector partners.
3. Examine [insert college or university] 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** | Bomb threat, Unattended item, Suspicious package, IED |
| **Scenario** | An interactive, discussion-based exercise focused on a phoned-in bomb threat, followed by the discovery of an abandoned item, a suspicious package, and an explosion. 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.] |
| **Point 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 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, 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 [insert college or university] partners, with a focus on intelligence community partners and higher education facilities. | * Intelligence and Information Sharing
* Operational Communications
* Planning
 |
| Examine multi-agency coordination using ICS concepts during a complex coordinated attack, including collaboration between higher education facilities and public sector partners. | * Operational Coordination
* Operational Communications
* Planning
* Public Information and Warning
* Situational Assessment
 |
| Examine [insert college or university] response procedures, interaction, and public relations collaboration during an active threat. | * Mass Care Services
* Operational Coordination
* Operational Communications
* Planning
* Public Information and Warning
* Public Health, Healthcare, and EMS
 |
| 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** 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 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** 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

## 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 only use 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

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

Over the past few years, there has been an increasing number of phoned-in bomb threats at colleges and universities throughout the United States. Most of these threats consist of little information about the caller and are often received during the early morning hours as classes are beginning. No groups or organizations have taken direct responsibility for the threats.

In the last month, 17 phoned-in bomb threats have been directed towards colleges and universities. Though none of these threats have concluded in the discovery of an explosive device, there is a sense of heightened awareness throughout the collegiate world. The Federal Bureau of Investigation (FBI) is looking into these phoned-in threats and is considering them possible hate crimes.

## Discussion Questions

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

## Scenario Update

### [Insert Month, Day, Year]

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

One of the dismissed students used social media to condemn 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 the campus with law enforcement unable to stop him.

Furthermore, he begins sending angry messages to university staff, particularly those in higher positions whom he deems most responsible for his dismissal. A friend of the suspect reports that he has been talking about attacking [insert college or university] in retribution.

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

The state / local fusion center has provided information concerning this incident to its registered members via its weekly reports process and to law enforcement, public safety partners, and private sector stakeholders. The student was removed from his dormitory, and the administration released him from his campus employment. His whereabouts are unknown. Local and federal law enforcement have attempted to question the student but have few leads.

## Discussion Questions

What do [insert college or university] stakeholders expect from the federal government and the intelligence community?

1. 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?

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

What security measures, if any, will [insert college or university] 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?

Is the area immediately surrounding your facility private property or is there an accessible public space where people may congregate?

Are there protections in place for students who are legally protesting?

Would any government involvement in protest-monitoring present concerns of First Amendment infringement?

What resources, if any, are available to students involved in campus protests to inform them of their rights and procedures?

Are faculty, law enforcement, and other government entities aware of the campus-specific protections given to students?

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

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

Does [insert college or university] monitor social media for potential threats?

What steps does [insert college or university] take once it receives notice of a credible threat?

Does [insert college or university] conduct any specific training based on credible threats?

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 (e.g., press release or formal statements)?

How would questions from alumni, patrons, and news organization be handled?

Does your [insert college or university] conduct any specific training based on credible threats?

This page is intentionally left blank.

# Module Two: Incident Response

## Scenario

### [Insert College / University Name and Location]

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

It is a calm, clear day at [insert college or university] with the semester in full swing. Today is one of your busier days of the year, with multiple alumni, visitors, and off-campus students on-site for various activities.

At approximately [insert time], the university president’s secretary received an anonymous phone call stating that bombs were being placed around your school and that the school would “pay for their misdeeds.”

At [insert time + 15 minutes], a report comes into your security office that a male wearing oversized dark clothing and carrying a large backpack was observed loitering around the lobby of your Administrative Building. This male has not talked with anyone and does not seem to be engaged in normal student behavior associated with the Administrative Building.

The male has been identified as the student who, just two weeks prior, had used social media to condemn [insert college or university] and boasted he could attack the campus at any time without being stopped by police. In his previous threats, the student claimed to be experienced in weaponry and explosives. As the building security staff were attempting to contact the student, he disappeared into the crowd, abandoning his backpack on a bench just inside the entrance to the Administrative Building.

## Discussion Questions

1. What level of security / law enforcement presence is at [insert college or university] daily?
	1. Are they armed?
	2. How are they trained to respond to these types of incidents?
2. Is there initial and ongoing training for IED recognition and bomb-making material awareness?
3. Are your security personnel trained in the difference between an “abandoned item” and a “suspicious package?”
4. Are there programs in place for reporting suspicious actions, such as “See Something / Say Something?”
5. How would response agencies and elected officials be alerted to this situation?
	1. Who is responsible for alerting them?
6. What explosive detection K-9 resources does [insert college or university] have access to?
	1. Does [insert college or university] have access to outside agency explosive detection K-9s?
7. If so, how would you request their assistance?
8. Once requested, how long would it take for them respond?
9. Are explosive detection K-9 teams familiar with your campus, and have they previously conducted training with your security staff?
10. Do you have memorandum of agreements in place to expedite response times?

## Scenario Update

### Time: [Insert time]

Utilizing the security camera footage, campus security has been able to track the suspects’ movements leading up to him abandoning the backpack on the bench at the Administrative Building. They reported that the suspect had left another backpack just outside the campus food court.

Security officers have responded to the campus food court and are reporting back to their supervisors that the backpack is partially open, and they can see cylindrical metal pipes with endcaps. They also see nails taped to the outside of the pipes and wires coming from the top of the pipes, leading to a cell phone, which is taped to the side of one of the pipes. They believe the items within the backpack are bombs and have begun evacuating the immediate area.

## Discussion Questions

Are there protocols in place at [insert college or university] to alert students and visitors of an emergency?

* 1. What is the message that would be sent?
1. Does [insert college or university] have emergency shelter in place or evacuation protocols?
	1. If so, how often are they updated and practiced?
2. What lockdown procedures does [insert college or university] have?
	1. How often are they updated and practiced?
3. Are there protocols in place to alert nearby businesses and organizations of an emergency?
4. How are university employees trained to respond in an incident such as this?
5. Is training conducted on a regular basis?
6. Does [insert college or university] have any type of organizational command structure in response to an emergency?
7. How and when is it stood up?
	1. Do local agencies or higher education organizations cross-train for this type of incident?
	2. How would campus security or law enforcement integrate with local response agencies?
	3. How would private security integrate with law enforcement?
	4. Does this differ from how campus law enforcement integrates?
8. What is the role of [insert college or university] in this incident command structure?
	1. How would [insert college or university] integrate into this command structure?
	2. Does your status as a public / private institution shape that role?
	3. Are [insert college or university] administration, security personnel, and employees trained on incident command procedures?
	4. Is there cross-training between [insert college or university] personnel and local first responders?
9. What additional notifications need to be made outside of [insert college or university]?
10. How is this notification process conducted?
11. Would other colleges or universities in the area be alerted to this situation?
12. Are there established protocols at [insert college or university] to alert students and visitors to an emergency?
	1. Who is responsible for enacting them?
	2. What is the alert message that would be sent?
13. Does [insert college or university] have a dispatch center?
	1. If so, how would it interact with law enforcement dispatch?
	2. Do you have capabilities to integrate with law enforcement and / or to assist them?
	3. Are you able to provide access to [insert college or university] cameras or other resources?
14. Are there established protocols to alert nearby businesses and organizations to an emergency?
	1. If so, who is responsible for enacting them?
15. What [insert college or university] stakeholders would be notified about an incident?
	1. Would other higher education organizations be included in those notifications?
	2. How are they alerted?
	3. Who is responsible for this communication?
16. 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

### [Insert time]

While response personnel are evacuating everyone from the food court area, the device explodes, sending a violent shock wave, an intense fireball, and deadly shrapnel through the air. Thick black smoke billows from the building, and debris is scattered everywhere. The food court building suffered significant structural damage. Initial reports indicate at least one security officer and seven students have been killed. Due to the chaos at the scene, the total number of fatalities and injuries are currently unknown.

## Discussion Questions

1. What are your immediate priorities following this event?
2. What plans do [insert college or university] have to request the bomb squad for response?
3. Can [insert college or university] call the bomb squad directly for response?
	1. If so, who do you call and do you have their number?
	2. If so, is there a succession of contact personnel for this emergency?
	3. Is the bomb squad familiar with your campus?
4. How would the command structure be impacted at this time?
5. Do you have emergency medical response units on campus?
6. Are law enforcement, fire, and EMS responders familiar with your campus?
7. Does your emergency operation plan include pre-determined access routes for off-campus emergency responders?
	1. Have those plans been shared with off-campus emergency responders?
	2. Have those plans been practiced? If so, how often?
8. Are emergency responders trained in mass casualty incidents where bomb blast injuries are expected?
9. What capacity does your campus medical response have to treat mass casualty incident patient surge?
10. What shelter-in-place or evacuation protocols does [insert college or university] have in place?

How often are they updated and practiced?

Do these procedures account for individuals with access and functional needs?

## Scenario Update

### [Insert time]

The suspect was apprehended, and local response agencies are assisting injured people. The building(s) is / are still under lockdown as local law enforcement continues to search and clear the campus.

Calls from concerned family members and loved ones overwhelm both the campus and 911 center. The media is on-site attempting to get details from anyone who will speak to them. Individuals are posting numerous images and statuses about the incident 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 [insert college or university] 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 assess 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 the media receive updates?

How is this coordinated with Incident / Unified Command?

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

What plans, policies, or procedures exist 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 does authority regarding restricting access during response operations differ for public versus private campuses?

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

Does your facility conduct an accountability check of its employees?

1. Do your plans and procedures outline this?

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

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

How are separated individuals reunited?

How quickly are reunification procedures put in place?

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

Do your plans, policies, or procedures outline this?

This page is intentionally left blank.

# Module Three: Recovery and Continuity

## Scenario

### [Insert Facility name and location]

### [Insert Month, Day, Year]

There were [insert number] fatalities and [insert number] injuries resulting from the explosion and the panic that ensued once the incident started. Several students, university employees, and first responders are showing signs of stress after 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 underway to determine whether the campus incurred structural damage. The [insert college or university] and surrounding businesses / organizations are working on continuity plans, while the media continues to contact a variety of organizations looking for any additional information.

## Discussion Questions

1. How do you determine the status of [insert college or university] before, during, and after an incident?
2. Based on the scenario, how does the damage to [insert college or university] impact operations?
	1. Are classroom location backups in place so classes can continue?
	2. What about backups for support facilities (e.g., libraries, labs, etc.)?
3. Does [insert college or university] 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 the incident impacted?
	2. How would available services be communicated?
7. Does [insert college or university] have trauma or mental health counseling available to students?
	1. Is it provided to visiting students?
	2. Do your plans, policies, and procedures outline this?
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 [insert college or university] if it were closed because of such an incident?
	1. What are the implications of being unable to open [insert college or university] to the public for a period of time?
	2. Can [insert college or university] relocate to another location?
	3. If so, how long would this take?
	4. Would other nearby higher education organizations be able to assist in any way?
10. Are there plans to handle donations management after the incident? Who is responsible for this task?
11. Are there plans 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 [insert college or university] have memoranda 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 to the public?
	1. Who in [insert college or university] is responsible for making this communication?
	2. How is [insert college or university] changing its narrative to ensure students and parents still feel safe?
		1. Do your plans, policies, and procedures outline this?
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 exist 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 [insert college or university] 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 |
| **FBI** | Federal Bureau of Investigation |
| **ICS** | Incident Command System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **MOU** | Memorandum of Understanding |
| **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  |

