[Insert Cover Picture]

Small Unmanned Aircraft System Improvised Explosive Device Nefarious Intent 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 |
| --- | --- | --- |
| 8:30 a.m. | 9:00 a.m. | Registration |
| 9:00 a.m. | 9:15 a.m. | Welcome and Participant Briefing |
| 9:15 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. | 11:30 a.m. | Module Two: Incident and Response |
| 11:30 a.m. | 11:45 a.m. | Break |
| 11:45 a.m. | 12:45 p.m. | Module Three: Recovery and Business Continuity |
| 12:45 p.m. | 1:00 p.m. | Hot Wash |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Small Unmanned Aircraft System (sUAS) Improvised Explosive Device (IED) Nefarious Intent 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
* On-Scene Security, Protection, and Law Enforcement
* Operational Coordination
* Physical Protective Measures
* Planning
* Public Information and Warning
* 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) / National Incident Management System (NIMS) concepts during a multi-agency, multi-jurisdictional response to an sUAS incident.
3. Examine public and private sector organization’s 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. 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 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 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 systems, 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 / NIMS 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 sector organization’s 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 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** 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: 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 attacks in the United States and internationally, and increased intelligence reporting calling for similar 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. For more information, please see **Appendix A.**

The alert states that the threat is from domestic terrorist groups in the United States with ties to international terrorist organizations. These groups are focused on mass gatherings, particularly at sports venues and sporting events. 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 and subsequent updates on the threat?
2. Does your organization subscribe to NTAS alerts?
3. Does your organization have experience working with local intelligence and information centers / fusion centers?
	1. Does your organization have a current contact at federal, state, or local intelligence and information centers?
4. Does your organization maintain a relationship with your Federal Aviation Administration (FAA) Law Enforcement Assistance Program (LEAP) agent?
	1. If so, do you have a rapid means of contacting them?
5. How is the alert disseminated to the departments within your organization? What do the department heads do with this information?
6. Does your organization have an emergency action plan (EAP) that addresses both natural and man-made threats and hazards?
	1. Does the EAP address sUAS threats?
	2. How often is the EAP updated?
	3. Do public safety officials review the EAP? Do they receive a copy?
	4. How are updates to the EAP communicated to your staff?
7. Does your organization conduct any specific training based on general or credible threats?
	1. Does your organization conduct training catered to both cyber and physical threats?
	2. Is there any training conducted specifically for sUAS threats?
	3. How often do employees take this training?
	4. How often is this training re-evaluated to account for evolving threats and developments in technology?
8. How is NTAS threat information or threat information from other sources shared with the customers who use your facility?
9. Is this information shared with external stakeholders? If so, how is it shared?
	1. What do external stakeholders do with this information?
10. How is this information shared with other businesses near your facility? What do these businesses do with this information?
11. How would your actions change if the threat were specific to large stadiums and arenas in your state?
	1. How would your actions change if the threat specifically mentions facilities like yours?
12. Are there any other stakeholders outside of your organization who would need to be notified based on this information? If so, who?
13. What kind of messaging, if any, would be released to the public?
	1. Who oversees this messaging?

# Module Two: Incident and Response

## Scenario

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

Thousands of people are gathered in your community’s town center to watch a local 5k race and cheer on the participants. As the first runners approach the final turn, spectators notice an sUAS flying over the crowd that has amassed near the finish line. As the runners get closer, it starts to bob and weave strategically, dipping down toward them as they veer out of the way.

A camera operator from the local media notices that the sUAS appears to be carrying a payload comprised of an unknown item. Some spectators record the incident on their cell phones and post videos of it on social media. After a few minutes, the sUAS flies away, and spectators go back to watching the race. Halted runners continue towards to the finish line.

## Discussion Questions

1. What actions would event organizers take upon hearing reports of an sUAS sighting?
	1. Are event organizers aware of sUAS security risks and trained on the proper way to communicate with and support law enforcement response?
	2. Are there any applications in place to streamline communications between staff and law enforcement during an emergency? If so, what are they?
	3. Is there a notification system to alert participants to any important information, including rally points during an emergency? If so, what is it, and who is responsible for sending out those communications?
	4. Are emergency protocols and resources (e.g., warning flyers, posters, etc.) made available to race participants? What kinds of resources are available to participants and attendees?
2. Which law enforcement entities will receive the sUAS sighting report?
	1. How would your sightings be reported?
	2. What information will you gather on the aircraft (e.g., size, color, markings, potential operator location, and speed / altitude / vector information)?
	3. Who would be responsible for maintaining visual contact, if anyone?
		1. How will visual contact be maintained?
3. What prevention, mitigation, and response procedures do your security and emergency response plans mandate regarding the incident?
	1. Do prevention and mitigation procedures include the use of sUAS detection technology before or during the event? Does this technology have geofencing capabilities?
	2. Do prevention procedures include applying for a Temporary Flight Restriction (TFR) for the area around the event?
	3. Do prevention procedures include conducting a site assessment to identify potential launch points (e.g., nearby parking lots or open fields where operators may launch from)?
4. As information inevitably goes up on social media, how is any potentially misleading information mitigated?
	1. Is there a designated person responsible for mitigating this information?
5. Does your event site or event organizer use an sUAS for operational purposes, and is it integrated into your incident response?
6. Would you use your sUAS to investigate? Does your agency or department have sUAS detection capabilities?
	1. How would you integrate you sUAS into your emergency operations center (EOC) to ensure synchronization of response effort?
7. Do you have sUAS detect, track, and identify (DTI) capabilities? If so, what are they?
	1. Are there measures to capture an unrecognized sUAS?

## Scenario Update

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

Some fans begin pointing upwards into the sky as they notice the sUAS come back into view, hovering above the crowd. Many fans begin waving at the sUAS and recording it on their cell phones when it begins to make a controlled descent towards the crowd. Fans begin to gather around the sUAS when it lands, and none of the fans seem to notice that the sUAS appears to be carrying a misshapen package with wires leading to a cell phone. Suddenly, the sUAS explodes, causing panic as people flee from the gate.

Preliminary reports are coming in from police and security, with [insert number] people killed or injured in the explosion and subsequent stampede. Reports of an attack at [insert your facility / location] are starting to show up on all forms of social media. Local law enforcement is responding to the incident and begins securing the scene, sweeping the area for any potential secondary threats.

## Discussion Questions

1. What protocols exist at an event such as this to alert participants or local organizations 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 event staff?
3. What level of security / law enforcement would be on-site for this event?
	1. How are they trained to respond to these types of incidents?
	2. How long would it take local hospitals to dispatch emergency personnel and equipment to this location?
4. What are the crowd control and / or evacuation procedures for an event of this type?
	1. Who is responsible for activating the evacuation procedures?
	2. Is there a specified location for evacuees to go during an incident?
		1. Would this location change in the event of inclement weather?
		2. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
	3. Are event staff members trained in the evacuation procedures?
	4. Are local first responders familiar with your emergency procedures?
		1. Are they trained for scenarios like this?
	5. How are the spectators notified of the evacuation plan once it is set in motion?
5. Does your community have an established crowd control plan for an event such as this?
6. Would your organization take accountability of the staff working at the event and, if so, how?
7. What command and control considerations would be taken at this point in the response?
8. Would fire personnel, EMS personnel, and IED response teams be delayed in entering the scene to assist injured participants?
	1. How could these delays be mitigated?
9. At what point would local hospitals be alerted to the incident?
	1. Who is responsible for alerting the hospitals?
10. If the cellular network is overwhelmed, does that affect your warning procedures?
	1. Is there an alternate alert method?
11. How quickly are messages being released to the public?
	1. Who is responsible for this type of messaging?
	2. How are these messages released?
	3. How are the messages coordinated across the different agencies and organizations?
	4. How will your organization use social media to inform the public of emergency protocols during and after an incident?
	5. Who would be in charge of the social media response?
12. In a similar scenario, what actions would your organization or facility take at this time?
	1. Who would you contact?
	2. How would you contact them?
13. What actions are local, state, and federal law enforcement agencies taking at this point?
14. What plans or procedures exist to work with populations with special needs?
15. What procedures are taken to stand up an EOC?
16. 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 between private and public sector stakeholders?
	3. Does your organization have representation within the EOC or the Incident / Unified Command?
17. How would your organization or business distribute messaging to your employees?
	1. To patrons or customers?
	2. Would the messaging be coordinated with any other businesses?
	3. Does your organization have an identified Public Information Officer (PIO)?
		1. If so, does your PIO have any experience working with other organizations’ or first responder PIOs?

This page is intentionally left blank.

# Module Three: Recovery and Business Continuity

## Scenario

### [Insert Incident + 3 Days]: [Insert Time]

There were [insert number] fatalities because of the initial IED attack. An additional [insert number] victims sustained varying levels of injuries from the IED attack and ensuing stampede.

Following the initial response, the community has turned to short-term recovery procedures. Businesses and organizations are executing continuity of operation plans, and families continue to try to locate lost loved ones who dispersed upon seeing the sUAS’s erratic flight pattern. The media continues to contact a variety of organizations looking for any additional information.

## Discussion Questions

1. Does your organization or business have a continuity of operations or business continuity plan?
	1. How would an IED attack compromise your business’ cyber and physical security?
	2. Is there a plan to mitigate or protect against sUASs after this incident?
2. Are there established contracts to assist in the cleanup of the area prior to reopening?
3. What are the short-term recovery procedures for your organization or business?
4. Who makes the decision on when the area will be reopened?
	1. How is that decision communicated to the public and the media?
5. What would the financial impact be on your organization if it were closed because of such an incident?
6. How would your organization change its physical or cyber security practices after this incident?
7. Would your business close because of this incident?
	1. How would the incident affect businesses in the area that weren’t directly involved in the event?
8. What social media monitoring, if any, is in place to maintain awareness of information spreading that may not be accurate?
	1. Who is responsible for this?
	2. What procedures exist to counter false information spreading online?
9. Is there personnel in charge of communicating with law enforcement post-incident?
10. At what point would you consider the area and all associated organizations or businesses stabilized and back to steady state?
	1. Who determines when it is safe for visitors to return to the area?
	2. How is that decision communicated to the public?
11. How would family assistance or reunification be handled immediately following the incidents?
	1. Who is responsible for this?
	2. What procedures exist for this?
	3. How are families made aware of where to go?
12. Does your organization or business have mental health services available for your employees?
	1. Is there an SOP for visitors that were impacted by the incident?
	2. How would available services be communicated?
	3. Are these services available to volunteers as well?
13. What impact would the incident have on an event such as this?
	1. Would event organizers hold the event again?
	2. How would this incident impact event support from local businesses?
14. Does your organization have procedures for reuniting individuals with possessions they may have left behind?
15. Are procedures or resources in place to set up memorials following a mass casualty event?

# Appendix A: Sample NTAS AlertSample NTAS alert. Sample reads as follows:   HEADER: National Terrorism Advisory System Alert  www.dhs.gov/advisories  [Insert Date]  DURATION: This Bulletin will expire on or before [Insert Date] at [Insert Time] EDT   TYPES OF ADVISORIES:  - Bulletin: Describes current developments or general trends regarding threats of terrorism  - Elevated Alert: Warns of a credible terrorism threat against the United States - Imminent Alert: Warns of a credible, specific and impending terrorism threat against the United States  BODY: [Insert Threat] [Insert text box with appropriate information]  HOW YOU CAN HELP:  - Report suspicious activity to local law enforcement who are best to offer specific details on terrorist indicators - Report suspicious activity of information about a threat, including online activity, to fusion centers and the FBI's Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative  - Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity   BE PREPARED:  - Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs information with you.  - Connect, Plan, Train and Report to prepare businesses and employees. Security resources can be accessed through the DHS's Hometown Security Campaign   STAY INFORMED:  - The U.S. Government will provide additional information about any emerging threat as additional information is identified. The public is encouraged to listen to local law enforcement and public safety officials.   FOOTER: If you see something, say something. Report suspicious activity to local law enforcement or call 911  The National Terrorism Advisory System provides information on homeland security issues and threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/advisories. To receive mobile updates: www.twitter.com/dhsgov

This page is intentionally left blank.

# Appendix B: 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] |
|  |
|  |
|  |

# Appendix C: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix D: Resources

CISA Office for Bombing Prevention (OBP) Resources

[Unauthorized Drone Activity Over Sporting Venues](https://www.cisa.gov/publication/unauthorized-drone-activity-over-sporting-venues)

[Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems](https://www.cisa.gov/publication/advisory-application-federal-laws-acquisition-and-use-technology-detect-and-mitigate)

* [UAS Considerations for Law Enforcement Action | CISA](https://www.cisa.gov/uas-law-enforcement)

This page is intentionally left blank.

# Appendix E: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DTI** | Detect, Track, and Identify |
| **EAP** | Emergency Action 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 |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **OBP** | Office for Bombing Prevention |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **sUAS** | Small Unmanned Aircraft System |
| **TFR** | Temporary Flight Restriction |
| **TTX** | Tabletop Exercise  |

