****COVID-19 Insider Threat Active Shooter 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 |
| --- | --- | --- |
| 7:45 a.m. | 8:30 a.m. | Registration |
| 8:39 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 9:45 a.m. | Module One: Pandemic Recovery |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module Two: Pre-Incident |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:05 p.m. | Module Three: Incident Response |
| 12:05 p.m. | 12:30 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | COVID-19 Insider 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], 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** | * Community Resilience
* Economic Recovery
* Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
* Situational Assessment
* [Insert additional capabilities as necessary]
 |
| **Objectives** | 1. Examine organizational recovery procedures and the coordination of recovery operations across stakeholder groups.
2. Discuss plans, policies, and procedures for continuity of operations and business continuity.
3. Examine plans for addressing a potential insider threat and workplace violence.
4. Assess the existing methods and effectiveness of internal and external communications and coordination during an adversarial event.
5. Examine the effectiveness of overall emergency response procedures to an adversarial event regarding the Incident Command System (ICS) and logistical coordination among on-scene authorities.
6. [List exercise objectives]
 |
| **Threat or Hazard** | Insider Threat |
| **Scenario** | A disgruntled employee is actively shooting in the workplace during pandemic recovery. |
| **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 organizational recovery procedures and the coordination of recovery operations across stakeholder groups. | * Community Resilience
* Operational Coordination
* Planning
* Public Information and Warning
* Situational Assessment
 |
| Discuss plans, policies, and procedures for continuity of operations and business continuity. | * Community Resilience
* Economic Recovery
* Long-Term Vulnerability Reduction
* Operational Coordination
* Planning
 |
| Examine plans for addressing a potential insider threat and workplace violence. | * Planning
* Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
 |
| Assess the existing methods and effectiveness of internal and external communications and coordination during response to an incident. | * Planning
* On-scene Security, Protection, and Law Enforcement
* Operational Coordination
 |
| Examine the effectiveness of overall emergency response procedures to an adversarial event regarding the ICS and logistical coordination among on-scene authorities. | * Planning
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
 |
| [Insert objective] | * [Insert capability aligned to each objective]
 |

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: Pandemic Recovery
* Module Two: Pre-Incident
* Module Three: Incident Response

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.

# Scenario Ground Truth

### [Insert Month, Day, Year]

Several months ago, the public was made aware of an emerging novel coronavirus known as SARS-CoV-2, and the subsequent disease it causes known as coronavirus 2019, or COVID-19, which could have catastrophic effects on daily life. Soon after, the virus spread across the globe and reached the United States through multiple vectors. As the illness spread throughout the country, the numbers of infected and deceased individuals reported in every state and territory increased exponentially.

Since then, the federal government recommended that state and local governments should take to limit the spread of the virus by recommending measures, such as limitations on mass gathering, social distancing policies, facial covering requirements, and stay-at-home orders. While these measures are effective in slowing the rate of transmission, the side effect of disrupting most commercial activity resulted in a massive surge in unemployment claims across the country and significant disruption for businesses of all types and sizes.

State governments took the lead in community response to the ongoing crisis and requested federal disaster declarations from the president to facilitate the engagement of federal resources as well as some states activating their state emergency operations centers (EOCs). Individual localities followed suit, activating their respective EOCs and relaying information on local impacts to the states to facilitate response and future recovery operations. New production capacity and distribution chains for medical equipment alleviated initial shortages and the resulting rapid depletion of emergency stockpiles. [Optional; Insert any additional key details specific to your organization.]

Current reports of the economic impact to [insert locality / state / critical infrastructure sector] are grim with jobless claims of [insert percent / number] and financial losses estimated at [insert dollars]. There are disparate impacts across various demographic groups. Residents are cooperating with social distancing policies and stay-at-home orders for the most part. Reduced use of public transportation, along with the massive decrease in commercial activity, is disrupting business operations for both small and large businesses as well as creating revenue shortfalls for both local and state governments. Experts warn that these economic impacts could result in serious long-term consequences.

This page is intentionally left blank.

# Module One: Pandemic Recovery

## Scenario

## [Insert Location]

### [Event + 3-6 Months]:

It has been three months since states across the country implemented measures to address the rapid spread of COVID-19. Medical experts continue to monitor the infection rates closely, though the reported numbers of new cases are steadily declining. Officials cite the collective response efforts, such as social distancing and physical protective measures, as policies that helped flatten the curve.

As public health improves because of the measures implemented to minimize the spread of the virus, the economic damage caused by the disruption of commerce leaves numerous storefronts empty and creates long waits to file for unemployment benefits, straining local government resources. State and local leaders, eager to re-establish economic productivity, begin to encourage citizens to return to work. To support the workforce, public transportation services restart their regular schedules.

Health officials warn that while the pandemic appears to be slowing down, a vaccine is not yet developed, and that stakeholders should take every precaution available to prevent a “second wave” of COVID-19 cases.

The governor of [insert state] provides a “new norm” framework for businesses to reopen and commercial activity to recommence. Private and public sector establishments are required to foster a safe environment for their staff that include the use of face masks, social distancing, and occupancy limits. Employees at [insert organization] inquire about their return to work and resuming normal business operations, with many expressing anxieties for their health and safety.

## Discussion Questions

1. What is the priority focus of recovery operations for your organization at this stage?
2. For your organization, what is the key turning point in stabilizing your operations and transitioning to the next stage of recovery?
3. Is the next stage of recovery returning to normal operations? If so, what would “normal” operations look like after the pandemic?
4. If you have enacted your organization’s business continuity plans, when can you begin to shift your posture and transition toward normal operations?
	1. Who in your organization makes that decision?
5. How are you managing the ongoing impacts to your business operations?
	1. What steps will your business be taking to gradually restore operations?
6. How are you managing the ongoing impacts to your workforce?
	1. If there are ongoing delays in restoring your skilled workforce to pre-pandemic levels, what is the impact to your business?
	2. Have you identified minimum staffing to maintain or re-establish your organization’s core business functions?
	3. Have you identified any changes in your workforce needs and capabilities moving forward?
	4. How long will it take to hire and train new personnel to meet your evolving needs?
	5. How are you filling skilled positions, especially if no one in your organization is available to train them?
	6. Would there be requirements for returning staff?
	7. What challenges would you face in implementing these requirements (e.g., testing shortages, policies to provide workers paid sick leave)?
7. How are you managing the challenges of ongoing impacts to you supply chain?
	1. How are you coordinating with suppliers to improve your access to the supply chain?
	2. How will ongoing supply chain capacity shortfalls impact your ability to operate?
	3. Would stabilization depend upon your upstream suppliers impacting your production capacity, your downstream vendors impacting demand levels, or a combination of both?
8. Does your organization have the flexibility to adapt plans if the situation worsens?
9. What government services (e.g., public transportation) will your organization rely on to facilitate stabilization and ongoing recovery efforts?
10. Will your restoration activities be dependent upon receipt of state and / or federal funding?
11. What restoration activities is your organization able to initiate prior to receipt of state and / or federal funds
	1. Is your transition to long-term recovery dependent on receipt of those funds?
12. How do you identify and prioritize unmet needs?
13. What information is being communicated to the public at this time? How is that messaging coordinated and distributed?
	1. Would your organization use social media to assist in these communications?
14. As you restore operations, what plans or procedures are in place to work with access and functional needs populations?
	1. Who is responsible for that coordination?
	2. What other resources could be used and how would that occur?
15. Are / were response and recovery plans and actions being documented accordingly?
16. How is your organization working at this stage to address vulnerability reduction?
17. What steps are you taking as you transition from intermediate recovery to long-term recovery?

This page is intentionally left blank.

# Module Two: Pre-Incident

## Scenario

### [Insert Event + 5-8 Months]

Businesses throughout [insert state] experience an uptick in revenue as restrictions are slowly eased and social anxiety starts to quell. [Insert organization] takes a phased approach to bring employees back to the worksite to meet the projected demand of its services. Additional guidelines are issues to all employees that outline mandatory workplace protective equipment requirements and social distancing etiquette.

As [insert organization] returns to normal operations and business hours, several employees have already expressed frustration with the “new norm” working environment, believing that the guidelines put forth seem excessive and unnecessary. Some members of the workforce are subject to pay cuts and or reduced hours due to financial setbacks during the pandemic and diminished revenue. There is even chatter among employees who state their support for the organized protests throughout the country concerning COVID-19 guidance.

An on-site supervisor is made aware that a few employees threatened to quit because of the COVID-19 policies, attributing their stress to workplace restrictions. Another manager received an anonymous tip that there are certain individuals who are becoming increasingly resentful since returning to work and are complaining about their cut wages.

## Discussion Questions

1. What formal information sharing processes would your organization use at this point?
2. What resources does your organization use to disseminate information?
	1. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools) does your organization use to share information and communicate the implementation of protective measures?
3. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased patrols)?
4. How is your organization coordinating with information sharing partners (e.g., local law enforcement, Joint Terrorism Task Force [JTTF], fusion centers, etc.)?
5. Who is responsible for coordinating the risk communications message for your organization?
6. What are the key messages that should be distributed concerning the continuing credible threat to your organization and stakeholders?
	1. Is the message coordinated with emergency services?
	2. If so, what is the process for coordinating this message?
7. What security measures, if any, will be employed by private sector stakeholders?
8. What security recommendations, if any, are local, state, and federal law enforcement making to private sector stakeholders at this time?
9. What additional actions are local, state, and federal law enforcement agencies taking at this point?
10. How does your agency or organization triage the information you receive, such as formal reporting, hearsay, and social media?
11. How would your agency or organization expect to receive information about a credible threat?
12. What steps does your organization take once they receive notice of a credible threat?
13. Are there additional notifications that need to be made outside of your organization?
14. What plans are in place describing the required protective measures that need to be taken?
15. Does your agency or organization conduct any specific training based on credible threats?

# Module Three: Incident Response

## Scenario

### [Insert Event + 6-9 Months]

Over the last couple of weeks, [insert organization] receives an increased number of complaints about an employee that many describe as “disgruntled.” According to the complaints, [insert name] has had multiple verbal altercations with his co-workers about using masks in the office and demonstrates aggressive behavior with those around him. A few co-workers are aware of a rumor that has spread about his pending divorce, which they believe aggravated his temperament at work.

On a busy morning, the Human Resources Department received an email from another employee about disturbing messages that [insert name] posted on social media. One post makes angry references to being furloughed and describes defamatory accusations against the company. Other messages allegedly contain threatening language and allusions to future violent actions from [insert name], including joining a small group of armed individuals protesting workplace restrictions in the city.

Upon discovering the social media posts, [insert name] is required by his supervisor to come to the office where they discuss the ongoing issues with his behavior at work. The supervisor also addresses ongoing issues with [insert name]’s poor performance and informs him that he will be placed on a probationary period, warning him that if his work and behavior do not improve, there will be steeper consequences. [Insert name] abruptly ends the meeting, not wishing to discuss anything further with his boss and is visibly angry when he leaves the office.

[Insert name] exits the building and walks out to the parking lot. He gets into his car and speeds off aggressively.

### [Insert + 1 Week]

On a busy day at the company, [insert name] approaches the building in dark and casual clothing, with a duffle bag in hand and employee credentials hanging by his belt. As soon as he enters through the door, he pulls a rifle out of the bag and starts indiscriminately shooting at everyone in sight. [Insert name] continues to the hallways, targeting occupied parts of the building, firing an abundant amount of shots as he seamlessly pulls a new magazine and reloads as he runs out of ammo going from area to area.

People instinctively disperse away from the shooting, with many tucking themselves away in corners of the building. Some fleeing bystanders seek out law enforcement who arrive on-scene, providing varying accounts of [insert name]’s description. Moments later, additional gunshots are heard, and officers direct evacuated facility personnel to a more secure location. Reports from employees who fled the facility indicate that the assailant is an employee and state he is headed towards the east side of the facility.

In a few short minutes, officers report that [insert name] was found dead, most likely the result of a self-inflicted wound. They continue to search the rest of the facility for other assailants and begin to evacuate remaining employees.

## Discussion Questions

1. What training is available to employees on dealing with insider threats and workplace violence?
	1. Is the training mandatory to all employees?
	2. Does the training instruct employees in documenting and reporting suspicious behavior?
	3. Does the training include information and protocols for addressing workplace violence?
	4. Does the training include information and protocols for addressing destructive behavior, such as theft, vandalism, and sabotage?
	5. Does the training include information and protocols for addressing cyber threats from insiders?
	6. Do employees know who to contact with questions and concerns relating to insider threats?
2. Should any action be taken by employees who witness their co-workers engage other as described in this incident?
	1. Are plans or procedures available to guide employees in their actions / decisions?
	2. Is there a system in place for reporting signs of potentially aggressive / violent behavior in the workplace?
	3. Is there a way to report non-violent suspicious behavior?
3. Does your company have a threat management or threat assessment team to address suspicious or potentially threatening behavior?
4. Is your company familiar with federal resources available for consultation once a threat management team opens a case, such as the U.S. Secret Service (USSS) National Threat Assessment Center?
	1. What organizations would you communicate with (e.g., local law enforcement, JTTF, fusion centers, etc.)?
	2. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
	3. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
5. Should the supervisor have spent more time with other employees to ask additional questions about recent interactions with the employee?
	1. Should other employees volunteer information that concern their co-worker’s personal life?
6. What actions, if any, should the supervisor take after the meeting with the employee in the office?
	1. What actions could have been taken to reduce disruptive, threatening, or potentially violent behaviors?
		1. Should the employee’s behavior be reported to security? Should he have been escorted out and, if so, by whom?
		2. If an employee were to be terminated, what protocols, if any, are in place to rescind access to company property and information systems?
	2. Did any of the actions taken by the supervisor potentially increase workplace violence risk factors?
7. Are there counseling services available to employees who show signs of stress or aggression / violent behavior?
8. What protocols or policies does your company employ to ensure the safety of employees following a known threat from a current previous employee?
	1. Is there security on-site at your facility? Is security trained to respond to hostile or suspicious activities by employees?
	2. Who maintains decision-making authority when management is not available?
9. Are facility / company policies adequate to de-escalate this from proceeding to a violent incident? Are there any way policies could be improved?
10. Does your company employ background checks or any screening practices when selecting new employees?
11. Do facility incident response plans (e.g., site security plans, emergency action plans, emergency response plans, or other appropriate plans) contain protocol for responding to an active shooter event?
	1. Are employees trained for this type of emergency incident?
		1. Is emergency contact information made available to the call desk?
		2. What procedures are in place for sheltering-in-place and evacuation?
	2. Do owners / operators have notification systems in place to warn employees both on- and off-site during such an incident?
	3. How do you communicate with employees during an incident?
	4. What instructions will be given to the employees (e.g., evacuation, shelter-in-place, lockdown)?
	5. Is there a way to account for employees (i.e., those who reported for work that day versus those on leave)?
	6. Are there any critical operations of the facility that must be secured for safety reasons? If so, are there procedures in place for doing so in an emergency?
	7. What other life safety issues should be considered?
12. Is there security on-site at your facility?
	1. How is security trained to respond to this type of incident? What are their roles and responsibilities?
	2. Do security personnel and first responders have interoperable radios / communication? Are plans in place for agencies to communicate if they cannot communicate via radio?
	3. Is security clearly identifiable upon arrival of law enforcement?
13. Does this facility have physical security measures that may be relevant to this scenario?
	1. What types of perimeter security does this facility have (e.g., fences, doors, gates)?
	2. What types of vehicle control checkpoints are present (e.g., barriers, driveways, parking lots)?
	3. Does the public have access to the facility?
14. How is the emergency response coordinated?
	1. Are any of the facility’s incident response plans (e.g., site security plans, emergency action plans, emergency response plans, or other appropriate plans) provided to first responders in preparation for potential incidents?
		1. If not, how is the key information communicated to first responders during the response to an incident?
	2. How do emergency response personnel access the buildings?
		1. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items, such as facility map / floor plans, access swipe cards, elevator keys, etc.?
	3. Are there any safety concerns for first responders that need to be addressed (e.g., entering restricted or hazardous areas)?
	4. Have local first responders participated in exercises and / or trainings at the facility?
	5. Do you know the specific local law enforcement policies and procedures regarding active shooter incidents for your location?
15. How is emergency communication handled?
	1. Are critical telephone calls getting through? If not, is there an alternate means of communication available?
	2. How will owners / operators interact with media representatives and control media access to the facility?
	3. Are there procedures in place to manage the media when they arrive?
	4. Should additional emergency announcements be made to the public?
16. Does the facility maintain security technology that can assist law enforcement in response efforts?
	1. Can security personnel assist in locating victims and assailants via closed-circuit television or similar capabilities?
	2. Are there access control capabilities at the facility to facilitate entry of first responders, prevent entry of visitors or additional employees, and manage contractors on-site?
	3. Does the facility have the ability to remotely control access to critical components or activate / deactivate card readers, including the capability to deactivate a specific card?
	4. Is there sufficient emergency lighting capability at the facility to deal with a nighttime incident?
17. How do state and local officials coordinate when responding to an incident at the facility?
	1. Do you have memorandums of understanding (MOUs) or memorandums of agreement (MOAs) in place with any local, regional, or state response agencies?
	2. What incident response plans do local, county, and state law agencies have in place for an active shooter situation? Who leads the response?
	3. What would state and local officials need from owners / operators during an incident similar to the scenario detailed in this module?
18. Do the facility’s incident response plans cover the emergency coordination activities described in the module?
	1. How is response coordinated and who maintains decision-making authority when management is not available?
	2. Is delegation of authority outlined in the security plan or any other plan?
	3. If doors to critical facility components are locked, how does law enforcement obtain access?
	4. Is there a safe location identified for people who are evacuating the immediate area?

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 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 | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **ICS** | Incident Command System |
| **IP** | Improvement Plan |
| **JTTF** | Joint Terrorism Task Force |
| **MOA** | Memorandum of Agreement |
| **MOU** | Memorandum of Understanding |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise  |
| **USSS** | U.S. Secret Service |

