[Insert Cover Picture]

Election Security Potential Civil Unrest Tabletop Exercise

Situation Manual

[Insert Date]

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

This Situation Manual (SitMan) provides exercise participants with 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. | 8:00 a.m. | Registration |
| 8:00 a.m. | 8:30 a.m. | Welcome and Participant Briefing |
| 8:30 a.m. | 9:30 a.m. | Module One: Information Sharing |
| 9:30 a.m. | 9:45 a.m. | Break |
| 9:45 a.m. | 10:45 a.m. | Module Two: Incident |
| 10:45 a.m. | 11:00 a.m. | Break |
| 11:00 a.m. | 12:00 p.m. | Module Two: Scenario Update |
| 12:00 p.m. | 12:15 p.m. | Break |
| 12:15 p.m. | 1:15 p.m. | Module Three: Recovery |
| 1:15 p.m. | 1:45 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Potential Civil Unrest at Election Site 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)** | Protection, Mitigation, Response, and Recovery [Select appropriate Mission Area(s)] |
| **Capabilities** | * Health and Social Services
* Infrastructure Systems
* Intelligence and Information Sharing
* 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
* [Insert additional capabilities 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 emergency preparedness plans and response procedures to potential civil unrest at a polling location.
3. Examine collaboration and coordination between election stakeholders and local, state, and federal agencies.
4. Examine recovery and continuity plans and procedures following potential civil unrest at a polling station.
5. [Insert additional exercise objectives as needed]
 |
| **Threat or Hazard** | Civil Unrest  |
| **Scenario** | An interactive, discussion-based exercise focused on civil unrest at a polling location on Election Day that leads to a physical altercation. |
| **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 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 intelligence and information sharing processes with local or regional critical infrastructure owners / operators prior to, during, and following potential civil unrest. | * Intelligence and Information Sharing
* Planning
* Public Information and Warning
 |
| Discuss emergency preparedness plans and response procedures to potential civil unrest. | * On-Scene Security, Protection, and Law Enforcement
* Operational Communication
* Operational Coordination
* Planning
* Public Information and Warning
 |
| Examine collaboration and coordination between election stakeholders and local, state, and federal agencies. | * Intelligence and Information Sharing
* Operational Coordination
* Public Health, Healthcare, and EMS
* Risk Management for Protection Programs and Activities
 |
| Examine recovery and continuity plans and procedures following potential civil unrest at a polling station. | * Health and Social Services
* Infrastructure Systems
* Operational Coordination
* Planning
 |
| [Insert additional Objectives, as necessary] | * [Insert capability aligned to each objective, 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 the discussion. 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. [Remove for in-person exercises].
* **Data Collectors** 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 two modules:

* Module One: Information Sharing
* Module Two: Incident
* Module Three: Recovery

Each module begins with a scenario 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: Information Sharing

## Scenario

## [Insert location]

### [Insert Month, Day, Year]

Approximately two weeks prior to Election Day, the [insert county] Commissioner’s Office receives numerous reports from concerned citizens stating that members of an online social media group are planning to target voting locations within [insert county] on Election Day. The social media group is asking its members to monitor voting locations while voters are casting ballots. The group is specifically encouraging its members to watch election workers for any suspicious activity or signs of voter fraud. This includes the reporting and transfer of ballots and election equipment after voting ends.

One post forwarded to the [insert county] Commissioner’s Office states that “poll workers cannot be trusted” and encourages group members to “do what they have to do” to prevent voter fraud and ensure that ballots are counted properly. A list of polling places around [insert county] has been posted to the social media group, and a few members have stated that they plan to be armed on Election Day.

## 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 with election workers and communicate the implementation of protective measures?
	2. Who is responsible for coordinating the risk communications message for your organization?
4. What level of risk would need to be realized before your organization responds to a potential threat?
5. Would any legal issues regarding First Amendment rights arise from monitoring social media posts?
	1. What communications would you have with [insert jurisdiction] attorneys at this point?
6. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased patrols, etc.)?
7. How is your organization coordinating with information sharing partners (e.g., local law enforcement, state police, Federal Bureau of Investigation [FBI], fusion centers, etc.)?
8. What steps does your organization take once it receives notice of a possible or credible threat?
9. How does your agency or organization triage the information you receive (e.g., from 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, how is this message coordinated?
11. Does your agency or organization conduct any specific training based on credible threats?
12. What security measures, if any, will your organization employ?
13. What are the state / local laws around open carry of guns?
	1. If the law prohibits this, do you have signs upon entering the voting location that open carry is prohibited?
14. What additional actions are local, state, and federal law enforcement agencies taking at this point?
15. What is the process for election workers to escalate and report information upward to election officials? How is this information handled at each level?
16. What are you communicating to your employees and volunteers?
	1. Who in your organization is responsible for addressing polling site employee / volunteer concerns?
	2. How is information shared with your polling site employees / volunteers?
17. What additional notifications need to be distributed to those outside of your organization, including to the public?

# Module Two: Incident Response

## Scenario

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

Election Day has arrived, and [insert polling location] has had a steady stream of voters throughout the morning. After polls have been open for a few hours, a small group of people enter the building and approach the voter check-in table. The group announces that they are members of a citizens’ poll watching organization, and one man begins to record video of the election workers while asking questions about how ballots are stored, transported, and tallied. Other members of the group disperse around the voting area, inspecting voting machines. Although the election workers answer the group’s questions to the best of their ability, some of the poll watchers become agitated and are unsatisfied with the information they are given.

## Discussion Questions

1. What are your polling site’s rules for employee / volunteer engagement with voters or other individuals at the polling station?
	1. Are rules posted and publicly available?
	2. How are employees / volunteers trained to respond when those rules are broken?
2. What types of on-site security are present at your polling site(s)?
	1. To whom do they report?
	2. How many are on-site at a given time?
	3. What are the rules of engagement for an incident like this? Are they armed?
	4. What steps would they take to protect facility personnel / property?
3. What protocols exist at the facility to alert law enforcement or local officials to an incident?
	1. Who is responsible for enacting the emergency protocols?
4. How are facility employees / volunteers trained to respond to such an incident?
5. What emergency operations plan / crisis communications plan exists at your facility?
6. What communication is taking place between voting location staff, county election staff, and local law enforcement during this situation?
7. How does this situation affect voting at your facility?
8. What is your organization’s policy regarding recording devices at voting locations on Election Day?
9. How do you transport and secure ballots?
10. What type of safety and security training does your organization provide for employees and volunteers?
	1. How often does that training take place?

## Scenario Update

### [Insert Month, Day, Year]: [Insert time + 10 mins]

A few of the poll watchers begin to ask about the ballot box and demand to be given access to the ballots when the ballot box is opened after the polls close. An election worker explains that the poll watchers are not provided access to the ballot box or the ballots nor are they allowed to touch any of the election materials. They are solely allowed to observe and not interfere. The election worker informs them that their antics constitute interference in the voting process and asks the group to leave the property.

Members of the group begin yelling about “voter fraud,” claiming voters are using illegitimate ballots. The group refuses to exit the building. One man approaches a voting machine and attempts to pry open the ballot box. When a poll worker tries to pull him away from the machine, he aggressively shoves the worker. Other members of the group become rowdy, flipping tables and aggressively yelling at and confronting voters who are still in the building.

## Discussion Questions

1. What are your organization’s immediate priorities during this incident?
2. What type of command structure would the responders establish?
	1. Who would staff each level of the structure?
		1. How are they trained on incident command procedures?
		2. Is there cross-training with local, state, and / or federal response agencies?
3. 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?
4. 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 poll workers to stay on-site?
	5. Do these procedures take into consideration the needs of persons with disabilities and access and functional needs?
5. If deemed necessary, does the polling station have capabilities to support basic first aid / medical care to wounded victims until EMS arrives on-scene?
	1. Can your facility handle minor medical emergencies if EMS were blocked from accessing your facility?
6. Can other voting locations assist or provide resources to the affected location and the overall response effort? Are there other public or private sector resources?
	1. How does this incident affect the operations and security measures at other voting locations?
	2. Are there pre-arranged agreements with any public or private sector organizations to provide resources? Are they formal or informal agreements?
	3. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
	4. How will this coordination and information sharing take place?
7. What public communications or warnings about the situation at the voting location is your organization disseminating and sharing with the public, if any?
	1. Who would make decisions regarding the release of information to the public?
	2. Is there a public information officer (PIO) in place?
	3. Who is responsible for distributing public messaging?
8. What communication is taking place with other voting locations?
	1. Who is responsible for that communication?
	2. How is it communicated?
	3. Is there redundancy set up if this communication fails?
9. What type of social media resources are available during and immediately after an incident?
10. What measures are taken to disrupt the distribution of misinformation / disinformation?
11. How are ballots, voting machines, and other sensitive materials secured during this situation?

This page is intentionally left blank.

**Module Three: Recovery**

**Scenario**

**[Insert Month, Day, Year]: [Insert Time + 1 hour]**

Law enforcement secured the scene and arrested those responsible for the unrest. Tables, chairs, privacy stations, ballots, and an assortment of other items are strewn across the floor at the polling station. There has been damage to [insert number] voting machines, and they are no longer operational. The panic has also left [insert number] people with minor injuries, including both voters and election workers. The aggressors who were not arrested have left the property, and only a small number of voters remain at the voting station.

The remaining voters begin to ask how they should proceed with voting, as there are several hours left before the polls are supposed to close. Rumors and speculation about the incident run rampant on social media, including numerous posts urging people to stay away from the voting location and concerns about possible ballot tampering. Local media outlets dispatch reporters to the scene to interview witnesses and capture footage of the area.

**Discussion Questions**

1. What are your immediate actions / priorities?
2. Is there a formal recovery plan for disruptions to voting operations and, if so, does it cover this type of incident?
	1. Does your organization have an identified backup location to continue voting operations if the original location is compromised?
		1. Who is responsible for making the decision to reopen the original location or move to a backup location?
	2. Are there any additional measures that law enforcement would take to ensure the safety of the facility or to reassure employees?
	3. Who makes the decision on when the area will be reopened?
		1. How is that decision communicated to poll workers, voters, and the media?
3. How would your command structure change at this point?
4. What is the standard operating procedure for handling damaged voting machines?
	1. What are the implications for completed ballots that are stored in these machines?
	2. Can damaged machines be repaired on-site, or will they need to be transported to a secondary location? Are there replacement machines available on-site or nearby?
	3. Does your county have post-election audit requirements to validate the accuracy of the reported results?
5. What communication takes place between voting location leadership and first responders after the incident?
	1. What other agencies / organizations need to be contacted at this time?
	2. Who are the key stakeholders or groups that your facility relies upon to help restore your operations and assets?
6. How quickly would this facility be able to return to normal operations?
	1. What counseling services or resources are available for employees and volunteers?
7. Does your organization have a crisis communications plan?
	1. What type of messaging will be sent to election workers, voters, and the media in the days following the incident?
	2. What training do employees and volunteers receive regarding media relations and the release of potentially sensitive information?
	3. How will you restore public confidence in coming to this polling station and other polling locations?
	4. 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 exist to counter false or misleading information on social media?
8. Are there established continuity of operations plans for private sector stakeholders and businesses that normally operate in the affected location?
	1. How is information communicated to private sector employees following the incident?
	2. What additional security measures would be put in place following this incident, if any?
	3. How would you reassure employees, volunteers, and voters that it is safe to return to polling stations?
9. What plans, if any, do you have to return personal items left at the scene to their owners?
10. At what point would you consider the situation stabilized?
	1. Who determines when it is safe for employees, volunteers, and voters to return to the voting location?

# 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: Maps and Sample Alerts

[Insert relevant maps or alerts used to supplement the exercise.]

This page is intentionally left blank.

# Appendix C: Reference List

## CISA Election Security Resources

* [CISA Election Security Reference Page](https://www.cisa.gov/election-security)
* [CISA Election Security Training Video Series](https://www.youtube.com/playlist?list=PL-BF3N9rHBLLv_JTmmPqVWWrMgFFUCiuf)

## [Insert state / local] Resources

*\*as applicable*

This page is intentionally left blank.

# 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 |
| **PIO** | Public Information Officer  |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert  |
| **TTX** | Tabletop Exercise  |

