[Insert Cover Picture]

Potential Civil Unrest 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 |
| --- | --- | --- |
| 8:00 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: Information Sharing |
| 9:45 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 11:00 a.m. | Module Two: Incident |
| 11:00 a.m. | 11:15 a.m. | Break |
| 11:15 a.m. | 12:15 p.m. | Module Three: Response and Recovery |
| 12:15 p.m. | 12:30 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Potential Civil Unrest Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [exercise duration], at [exercise location]. Exercise play is limited to [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 applicable Mission Areas] |
| **Capabilities** | * Health and Social Services * Infrastructure Systems * Intelligence and Information Sharing * Mass Care Services * On-Scene Security, Protection, and Law Enforcement * Operational Communication * Operational Coordination * Planning * Public Health, Healthcare, and Emergency Medical Services (EMS) * Public Information and Warning * Risk Management for Protection Programs and Activities * [modify as needed] |
| **Objectives** | 1. Review intelligence and information sharing processes with local or regional critical infrastructure owners / operators prior to, during, and following potential civil unrest. 2. Discuss private sector stakeholders’ and their partners’ emergency preparedness plans and response procedures to potential civil unrest and the coordination with local, state, and federal agencies. 3. Examine recovery and business continuity plans and procedures following potential civil unrest at [insert facility]. 4. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Potential Civil Unrest |
| **Scenario** | Daily operations at [insert facility] are impacted by nearby protests. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable] |
| **Participating Organizations** | [Insert a brief summary of the total number of participants and participation level (i.e., federal, state, local, tribal, non-governmental organizations [NGOs], private sector, and / or international agencies). Consider including the full list of participating agencies in Appendix A. Delete Appendix A if not required.] |
| **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 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** |
| --- | --- |
| Review intelligence and information sharing processes with local or regional critical infrastructure owners / operators following potential civil unrest. | * Intelligence and Information Sharing * Planning * Public Information and Warning |
| Discuss private sector stakeholders’ and their partners’ emergency preparedness plans and response procedures to potential civil unrest and the coordination activities with local, state, and federal agencies. | * Operational Communication * Operational Coordination * Planning * Public Information and Warning * Risk Management for Protection Programs and Activities * Situational Assessment |
| Examine recovery and business continuity plans and procedures following potential civil unrest at [insert facility]. | * Economic Recovery * Health and Social Services * Operational Coordination * Planning |
| [Insert additional objectives as necessary] | * [Insert additional capabilities as necessary] |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

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

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

## Exercise Structure

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

* Module One: Information Sharing
* Module Two: Incident
* Module Three: Response 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).

# Module One: Information Sharing

## Scenario

## [Insert Location]

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

An organized protest is set to take place throughout [insert location] in the upcoming days. According to the filed public gathering request, the main roads that the protest will occupy will be close to a number of businesses, including [insert facility name].

While the organizers of the planned protest stressed that it will be a peaceful demonstration and condemn violence of all forms, the event has caught the attention of some opposing groups on various online forums, including opposing groups that have been known to incite or enact violence to further their own agendas.

Following the attention from these opposing groups, there has been a significant uptick in the number of individuals online and social media accounts who have begun posting alarming comments about the protest. Several of the posts call for individuals to rally at [insert location near facility] on the day the protest is scheduled to ‘counter’ the planned protest with several commenters stating they would show up armed.

Law enforcement noticed one such social media post, which has been shared heavily online amongst known members of opposing organizations, stating, “We will make sure these people get what’s coming to them, just like we did last month.” Included in the post is a picture from a previous demonstration that had ended in a violent altercation between opposing factions resulting in several people being grievously injured.

## Discussion Questions

1. How does your organization gather threat information?
   1. Does your organization conduct any social media monitoring?
      1. How does your organization address potential constitutional concerns with social media monitoring?
      2. How does your organization monitor social media while maintaining terms of service agreements with those respective platforms?
   2. Does your organization or a parent organization have any threat detection services?
   3. How would your organization expect to receive information about a credible threat?
2. What formal information sharing processes would your organization use at this point?
3. What resources are used to disseminate information?
   1. What notification capabilities (e.g., alerts, emails, telecom, text messages, special tools) do you use to share information and communicate the implementation of protective measures?
4. What is your organization’s risk threshold for responding to a potential threat?
5. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased patrols)?
6. How is your organization coordinating with information sharing partners (e.g., local law enforcement, Federal Bureau of Investigation [FBI], fusion centers, etc.)?
7. Who is responsible for coordinating the risk communications message for your organization?
8. What steps does your organization take once they receive notice of a possible or credible threat?
9. How does your agency or organization triage the information you receive (formal reporting, hearsay, and social media)?
10. What are the key messages that should be distributed concerning the possible 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?
11. Does your agency or organization conduct any specific training based on credible threats?
12. What security measures, if any, will private sector stakeholders employ?
13. What security recommendations, if any, are local, state, and federal law enforcement making to private sector stakeholders at this time?
14. What additional actions are local, state, and federal law enforcement agencies taking at this time?
15. What plans are in place describing the required protective measures that need to be taken prior to the event?
16. What are you communicating to your employees?
    1. Who in your organization is responsible for addressing employee concerns?
    2. How is information shared with your employees?
17. What additional notifications need to be distributed to those outside of your organization?

# Module Two: Incident

## Scenario

## [Insert Facility Name and Location]

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

[Insert facility name] is engaged in its usual daily operations. Around the early afternoon, a member of the [insert facility name] staff notices a large gathering of people walking in the direction of the facility. As the crowd moves closer, it becomes clear that the group is part of the organized protest; demonstrators are carrying picket signs and chanting with several bullhorns. The employee notices that the demonstration has steered off the official path causing traffic congestions on the roads by the facility.

The staff member alerts on-site security guards of the situation. The guards observe that the demonstration continues in a peaceful manner for some time but notify local law enforcement of the events taking place. More people seemingly join the demonstrations, pushing the crowd closer towards the building and effectively blocking the egress routes from the facility, as well as creating additional traffic congestion and blocked routes around the immediate area. Security instructs the group to back away and to move off the private property where applicable. The majority of the protestors slowly move to comply. A small cohesive group, who all appear to be wearing the same kind of face coverings [Insert distinguishing features/attire (e.g., grey bandanas, black face masks, etc.)], separates from the crowd and advances toward the facility, ignoring the security guards’ instructions.

A few of the individuals from the separated group throw items at the entrance and security staff, including large and sharp objects. A panicked voice from the main body of the demonstration is heard claiming that someone is in possession of a firearm. Security attempts to identify a weapon within the crowd, but protestors disperse in all directions in response. Several are injured in the process.

## Discussion Questions

1. Is the area immediately surrounding your facility private property or is there an accessible public space where people may congregate?
2. What protocols are in place at the facility to alert employees of an emergency?
   1. Who is responsible for enacting the emergency protocols?
   2. How are alerts sent to facility employees?
   3. What is the message that is sent to facility employees?
3. How are facility employees trained to respond to such an incident?
   1. Does the threat of a weapon impact your facility’s response protocols?
4. Does your facility have on-site security personnel?
   1. To whom do they report?
   2. What are their rules of engagement for an incident like this?
   3. How many are on-site at a given time?
   4. What steps would they take to protect facility personnel / property?
5. Does your facility have closed circuit cameras on-site?
   1. Can images / recordings be shared with law enforcement?
6. What emergency operations plan / crisis communications plan are in place at your facility?
7. What type of command structure would the responders establish?
   1. Who would be in charge of the command structure?
   2. What is the role of private sector stakeholders in this command structure?
      1. How are they trained on incident command procedures?
      2. Is there cross-training with local, state, and / or federal response agencies?
   3. Who is in charge of securing the scene?
8. How would law enforcement ensure the scene is secure?
   1. What steps need to take place to ensure the area is cleared of all other potential threats?
   2. What steps must be taken prior to engaging the perpetrators?
9. Would EMS personnel be delayed in entering the scene to assist injured participants?
   1. Does your jurisdiction have Rescue Task Force capabilities?
10. What types of crowd control procedures would be enacted?
    1. Is training conducted for these procedures? If so, how often?
    2. Would your facility encourage staff to not engage with protestors?
11. What external assets or resources are available to assist your organization and the overall response effort?
    1. Are pre-arranged agreements in place with any public or private sector organizations to provide resources? Are they formal or informal agreements?
    2. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
    3. How will this coordination and information sharing take place?
12. What communication takes place with surrounding buildings / organizations?
    1. Who is responsible for that communication?
    2. How is it communicated?
    3. Is there redundancy set up if this communication fails?
13. What public communications or warnings is your organization disseminating?
    1. Who would make decisions regarding the release of information to the public?
    2. Is there a Public Information Officer (PIO) in place?
    3. How is public messaging coordinated across the relevant stakeholders?
    4. How is your organization coordinating messages with the public sector?
    5. Who is responsible for distributing public messaging?
    6. What steps are the organization taking to provide accessible messaging for persons with disabilities?
14. Is consideration needed for those who may have limited English proficiency in the impacted area?
15. What type of social media resources are available during and immediately after an incident?
16. What measures are taken to disrupt the distribution of fake information?
17. What is the process to collect evidence that belongs to citizens (cell phone video, cameras, security footage from the private businesses, etc.)?
    1. How are these items returned to the owners?

This page is intentionally left blank.

# Module Three: Response and Recovery

## Scenario

## Location: [Insert Facility Name and Location]

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

Officers respond to the scene, securing the area and controlling the situation with the small group of individuals that were throwing items. The incident and ensuing panic left [insert number] of individuals with minor injuries lightly wounded, including some employees who were watching the demonstrations nearby, and [insert value/level] of property damage has been done to the facility / grounds. Though most of the crowd retreated, many people remain in the area, posting photos and videos of the scene on social media. Law enforcement officials conduct an on-site investigation and identify several suspects responsible for inciting or committing violence, but it is unclear if they were a part of the demonstration or a separate group sowing disorder to detract from the demonstration’s goals.

As EMS arrives and treats the wounded, uninjured security guards start to take account of the facility and property damage.

Law enforcement confirms that there were no armed individuals on-scene and believe that the report resulted from a panicked demonstrator.

Social media runs rampant with rumors and speculations about the incident. Some claim that shots were fired in the chaos. Media outlets arrive on-scene and attempt to interview protesters, employees, and first responders.

## Discussion Questions

1. What are your organization’s immediate actions / priorities?
2. If deemed necessary, does [insert facility name] have capabilities to support basic first aid / medical care to wounded victims until EMS arrives on-scene?
   1. Would your facility be able to handle minor medical emergencies if EMS was blocked from accessing your facility?
   2. How would your facility handle a major medical emergency (cardiac arrest, etc.)?
3. What types of crowd control, evacuation, and / or shelter-in-place procedures would be enacted?
   1. Who is responsible for activating the evacuation or shelter-in-place procedures?
   2. Is there a specified location for evacuees? Are there secondary or tertiary rally points in case the primary location is part of the security incident?
   3. Is training conducted for these procedures? If so, how often?
   4. If egress routes are blocked, would you encourage employees to stay on-site?
   5. Do these procedures take into consideration the needs of persons with disabilities and access the functional needs?
4. How does your organization conduct an accountability check of its employees?
5. How quickly is the incident communicated to surrounding businesses / organizations?
6. Does your organization have a formal recovery plan and, if so, does it cover this type of incident?
   1. Are there any additional measures that law enforcement would take to ensure the safety of the facility or to reassure employees?
      1. How would these measures be resourced?
   2. Who makes the decision on when the area will be reopened?
      1. How is that decision communicated to employees and the media?
7. What communication takes place between facility leadership and first responders after the incident?
   1. What other agencies / organizations need to be contacted at this time?
   2. What stakeholders are dependent upon your organization and its services?
   3. Who are the key stakeholders or groups that your facility relies upon to help restore your operations and assets?
8. What business continuity plans are in place at your facility?
   1. Does it include a crisis communications plan?
      1. If so, how would this plan be coordinated with other stakeholder’s PIOs?
      2. How and what type of messaging will be sent to employees, vendors, and customers?
      3. What training do employees receive regarding media relations and the release of sensitive information?
   2. What are the short-term recovery objectives for your organization?
   3. What are the implications of being unable to open or operate for a period of time?
      1. Given the scenario, how long would the incident area remain cordoned off for the investigation?
      2. What would the financial impact be on your facility if a building was closed resulting from such an incident and the ensuing investigation?
   4. Does your organization have the ability to move key operations to another location?
      1. If so, how long would this take?
9. What training plans are in place for the business continuity plan? Does your organization exercise these plans (other than today)? 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 following the incident?
   2. What counseling services or resources are available for employees and family members?
   3. How does your organization address leave or time-off for employees?
   4. If operations are suspended for a length of time, is there financial assistance available to employees?
   5. What are additional security measures that you put into place following this event, if any?
   6. How do you reassure employees as to their safety on the job?
   7. If any of your employees were killed or injured in the attack, how would it change your actions?
      1. What kind of assistance is available for injured employees (counseling, monetary, legal, etc.)?
      2. What kind of assistance would be available for the families of those employees who were killed (counseling, monetary, legal, etc.)?
      3. How would the loss of personnel impact your operations? What steps might be taken to adjust for, or to mitigate this?
10. How can facility owners / operators prepare to handle the public messaging / media in the aftermath of such an incident?
    1. What messaging is sent out to the media about the current situation?
    2. What and how is information conveyed to the public at this time?
    3. How will you restore public confidence?
    4. How will you resolve potential misinformation?
    5. Is social media being monitored for the spread of information that may not be accurate?
       1. Who is responsible for monitoring social media for inaccurate information concerning the incident?
       2. What procedures are in place to counter false information on social media?
    6. What steps are the organization taking to provide accessible messaging for persons with disabilities?
    7. Is consideration needed for those who may have limited English proficiency in the impacted area?
11. Would reunification centers be set up following the incident?
    1. If so, who is responsible for setting up the reunification centers?
    2. What procedures are in place for this?
    3. How are personal items reunified with their owner if left at the scene?
12. At what point would you consider the facility and all associated businesses stabilized?
    1. Who determines when it is safe for employees to return to the area?

# 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: Resources

| **Private Sector Considerations** |
| --- |
| CISA’s Protecting Infrastructure During Public Demonstrations: <https://www.cisa.gov/sites/default/files/publications/Protecting%20Infrastructure%20During%20Public%20Demonstrations_102220_FINAL_508.pdf> |
| CISA’s Protecting Patrons in Outdoor Eating Venues: <https://www.cisa.gov/sites/default/files/publications/CISA_Protecting%20Patrons%20in%20Outdoor%20Eating%20Venues_Fact%20Sheet_508.pdf> |
| U.S. Chamber of Commerce list of available resources and emergency loan guidance: [www.uschamber.com](http://www.uschamber.com) |
| The Small Business Administration (SBA) offers disaster assistance in the form of low- interest loans to businesses, renters, and homeowners: [www.sba.gov/disaster-assistance/coronavirus- covid-19](http://www.sba.gov/disaster-assistance/coronavirus-%20covid-19) |
| The SBA offers information on business insurance: <https://www.sba.gov/business-guide/launch-your-%20business/get-business-insurance> |

| **Reconstruction Planning Considerations** |
| --- |
| Continuity Guidance Circular: [www.fema.gov/continuity-guidance-circular-cgc](http://www.fema.gov/continuity-guidance-circular-cgc) |
| Federal Emergency Management Agency’s (FEMA ) National Continuity Programs (NCP): [www.fema.gov/national-continuity-programs](http://www.fema.gov/national-continuity-programs) |
| NCP’s Continuity Resource Toolkit for continuity and reconstitution tools, templates, and resources: [www.fema.gov/continuity-resource-toolkit](http://www.fema.gov/continuity-resource-toolkit) |

| **Cleaning Considerations** |
| --- |
| Centers for Disease Control (CDC) Considerations: [www.cdc.gov/coronavirus/2019- ncov/community/organizations/cleaning-disinfection.html](http://www.cdc.gov/coronavirus/2019-%20ncov/community/organizations/cleaning-disinfection.html) |
| Occupational Safety and Health Administration: [www.osha.gov/SLTC/covid-19/](http://www.osha.gov/SLTC/covid-19/) |

| **State, Local, Territorial, and Tribal Government Considerations** |
| --- |
| Department of Education COVID-19 guidance and resources: [www.ed.gov/coronavirus](http://www.ed.gov/coronavirus) |
| Department of Transportation - develop plans for ensuring public health while using public transportation: [www.transportation.gov/coronavirus](http://www.transportation.gov/coronavirus) |
| FEMA’s “Disaster Financial Management Guide” for state and local jurisdictions: [www.fema.gov/media-library/assets/documents/187126](http://www.fema.gov/media-library/assets/documents/187126) |

| **COVID-19** |
| --- |
| Coronavirus Aid, Relief, and Economic Security (CARES) Act, PL 116-136: <https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf> |
| Coronavirus Preparedness and Response Supplemental Appropriations Act, PL 116-123: <https://www.congress.gov/116/plaws/publ123/PLAW-116publ123.pdf> |
| Families First Coronavirus Response Act, PL 116-127: <https://www.congress.gov/116/plaws/publ127/PLAW-116publ127.pdf> |

| **Additional Resources** |
| --- |
| CDC Coronavirus Guidance Documents: [www.cdc.gov/coronavirus/2019-ncov](http://www.cdc.gov/coronavirus/2019-ncov) |
| Cybersecurity and Infrastructure Security Agency: [https://www.cisa.gov/coronavirus](http://www.cisa.gov/coronavirus) |
| Department of Health and Human Services Coronavirus Updates: [www.hhs.gov/about/news/coronavirus](http://www.hhs.gov/about/news/coronavirus) |
| Department of Labor “Guidelines for Preparing Workplace for Coronavirus”: [www.dol.gov/coronavirus](http://www.dol.gov/coronavirus) |
| FEMA COVID-19 Response: [www.fema.gov/coronavirus](http://www.fema.gov/coronavirus) |
| General Services Administration:  <https://www.gsa.gov/governmentwide-initiatives/emergency-response/covid19-coronavirus> |
| National Institutes of Health: [www.nih.gov](http://www.nih.gov) |
| Office of Personnel Management: [www.opm.gov/policy-data-oversight/covid-19/](http://www.opm.gov/policy-data-oversight/covid-19/) |
| Office of the Assistant Secretary for Preparedness and Response:  <https://www.phe.gov/about/aspr/Pages/default.aspx> |
| White House/CDC/FEMA COVID-19: [www.coronavirus.gov](http://www.coronavirus.gov) |
| White House “Opening Up America Again” Guidelines: [www.whitehouse.gov/openingamerica/](http://www.whitehouse.gov/openingamerica/) |

# Appendix D: 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 |
| **IP** | Improvement Plan |
| **NGO** | Non-Governmental Organization |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise |

