[Insert Cover Picture]

Small Unmanned Aircraft System / Improvised Explosive Device Airport 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 |
| --- | --- | --- |
| 9:00 a.m. | 9:30 a.m. | Welcome and Introductions |
| 9:30 a.m. | 10:15 a.m. | Module One: Intelligence and Information Sharing |
| 10:15 a.m. | 10:30 a.m. | Break |
| 10:30 a.m. | 11:15 a.m. | Module Two: Incident Response |
| 11:15 a.m. | 11:30 a.m. | Break |
| 11:30 a.m. | 12:15 p.m. | Module Three: Recovery and Business Continuity |
| 12:15 p.m. | 12:30 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Small Unmanned Aircraft System (sUAS) / Improvised Explosive Device (IED) Airport 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** | * Intelligence and Information Sharing * Physical Protective Measures * Planning * Public Information and Warning * On-scene Security, Protection, and Law Enforcement * Operational Coordination * Risk Management for Protection Programs and Activities |
| **Objectives** | 1. Examine threat and incident information sharing, notification systems, and alert procedures between public and private sector partners, including public messaging protocols. 2. Examine operational coordination using Incident Command System (ICS) concepts during a multi-agency, multi-jurisdictional response to an sUAS incident. 3. Examine public and private organization response procedures, interaction, and public relations collaboration during an sUAS incident. 4. Discuss recovery and business continuity plans in the wake of an sUAS incident. 5. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | sUAS-based attack |
| **Scenario** | An interactive, discussion-based exercise focused on an active threat involving an sUAS device and IED incident. The scenario consists of three modules: Intelligence and Information Sharing, Incident Response, and 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 B.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine threat and incident information sharing, notification, and alert procedures between public and private sector partners, including public messaging protocols. | * Intelligence and Information Sharing * Operational Communication * Operational Coordination * Planning * Public Information and Warning * Situational Assessment |
| Examine operational coordination using ICS concepts during a multi-agency, multi-jurisdictional response to an sUAS incident. | * Operational Communication * Operational Coordination * Planning * Public Health, Healthcare, and Emergency Medical Services (EMS) |
| Examine public and private organization response procedures, interaction, and public relations collaboration during an sUAS incident. | * Operational Coordination * Planning * Public Information and Warning |
| Discuss recovery and business continuity plans in the wake of an sUAS incident. | * Economic Recovery * Operational Coordination * Planning |
| [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** 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.
* **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 three modules:

* Module One: Intelligence and Information Sharing
* Module Two: Incident and Response
* Module Three: Recovery and Business Continuity

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

# Module One: Intelligence and Information Sharing

## Scenario

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



Based on recent sUAS threats in the United States and internationally, and increased intelligence reporting calling for similar sUAS-based attacks, the Secretary of Homeland Security, in coordination with other federal entities, issues an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against the United States. There is no specific information at this time that would warrant the release of an “Imminent” threat alert.

The alert states the threat is from domestic, U.S.-based terrorist groups with ties to international terrorist organizations. These groups are focused on mass gatherings, particularly at transportation hubs, airports, and rail systems. Additionally, the alert indicates that these terrorists are using commercially available sUASs equipped with IEDs. The alert is to remain in place for three months, ending on [insert date + 3 months].

## Discussion Questions

1. How would your organization expect to receive an NTAS alert?
   1. Does your organization subscribe to NTAS alerts, including subsequent updates to the threat?
2. Does your organization have a contact at federal, state, or local intelligence and information centers / fusion centers?
   1. What experience does your organization have working with local intelligence centers?
   2. How is information shared among multiple local and federal law enforcement agencies at an airport?
3. Does your organization maintain a relationship with your Federal Aviation Administration (FAA) Law Enforcement Assistance Program (LEAP) agent? If so, do you have a rapid means of contacting them?
4. Has your airport revised, is it currently revising, or does it plan to revise its airport emergency plans to comply with the FAA’s “Updated Guidance for Airport Emergency Plans (AEP) under 14 Code of Federal Regulations (CFR) Part 139.325(b)(7)” dated 9/21/2021?
5. Has your airport undergone a UAS-specific Joint Vulnerability Self-Assessment through the Transportation Security Administration (TSA) Federal Air Marshall Service?
6. How is the alert communicated to the departments within your organization? How do departments distribute this information?
7. What trainings, if any, does your organization conduct based on general or credible threats?
   1. Is there any specific training or briefing conducted for sUAS threats?
   2. How often do employees take this training?
   3. How often is this training re-evaluated to account for evolving threats and developments in technology?
8. Do your existing plans, policies, and procedures address counter-IED (C-IED) considerations? If so, how?
   1. How often are these plans updated?
   2. If not, are you familiar with the resources available through the Department of Homeland Security (DHS) Office of Bombing Prevention to assist in incorporating C-IED measures into planning efforts?
9. Do your existing plans, policies, and procedures address sUAS threats?
   1. How often are these plans updated?
   2. If not, are you familiar with the resources available through CISA’s sUAS Security Program to assist in incorporating sUAS measures into planning efforts?
10. How is the NTAS information shared with the customers who use your facility, especially private sector partners such as vendors, rental car hubs, restaurants, etc.?
11. Is the NTAS information shared with external stakeholders? If so, how is it shared?
    1. What do they do with this information?
12. How is this information shared with other tenants near your facility? What do these businesses do with this information?
13. Are there any other stakeholders outside of your organization who would need to be notified based on this information? If so, who?
14. What kind of messaging, if any, would be released to the public?
    1. Who oversees this messaging?
15. How would your actions change if the threat specifically mentions facilities like yours?

# Module Two: Incident Response

## Scenario

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

During an international commercial fight operation, the pilot of [insert airline company and flight number] originating from [insert country and airport] observes an sUAS enter the flight path approximately 1000 feet from the runway. Simultaneously, an air traffic controller notices the sUAS flying near the commercial aircraft. The pilot executes a missed approach safety maneuver and reports that the sUAS quickly gained speed and appeared to target the aircraft.

## Discussion Questions

1. What are your organization’s / agency’s immediate priorities at this point?
2. What actions would airport operations take upon hearing reports of an sUAS sighting?
   1. What applications exist to streamline communication between airport security and local law enforcement during an emergency?
   2. Is there a notification system for civilians in the area to relay important information, including rally points during an emergency? If so, what is it and who is responsible for sending out those communications?
3. Are there any added risks of an sUAS threat given the location or significance of this airport?
4. If there is identified “suspicious behavior” observed at your airport, how does the staff report this information to law enforcement officials and other members of your organization?
   1. Are suspicious activity trends tracked nationally across your sector?
   2. Are your employees trained in “See Something, Say Something” practices?
5. What are your organization’s suspicious activity reporting (SAR) protocols?
   1. Does your organization provide SAR training for all employees?
6. Which law enforcement entities will receive the sUAS sighting report?
   1. Who is responsible for disseminating this information?
   2. What information will you gather on the aircraft (e.g., size, color, markings, potential operator location, and speed / altitude / vector information)?
   3. Who, if anyone, would be responsible for maintaining visual contact of the device?
      1. How will this person maintain visual contact?
7. Does your agency or department have or have access to sUAS detection, tracking, identification, or mitigation capabilities? How are they integrated into your emergency operations center (EOC) to ensure synchronization of response effort?
   1. If you have access to another organization’s capability, what are the procedures for requesting that capability?
   2. Are you aware of the Counter-UAS (C-UAS) Request for Assistance Process where your organization may request C-UAS support from DHS in the event of an emergency?
8. What, if any, are your prevention, mitigation, and response procedures to a UAS threat?
9. What are the authorities; federal, state, or local laws; or protection capabilities your facility or law enforcement partners employ in immediate response, investigation, or prosecution of civil or criminal penalties?
10. As information inevitably goes up on social media, how is any potentially misleading information mitigated?
11. Does your event site or event organizer use an sUAS for operational purposes, and is it integrated into your incident response? How is it integrated?
12. Does the first responding agency or law enforcement agency supporting the airport plan to employ C-UAS technology? If so, what technology?

## Scenario Update

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

In addition to the sighting from the pilot, an air traffic controller reports an additional sUAS that has landed on the main terminal ramp. Meanwhile, a 9-1-1 caller reports seeing multiple sUASs near the airport, and the air traffic control (ATC) tower confirms sighting two sUASs in and around the runway. Patrons looking out the windows at the airport spot an sUAS and begin waving and recording it on their cell phones. One patron notices that the sUAS appears to be carrying a package with exposed wires, but within moments the sUAS flies away.

As travelers continue to arrive at the [insert terminal] entrance, some notice an sUAS hovering above the entrance and call for security. A few curious employees and travelers begin to gather around the sUAS as it lands. Suddenly, the sUAS explodes, causing panic as people flee from the entrance.

## Discussion Questions

1. What protocols exist at your airport to alert emergency management officials to this type of incident?
   1. Who is responsible for sending out the alert or warning?
2. Do any standard operating procedures (SOPs) include roles and responsibilities for airport staff? If so, what are they?
3. What level of security / law enforcement would be on-site during normal operations?
   1. How are these officers trained to respond to these types of incidents?
4. What actions are on-scene security and law enforcement taking in response to the suspicious sUAS / IED threats?
   1. What information would be conveyed to the airport employees and security personnel?
   2. How would this information be shared?
5. How quickly could additional support, such as K-9, bomb squads, or state and federal resources be brought to the scene?
6. What are crowd control and / or evacuation procedures for an incident of this type?
   1. Who is responsible for activating the evacuation procedures?
   2. Is there a specified location for evacuees?
      1. Would this location change in the event of inclement weather?
      2. Are there secondary or tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
   3. Are operations staff trained in the evacuation procedures?
   4. Are local responders familiar with your emergency procedures?
      1. Are they trained for scenarios like this?
   5. How are the travelers notified of the evacuation plan once the plan is set in motion?
7. Would your organization take accountability for the staff working at the event, and, if so, how?
8. What command and control considerations would be taken at this point in the response?
9. Would fire and EMS personnel be delayed in entering the scene to assist patrons who require assistance? Why or why not?
   1. What are the potential delays that could result?
      1. How would they be mitigated?
10. How quickly are messages being released to the public?
    1. Who is responsible for this type of messaging?
    2. How is it being released?
    3. How are messages coordinated across the different agencies and organizations?
    4. How would you notify nearby critical infrastructure partners and other federal agencies interested in sUAS reporting?
11. What plans or procedures exist to work with those with access and functional needs?
12. What is the role of private sector stakeholders in this command structure?
    1. Are they trained on incident command procedures?
    2. Is there cross-training among private and public sector responders?
    3. Does your organization have representation within the EOC or the Unified Command?
13. How would your organization or business distribute messaging to your employees?
    1. To patrons or customers?
    2. How would you distribute patron and customer messaging?
    3. Would you coordinate it with any other businesses?
    4. Does your organization have an identified Public Information Officer (PIO)?
       1. If so, does your PIO have any experience working with other organization’s or first responders PIOs?

## Scenario Update

### [Insert Month, Day, Year]: [Insert Time + 15 Minutes]

As initial response continues, law enforcement locates an individual near [insert a nearby location] with multiple controlling devices and one sUAS in his possession matching the descriptions people reported. Law enforcement detains the individual and confiscate all materials.

Local law enforcement is responding to the incident and begins securing the scene, sweeping the area for any potential secondary threats. Additional reports of other sUAS have been called into the airport and 9-1-1.

## Discussion Questions

1. What actions are local, state, and federal law enforcement agencies taking at this point?
2. What procedures are taken to stand up an EOC?
   1. Who would lead the establishment of an EOC?
   2. What agencies / organizations are included in EOC operation?
   3. How would your agency / organization integrate into the EOC?
3. How would a second explosion impact response agencies’ priorities?
4. If the cellular network is overwhelmed, does that affect your warning procedures?
   1. What communication redundancies does your organization / agency have established?
   2. Are all pertinent individuals aware of and included in these redundancies?
5. As information inevitably goes up on social media, how is any potentially misleading information mitigated?
6. How would an incident such as this impact airport operations?
   1. Would other flights be cancelled?
   2. Would other parts of the airport be shut down or just the terminal that was targeted?
   3. Who is responsible for making this decision?

This page is intentionally left blank.

# Module Three: Recovery and Business Continuity

## Scenario

### [Insert Incident + 12 Hours]

Preliminary reports are coming in from law enforcement, with [insert number] people killed or injured in the explosion and subsequent stampede. Reports of an attack at [insert airport] are flooding local media news desks as the public begins self-reporting the incidents.

Following the initial response, the community has turned to short-term recovery procedures. Businesses and organizations are executing continuity of operations plans, while families continue looking for lost loved ones. The media continues to contact a variety of organizations looking for any additional information, and elected officials throughout the state are being briefed on the situation. Customers are calling different airlines asking about safety measures and some are trying to cancel their upcoming flights because of fears about the security of the airport.

## Discussion Questions

1. Does your organization or business have a continuity of operations plan? If so, what does it entail?
   1. Would it be enacted for a situation like this?
   2. Who is responsible for enacting these plans?
2. How would your organization’s physical security be compromised in the aftermath of an IED attack?
   1. Is there a plan to mitigate or protect against future sUAS threats after this incident?
   2. How would your organization mitigate cyber-related physical infrastructure damage, such as communication lines or electronic security / access points?
3. What are your organization’s immediate recovery priorities following an IED detonation?
4. Are there established contracts to assist in the cleanup of the area prior to reopening? If so, what are they?
5. What impact would the incidents have on an airport such as this?
   1. Would travel be redirected?
   2. If the search for the sUAS operator was prolonged or sUASs harassed the airport for a prolonged period, is there a plan to handle impacted flights for a lengthy amount of time?
6. What would the financial impact be on your organization if the airport closed because of such an incident?
7. Would your business close because of these incidents? If so, for how long?
   1. How would the incident affect businesses in the area that weren’t directly involved in the incident?
   2. Would your organization change its physical or cybersecurity practices based on this incident?
8. At what point would you consider the airport and all associated organizations or businesses stabilized and back to steady state?
   1. Who makes the decision on when the area is safe and will be reopened for regular operations after the incident?
   2. How is that decision communicated to the public and the media?
9. Is social media being monitored to maintain awareness of information spreading that may not be accurate? If so, by who?
   1. What procedures exist to counter false information spreading on social media?
10. Is there personnel in charge of communicating with law enforcement post-incident? Who is responsible for this?
11. Who is responsible for communicating with local, state, or federal elected officials?
12. Does your organization have procedures for reuniting individuals with possessions they may have left behind? What are these procedures?
    1. Would family assistance or reunification centers be set up immediately following any incident?
    2. Who is responsible for this?
    3. What procedures are in place for this?
    4. How are families made aware of where to go?
13. Does your organization or business have mental health services available for your employees? If so, what are they?
    1. Is there an SOP for passengers and patrons that the incident impacted?
    2. How would available services be communicated to them?
14. How will your organization address lost or damaged personal items resulting from the IED explosion?
15. Based on your vulnerability assessment and security plan, were you able to determine if your existing plans have gaps? How would you fill those gaps?
16. Do procedure or resources exist to set up memorials following a mass casualty event? If so, what are they?

# 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 |
| **AEP** | Airport Emergency Plans |
| **ATC** | Air Traffic Control |
| **CFR** | Code of Federal Regulations |
| **C-IED** | Counter-Improvised Explosive Device |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **C-UAS** | Counter-Unmanned Aerial System |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **AEP** | Airport Emergency Plan |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **FAA** | Federal Aviation Administration |
| **ICS** | Incident Command System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **LEAP** | Law Enforcement Assistance Program |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SAR** | Suspicious Activity Report |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **sUAS** | Small Unmanned Aircraft System |
| **TSA** | Transportation Security Administration |
| **TTX** | Tabletop Exercise |

This page is intentionally left blank.

