[Insert Cover Picture]

Defense Industrial Base 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 and Response |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:05 p.m. | Module Three: Business Continuity and Recovery |
| 12:05 p.m. | 12:30 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Defense Industrial Base 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 * Interdiction and Disruption * On-Scene Security, Protection, and Law Enforcement * Operational Coordination * Planning * Public Information and Warning * [Insert other capabilities as necessary] |
| **Objectives** | 1. Review pre-incident and incident response information sharing procedures between military branches, military service components, military installation command, corporate leadership, employees, and emergency responders. 2. Discuss private sector stakeholders’ emergency preparedness plans and response procedures to an active shooter / improvised explosive device (IED) incident and coordination activities under National Incident Management System (NIMS) with local, state, and federal agencies. 3. Consider participating organizations’ business continuity plans or continuity of operations plans to identify best practices in the aftermath of a complex coordinated attack on a large defense industrial base (DIB) workshop facility. 4. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Active Shooter and IED |
| **Scenario** | An interactive, discussion-based exercise focused on an active shooter / IED incident threatening a large DIB workshop facility. The scenario consists of three modules: Intelligence and Information Sharing, Incident and Response, and Business Continuity and Recovery. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix B.] |
| **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** |
| --- | --- |
| Review pre-incident and incident response information sharing procedures between military branches, military service components, military installation command, corporate leadership, employees, and emergency responders. | * Intelligence and Information Sharing * Planning * Public Information and Warning |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to an active shooter / IED incident and coordination activities under NIMS with local, state, and federal agencies. | * Intelligence and Information Sharing * Interdiction and Disruption * Operational Coordination * On-Scene Security, Protection, and Law Enforcement * Planning |
| Consider participating organizations’ business continuity plans or continuity of operations plans to identify best practices in the aftermath of a complex coordinated attack on a large DIB workshop facility. | * Economic Recovery * Health and Social Services * Planning |
| [Insert additional objectives as necessary]. | * [Insert additional core 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 and Response
* Module Three: Business Continuity and Recovery

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

### [Insert Month, Day, Year]

Based on recent attacks in the United States, 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 details of the alert state the threat is from domestic anti-government terrorist groups in the United States with ties to international terrorist organizations that are focused on large DIB workshop facilities. The alert is to remain in place until [insert date + 3 months].

The [insert relevant state or local agency] using the [insert state / regional fusion center] has passed the alert on to its partners in the Commercial Facilities Sector.

## Discussion Questions

1. How would your agency or organization expect to receive information about a credible threat?
   1. What steps does your agency or organization take once they receive notice of a credible threat?
2. Does your agency or organization receive NTAS alerts?
   1. What about Suspicious Activity Report (SAR) Bulletins?
3. What organizations would you communicate with regarding this incident (e.g., local law enforcement agencies, your Joint Terrorism Task Force [JTTF], Federal Bureau of Investigation [FBI], Department of Defense [DoD], etc.)?
4. Does your organization maintain a relationship with your U.S. Department of Homeland Security (DHS) Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
5. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
6. What internal information sharing and dissemination processes does your organization currently use?
   1. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media, etc.) for further dissemination within your organization?
   2. Do you push information to your service and business partners, such as parking services, janitorial staff, and other support personnel?
7. What information or warnings about the elevated threat level are being released to the public?
   1. Do you have a Public Information Officer (PIO)?
   2. Who is responsible for the initial messaging?
   3. How quickly is information being released?
   4. What methods are being used to distribute information?
   5. What should the content of the messaging be?
   6. Are businesses or other organizations providing their own messaging to their employees?
   7. How are messages coordinated across the different agencies and organizations?
8. If “suspicious behavior” is observed at your facility, how do you report this information locally and within the DIB?
   1. Are trends of suspicious behaviors tracked and disseminated across the DIB nationwide?
9. Does your facility have written emergency plans or policies that guide emergency decision making, command and control decisions, and information sharing?
   1. Have you incorporated local law enforcement or emergency management agencies into the planning development process?
   2. Are local law enforcement and emergency management agencies aware of your expected needs and / or resource gaps?
10. Would your facility adjust its security measures after the issuance of the NTAS elevated threat alert? If so, how?
11. Would you share this threat information with international industry partners?
    1. What would be the benefit of doing so, if any?
12. Are there technological barriers, policies, legal considerations, or institutional sensitivities that might affect information sharing?
13. Does your agency or organization conduct any specific training based on credible threats?
14. What risk mitigation or protective actions would you implement?
    1. Would you take any additional measures to monitor for suspicious activities?

# Module Two: Incident and Response

## Scenario

### [Insert Month, Day, Year + 7 Days]: [Time]

At approximately [insert time], two individuals drive into the [Insert Facility Name] parking lot in a dark blue delivery van and park near the main entrance of [Insert Facility Name]. A short time later, one man exits from the driver’s seat carrying a large backpack, while the second exits from the van’s rear doors a few moments later holding a duffel bag. The two enter the large workshop facility and begin walking down the assembly lines towards the rear of the workshop.

As the men move towards the rear, a shop supervisor in the immediate vicinity becomes suspicious and alerts security. When two security guards arrive and approach the two, the backpack carrying individual removes a handgun from under his jacket and fires it, hitting and wounding both security guards.

Upon hearing gunfire, employees in the area begin panicking, running towards the secondary exits, and hiding behind any shelter they can find. Some employees that were able to escape the vicinity of the gun fire begin to desperately call 911 dispatch.

After the backpack wearing individual shoots the security guards, the individual with the duffel bag draws a shotgun out of the duffel bag and starts walking down the assembly line firing indiscriminately at workshop employees.

## Discussion Questions

1. What actions would your organization take at this time?
   1. What resources and assets do you have available to assist in the response?
2. Are there established protocols at the workshop to alert employees to an emergency?
   1. Who is in charge of enacting them?
3. What are crowd control and / or evacuation procedures for an incident of this type?
   1. Who is responsible for activating the evacuation procedures?
   2. Is there a specific location for evacuees?
      1. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
4. Would there be any accountability taken of the employees in the workshop? If so, how is this accomplished?
5. Is there security staff on-site?
   1. How are they trained to respond to active shooter incidents?
   2. Is local law enforcement familiar with the site?
6. How will local law enforcement respond to this incident?
   1. What steps must be taken prior to engaging the shooters?
   2. In addition to responding to the threat, what other services would they be expected or asked to provide?
   3. What other emergency services would respond to this incident?
7. What additional local response assets are available to be requested?
   1. What would their response time be?
8. Do you have mutual aid agreements (MAA) to assist in an emergency?
   1. Would they be requested at this time?
9. At this point in the response, are there any messages being released to the public?
   1. Who is responsible for this type of messaging?
   2. How is this messaging coordinated?
10. At this point in the response, would you share information with other relevant organizations in your area?
    1. Who is responsible for this type of messaging?
    2. What would other organizations do with this information?
    3. Would other organizations assist you in your response?
    4. Are there any memorandums of understanding (MOU) in place?
    5. How would local law enforcement share information with the community?
11. What measures will be taken to streamline the information sharing process?
    1. How will you resolve potential misinformation?
    2. How will you respond to and coordinate any of the media’s requests for comment?

## Scenario Update

### [Insert Month, Day, Year]: [Time: Incident + 20 minutes]

Calls continue to flood the local 911 dispatch from employees that have either fled the scene or are still trapped in the workshop facility. According to callers inside the facility, the gunmen are walking through the workshop wielding assault rifle-styled weaponry and shooting at anyone they find. Callers report several wounded employees, including multiple people lying motionless on the ground.

As law enforcement arrives and enters the workshop, an explosion erupts from inside the shooters’ van in front of the workshop facility. The explosion injures a law enforcement officer and damages several of their response vehicles in addition to devastating several nearby parked cars.

Outside callers and local response agencies, via radio communications, report the detonation. In response to this newly received information, additional police, fire, and emergency medical service (EMS) units are requested, along with bomb squad.

**Discussion Questions**

1. What procedures, if any, do law enforcement, fire, and EMS agencies have to respond to an attack on their own personnel?
2. Do local first responders have Rescue Task Force (RTF) capabilities that could be used in this situation?
   1. Who is responsible for activating the use of any RTFs?
3. If MAAs were not activated before, would they be activated now?
   1. Would this scenario have changed the type of mutual aid that was requested?
4. If incident command / commander staff is killed, injured or otherwise unavailable, who takes command?
   1. Is there a designated line of succession?
   2. Is this process well known and exercised?
   3. About how long would it take to re-establish a working command post?
   4. What procedures would be considered to ensure the safety of first responders and command staff?
   5. What additional security procedures are in place to ensure responders’ safety that would suspend or slow life-saving operations until fully implemented?
5. What is standard operating procedure after law enforcement officers encounter IEDs in this situation?
   1. Will additional response, predominantly regarding engaging the active shooters, be delayed?
6. How would law enforcement re-establish the surrounding area as secure?
7. What steps need to take place to ensure the area is cleared of all potential threats?
8. Would these actions be concurrent or take place after entry of the workshop?
9. What impact does the expanding incident area have on the command structure?
10. Would there be sufficient resources immediately available for both incidents?
11. What information, if any, would be passed on to the public? Who is in charge of this messaging?
12. At what point would federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) be contacted?
13. Do your agencies or organizations cross-train on complex coordinated attack scenarios?

## Scenario Update

### [Insert Month, Day, Year] [Time: Insert Time + 40 minutes]

Other than one law enforcement officer, the rest of the responding law enforcement officers were uninjured from the vehicle-borne improvised explosive device (VBIED) blast and make entry through the front entrance into the workshop facility. Law enforcement eventually catch up with and engage the two gunmen, wherein they neutralize both gunmen.

Law enforcement secures the inside of the workshop for any other potential gunmen and starts to evacuate employees to the rear of the building away from the van blast. Law enforcement attends to the wounded until fire and EMS arrive on-scene.

Bomb squad is called and sets a perimeter around the parking lot and workshop. Both are later deemed safe of any additional potential IEDs / VBIEDs. Reports are saying that there are at least [insert number] confirmed fatalities as well as approximately [insert number] victims with injuries varying in severity.

**Discussion Questions**

1. Who is in charge of securing the scene?
   1. Would this differ for the exterior parking lot and the interior of the workshop?
2. What steps need to take place to ensure the workshop is cleared of all gunmen and potential IEDs?
3. What protocols exist to allow fire and EMS personnel to enter into the workshop facility to assist injured employees and casualties?
4. What procedures are taken to stand up an emergency operations center (EOC)?
   1. What level of activation do you anticipate for this incident?
   2. What are the communication procedures for the different levels?
5. Would incident command establish a joint information center (JIC)?
   1. If so, who would be included in the JIC?
6. How are hospitals notified about the number and severity of the wounded?
   1. What procedures exist to handle a mass casualty incident?
7. Would mass care facilities, family assistance, or reunification centers be set up?
   1. What procedures exist for this to happen?
   2. Which agency or organization would be in charge?

Who is responsible for communicating information to the family members of those killed or injured?

This page is intentionally left blank.

# Module Three: Business Continuity and Recovery

## Scenario

### [Insert Month, Day, Year + 3 Days]

Three days have passed since the attack on [Insert Name], and the investigation is still underway. A distinct motive for selecting [Insert Name] is not evident, although investigators identified ties between the deceased gunmen and domestic anti-corporate terrorist group known as the Universal Advisory.

There was a total of [insert number] fatalities from the shooting and IED incident. An additional [insert number] victims sustained various injuries resulting from the ensuing panic; [insert number] of these were life threatening. Those [insert number], along with [insert number] others, are still hospitalized at the present time.

Local and federal authorities continue to gather all evidence from the large workshop facility and parking lot. It is unknown when the security of the vicinity will be turned back over to [Insert Name] ownership, where they can then begin cleanup and recovery operations.

## Discussion Questions

1. How will the ramifications of such an event be addressed regarding business continuity planning or rapid recovery operations?
   1. Does your organization have an established continuity of operations plan or business continuity plan?
   2. What are the implications of being unable to open your workshop facility for a period of time?
   3. Does your facility’s closure affect any other production facilities or supply chains?
   4. Can your organization relocate to another facility?
      1. If so, how long would this take?
   5. How would the loss of personnel impact your operations?
      1. What steps would be taken to adjust for or mitigate this?
   6. How is information communicated with personnel and families during the days following the incident?
   7. Will owners / operators face liability issues from the attack?
2. How will government organizations manage response efforts while beginning long-term recovery processes?
3. How will employee absences (due to personal / family impacts from the incident) affect response and recovery efforts?
4. Will your organization set up a memorial for the deceased?
5. Do you have a plan to handle donations?
6. Do you have a plan to handle protests?
7. What state and / or federal resources would your organization request or require?
8. What aid would your organization provide to private sector assets or resources?
   * 1. How are roles and responsibilities delineated?
     2. What plans or programs outline this aid or assistance?
9. What private sector assets or resources are available to assist your organization and the overall response effort?
10. Are pre-arranged agreements in place with private sector organizations to provide resources?
11. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
12. How will this coordination and information sharing take place?
13. How will patron and employee personal item loss, including motor vehicles damaged in the IED explosion, be addressed?
14. Given the scenario, what measures would be needed to support your organization’s employees following this event?
    1. How is information communicated to employees during the days and weeks following the incident?
    2. Will mental health counseling for employees and family members be available?
    3. Is financial assistance available to employees if operations are suspended for an extended length of time?
15. At what point would you consider the impacted area and all associated organizations or businesses stabilized and back to steady state?

# Appendix A: Sample NTAS Alert

This image shows a sample NTAS alert that reads as follows: 

HEADER: National Terrorism Advisory System Elevated Alert 
www.dhs.gov/advisories [insert date] 

DURATION: This Bulletin will expire on or before [insert date] at [insert time] EDT.

TYPES OF ADVISORIES: 
Bulletin: Describes current developments or general trends regarding threats of terrorism 

Elevated Alert: Warns of a credible terrorism threat against the United States 

Imminent Alerts: Warns of a credible, specific, and impending terrorism threat against the United States. 

BODY: SUMMARY OF TERRORISM THREAT TO THE U.S. HOMELAND 
- Based on recent incidents intelligence gathering efforts, the Department of Homeland Security is issuing an Elevated Threat alert for the Commercial Facilities Sector. 
- Current intelligence indicates that an attack could be focused on large Defense Industrial Base workshop facilities. 
-Authorities are currently investigating a  number of domestic anti-corporate terrorist groups within the United States with ties to international terrorist organizations. 
-Local law enforcement are encouraged to work with their private sector partners to ensure they are aware of the Elevated Threat status. 

HOW YOU CAN HELP: 
- Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators. 
-Report suspicious activity or information about a threat, including online activity to fusion centers and the FBI's Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative
-Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity 

BE PREPARED: 
- Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs information with you. 
-Connect, plan, train, and report to prepare business and employees. Security resources can be accessed through the DHS's Hometown Security Campaign. 

STAY INFORMED: 
- The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials. 

FOOTER: 
If You See Something, Say Something. Report suspicious activity to local law enforcement of call 911. 

The National Terrorism Advisory System provides information on homeland security issues and threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates:  www.twitter.com/dhsgov 



**Figure 1. – Sample NTAS Alert**

This page is intentionally left blank

# Appendix B: 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 C: Relevant Plans

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

This page is intentionally left blank.

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **ATF** | Bureau of Alcohol, Tobacco, Firearms and Explosives |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | U.S. Department of Homeland Security |
| **DIB** | Defense Industrial Base |
| **DoD** | Department of Defense |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **JTTF** | Joint Terrorism Task Force |
| **MAA** | Mutual Aid Agreement |
| **MOU** | Memorandums of Understanding |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Report |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **RTF** | Rescue Task Force |
| **TTX** | Tabletop Exercise |

|  |  |
| --- | --- |
| **Acronym** | **Term** |
| **VBIED** | Vehicle-Borne Improvised Explosive Device |

