[Insert Cover Picture]

Election Security Insider Threat 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 |
| --- | --- | --- |
| 7:30 a.m. | 8:00 a.m. | Registration |
| 8:00 a.m. | 8:30 a.m. | Welcome and Participant Briefing |
| 8:30 a.m. | 8:45 a.m. | Ground Truth |
| 8:45 a.m. | 9:45 a.m. | Module One: Incident Response |
| 9:45 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 11:00 a.m. | Module Two: Short-Term Recovery |
| 11:00 a.m. | 11:30 a.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Election Security 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 National Preparedness Goal Mission Area(s)] |
| **Capabilities** | * Access Control and Identity Verification * Infrastructure Systems * Intelligence and Information Sharing * Interdiction and Disruption * On-Scene Security, Protection, and Law Enforcement * Operational Communication * Operational Coordination * Planning * Public Information and Warning |
| **Objectives** | 1. Review intelligence and information sharing processes with local and regional critical infrastructure owners / operators prior to, during, and following an insider threat incident. 2. Examine collaboration and coordination between election stakeholders and local, state, and federal agencies. 3. Discuss plans and procedures following an incident with a focus on agency / organizational recovery and business continuity. |
| **Threat or Hazard** | Insider Threat / Suspicious Activity |
| **Scenario** | An interactive, discussion-based exercise focused on agency / organizational recovery and business continuity. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise 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 and regional critical infrastructure owners / operators prior to, during, and following an insider threat incident. | * Access Control and Identity Verification * Intelligence and Information Sharing * Interdiction and Disruption * Operational Communication * Operational Coordination * Planning * Public Information and Warning |
| Examine collaboration and coordination between election stakeholders and local, state, and federal agencies | * On-Scene Security, Protection and Law Enforcement * Operational Communication * Operational Coordination * Planning * Public Information and Warning |
| Discuss plans and procedures following an incident with a focus on agency / organizational recovery and business continuity. | * Infrastructure Systems * Operational Communication * Operational Coordination * Public Information and Warning |
| [Insert additional objective, 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: Incident Response
* Module Two: Short-Term 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.

# Ground Truth

### Three Months Prior to Election Day

In recent months and as a new election season approaches in the United States, election officials are leaving the industry for other opportunities or retiring due to a severe uptick in election-related stress and threats targeting election workers.

Election officials have increasing concerns of insider threats to election security, as new people are hired and appointed to fill election-related job vacancies. While some new hires, seasonal workers, and volunteers may unintentionally present insider threats to election security due to a lack of training and institutional knowledge, there is also a threat of nefarious actors seeking to fill such positions.

This page is intentionally left blank.

# Module One: Incident Response

## Scenario

## [Insert location]

### [Insert Month, Day, Year]: One Week Prior to Election Day

Election jurisdictions across the country are preparing for the election. Election workers take their respective oaths of office and are reminded that it is their duty to remain politically neutral while working to ensure election integrity. During poll worker training, election workers are also taught about the circulating social media threats directed toward voting locations, stories involving election integrity in the media, and the overall tense environment surrounding election security.

Later in the week, the [insert state] election office receives anonymous reports of unauthorized access to election equipment in [insert Election Jurisdiction]’s election offices. Importantly, this office location contains the election management system (EMS) that aggregates the election results. Following initial investigation and fact finding, camera footage reveals that a temporary employee gave official election observers a tour of the election office after the public logic and accuracy test and after the office was closed for the day.

At one point in the security footage, a member of the tour is seen breaking away from the main group and appears to insert a USB flash drive into one of the EMS computers. After numerous attempts, the individual was unsuccessful in logging into the password-protected computer and rejoined the tour. The election official does not appear notice the individual’s absence and proceeds to finish the tour.

## Discussion Questions

1. How would your organization expect to receive information about a credible threat?
   1. Are these information sharing processes formal or informal?
   2. How does your organization triage this information (e.g., from formal reporting, hearsay, social media, etc.)?
   3. What steps does your organization take once they receive notice of a possible or credible threat?
   4. What local, state, and / or federal partners does your organization collaborate with when potential threat information is received?
2. What is your jurisdiction’s process for reporting suspicious activity surrounding the election process?
   1. Are staff, election workers, vendors, etc. trained on whistleblower laws, rules, and protections?
3. How would an insider threat allegation or incident be investigated?
4. How does your organization / jurisdiction prioritize transparency among its election staff?
   1. How would this transparency extend to the public for an insider threat incident?
5. What plans exist describing the required protection and detection measures that need to be taken at your election offices throughout the year (e.g., tampering, disruption, etc.)?
   1. Do these security measures change as Election Day nears?
6. Does your election office have a continuity of operations plan (COOP)? If so, how would you use it to respond to this situation?
7. How are access credentials given to election officials or workers?
   1. For individuals with election office access privileges, what security screenings, if any, must they pass?
   2. Are background investigations conducted on election workers before Election Day?
   3. What sort of physical security measures exist to prevent unauthorized access to voting systems?
   4. What sort of tracking measures, digital or paper based, monitor and audit system access?
   5. What information technology (IT) security measures exist for your voting systems?
8. What is your election office communicating to your election workers?
   1. Who in your organization is responsible for addressing election worker concerns?
   2. How is this information distributed (e.g., phone tree, dashboard, etc.)?
9. How would law enforcement and security partners such as CISA, be factored into the response of this breach, if at all?
10. How and when are you coordinating with your local / county attorney?
11. Does your state have laws against tampering with equipment that is used for official election business? If so, what are these laws, and what are the consequences for breaking them?
12. What legal reporting requirements govern information sharing to the public during this type of incident?
13. At this point, what additional notifications need to be distributed to those outside of your organization?
    1. What notifications, if any, are given to the media?
    2. What notifications, if any, are given to the public?
    3. Who is responsible coordinating and disseminating these notifications?
14. What additional actions are local, state, and federal organizations taking at this point?

# Module Two: Short-Term Recovery

## Scenario

### [Insert Month, Day, Year]: 72 hours Prior to Election Day

The [insert chief state election official] notifies the [insert local election office] of the unauthorized tour and attempted EMS breach. The temporary employee is terminated and [insert local election office] and [insert local law enforcement agency] question him. The [insert local election office] confirms the EMS does not have any signs of compromise.

While election and voting operations are expected to continue as planned, other election workers hear about the incident and begin asking election office staff about consequences the incident may have on election integrity. Rumors and speculation about the breach begin to spread on local news and social media platforms, leading many members of the public to question the integrity of the outcome of the election.

## Discussion Questions

1. What are the standard operating procedures (SOPs) for protecting, detecting, and recovering from an attempted unauthorized access to EMS, or to tampered EMS or voting systems that has been tampered with?
   1. How would your organization confirm a breach has not impacted the EMS?
   2. In the event of a breach, how would your organization secure the EMS?
   3. Does your organization have policies to reconfigure EMS to ensure integrity?
2. What codes of conduct, rules of engagement, or binding documents are election workers held to and what repercussions are included in that doctrine?
   1. What policies or procedures exist to suspend or terminate an election worker found to be in violation of these terms?
   2. Would this suspension include additional restrictions for future election involvement? How is that enforced?
3. How would background checks for election workers for upcoming elections change, if at all?
   1. Based on the attempted breach, would there be further election office access credential limitations?
4. What are the investigative priorities for the local election office?
   1. Would there be a local law enforcement integration into this investigation?
   2. Would the Secretary of State (SoS) office our any other state agencies assist with this investigation?
   3. Would federal partners assist with this investigation?
5. What messaging is being released to the public about the unauthorized tour and attempted breach?
   1. Is this messaging coordinated through a public information officer (PIO) and / or local law enforcement?
6. How will your organization restore public confidence in securing access of the election office and EMS computer?
   1. Are legal measures helping restore public confidence? How so?
7. How is your organization responding to media inquiries?
   1. Who is responsible for coordinating media relations?
8. Is your organization monitoring social media?
   1. Who is responsible for monitoring inaccurate information?
   2. What procedures exist to counter false or misleading information?
9. How would this incident affect protective and detection measures for your organization or with the election office moving forward?
10. At what point would your organization consider the situation fully stabilized?

**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: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **COOP** | Continuity of Operations Plan |
| **CTEP** | CISA Cybersecurity Tabletop Exercise Package |
| **EMS** | Election Management System |
| **EPT** | Exercise Planning Team |
| **IP** | Improvement Plan |
| **IT** | Information Technology |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **SoS** | Secretary of State |
| **TTX** | Tabletop Exercise |

