PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0031 September 2021

Airport Response to Unmanned Aircraft System (UAS) Threats

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Principal Investigator:
Zachary Shuman
Woolpert
Denver, CO

Contributors:
Rick Day, 6 DOTs
Aaron Lawrence, Woolpert
Sheldon Menezes, Woolpert
Maria Muia, Woolpert
Drishti Valecha, Woolpert

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0031 PROJECT PANEL

Adam Bouchard *Tampa International Airport*
Jason Byers *Dallas/Fort Worth International Airport*
Frank Capello *Fort Lauderdale–Hollywood International Airport*
Cory Chase *Port of Portland Police Department*
Collen Chamberlain *American Association of Airport Executives*
Mark Coates *Seattle-Tacoma International Airport*
Trevis Gardner *Metropolitan Knoxville Airport Authority*
David Hornsby *Dallas/Fort Worth International Airport*
Bill Marrison *Safe Skies Board of Directors*
Timothy Tyler *Metropolitan Washington Airport Authority Police*
Stephan Van Der Merwe *National Safe Skies Alliance*
Kevin Vandeberg *Huntsville International Airport*
Jeremy Worrall *State of Alaska DOT*

Ex Officio

Mike DiPilato *FAA Airport Safety R&D Section*
Charles King *Transportation Security Administration*

CONTENTS

TABLES & FIGURES

SUMMARY

The popularity and affordability of Unmanned Aircraft Systems (UAS) bring both benefits and risk. For airport operators, a significant risk exists because of the low barrier to entry, limited restrictions, and few tracking and reporting mechanisms associated with UAS. While regulations are slowly catching up to technological advances, there is still a significant gap, and airports have few places to turn for resources to prepare for UAS threats. The FAA does not currently have specific guidance for responding to UAS threats; however, other federal agencies (e.g., DHS and Department of Justice) have developed guidance that could be useful references for airports when updating their airport emergency plan (AEP). This guidebook has been created to assist airport operators with planning for potential threats from UAS operating in unauthorized airspace.

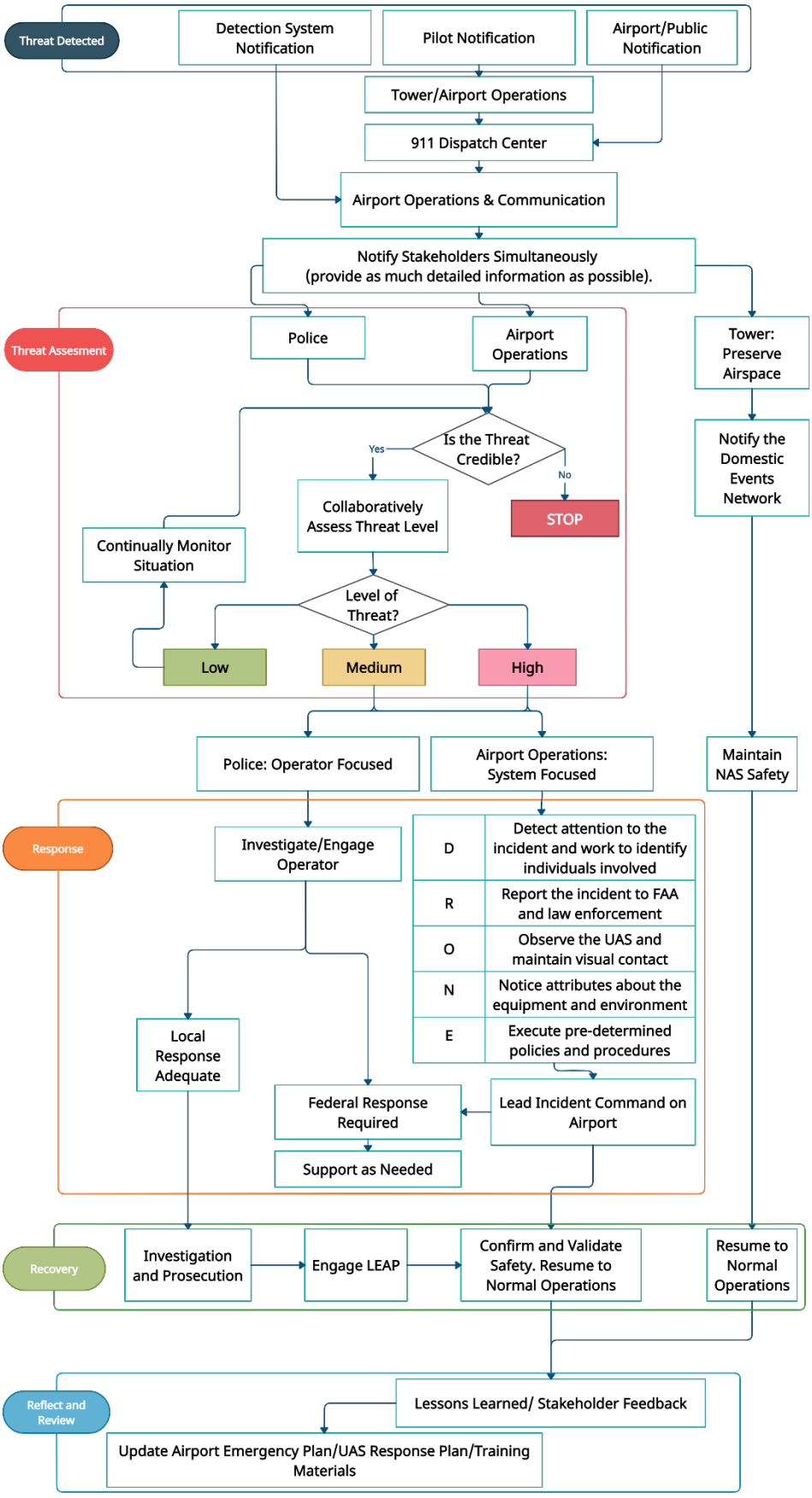
UAS operations around airports can be from numerous different types of operators with varying intents. This guidebook is not intended to provide best practices to restrict UAS operations, but rather to prepare for the non-responsible operators: the clueless, careless, and reckless. Authorized and safe UAS operations in and around airports are not the focus of these responses.

An airport's response to a UAS threat will be most successful when the response is planned, documented, and effectively executed by trained staff. Airport officials can utilize this guidebook to develop their own response plans that incorporate the unique characteristics and structure of their airports.

Part of a successful response plan also includes identifying the appropriate stakeholders that should be included in the response, and outlining a communication plan. Conducting training and tabletop exercises will assist in threat preparedness. These elements and other best practices are discussed in this guidance document. While one size does not fit all, the guidance presented in the next sections outline the fundamental elements necessary for a thorough response, with variation expected based on airport size, available resources, organizational hierarchy, and budget considerations.

An airport's response can most easily be outlined through the flow chart below, which is divided into three sections: threat assessment, response, and recovery. The flow chart and its associated best practices can be utilized by most airports and tailored for their specific needs.

Figure 1. Airport UAS Threat Life Cycle Flowchart



PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

AEP	Airport Emergency Plan
ATC	Air Traffic Control
CONOPS	Concept of Operations
C-UAS	Counter Unmanned Aircraft System
DFW	Dallas/Fort Worth International Airport
DEN	Domestic Events Network
FAM	Federal Air Marshal
LEAP	Law Enforcement Assistance Program
LAANC	Low-Altitude Authorization and Notification Capability
MANPADS	Man-Portable Air-Defense System
NAS	National Airspace System
ASH	Security and Hazardous Materials Safety
TRP	Tactical Response Plan
TPA	Tampa International Airport
UAS	Unmanned Aircraft Systems

SECTION 1: PLANNING

With the emergence of UAS in the National Airspace System (NAS), planning for a UAS threat is critical to protecting the safety of an airfield. There are numerous facets of planning, including:

- Stakeholder engagement
- Response operations guide
- Training and exercises
- Community awareness
- Airport detection, tracking, and identification (DTI) technology

At a minimum, a planning document should include roles and responsibilities, training protocols, communication infrastructure, threat assessment, response, and recovery plan to each threat level. All planning documents should be created and maintained as "living" documents (i.e., those that can be changed and updated over time). As the industry, technology, and policies around UAS change rapidly, reviewing planning documents at least once a year is important to keep them current.

A UAS response plan can be incorporated into the AEP to leverage existing practices, resources, and tools for continuity and ease of training. These response plans should focus on a UAS incursion of airspace. In the unlikely event the UAS strikes an aircraft, predefined protocols in the AEP for collisions should be followed. UAS threats to airspace and its operators can be treated like other threats originating off airports or as on-airport irregular operations events. For example, strategies can be pulled from response protocols to laser incidents or man-portable air-defense system (MANPADS) for best practices as it relates to UAS threat response (Gould & Schroeder, 2004). The following subsections outline strategies to plan for a UAS threat.

There are different types of UAS transgressors, including nefarious/criminal actors and those characterized as clueless and careless. Each category can warrant a different response, and can be planned for and mitigated in different ways. Some of these are outlined below and in the different threat levels discussed.

1.1 Stakeholder Engagement

Effectively preparing for and responding to a UAS threat on an airport requires significant collaboration with stakeholders. Involving appropriate stakeholders early and often is key to preparing for a UAS threat. Airports should create a UAS working group with all internal and external applicable stakeholders, which should meet at least once a year to coordinate and train for a threat response. Table 1 and the following subsections outline key stakeholders and their corresponding responsibilities in planning for and responding to a UAS threat. Also, consider involving stakeholders that may have concerns that indirectly relate to unauthorized UAS operations; for example, Border Patrol and National Guard may be concerned with potential privacy concerns due to UAS flying overhead. In order to develop a holistic response plan, conversations should be conducted with all stakeholders regarding their concerns, and results should be documented.

During responses for a medium or high threat,[1] it is critical to set-up a unified command per the airports AEP. The specific level or type of threat that requires a unified response should be decided in the

[1] See Section 2 for more information on threat levels.

response plan. The response and communication between stakeholders should follow the National Incident Management System (NIMS) and AEP. A matrix that summarizes roles and responsibilities of the unified command during the life cycle of a UAS threat is illustrated in Table 1.

Table 1. Unified Command Stakeholder Roles and Responsibilities

STAKEHOLDER	JURISDICTION	PLANNING	THREAT ASSESSMENT	RESPONSE	RECOVERY
Airport	Operations, Safety, and Security	Coordinate planning, training and exercises. Conduct stakeholder engagement and foster community awareness. Maintain Detection Infrastructure. Create and maintain the UAS Response Plan	Refer to UAS Response Plan, Threat Assessment Matrix, notify unified command based on threat level	Lead incident command and direct response on-airport property. Develop accurate and timely information for use in media/ social briefings	Airport Inspection to validate return to normal operations, lessons learned
Air Traffic Control	Airspace	Review Incident Safety Plan, training and exercises	Disseminate real time information to accurately assist with threat assessment	Safety of manned aircraft, communications to pilots and coordination with NAS stakeholders	Makes the call to resume to normal operations based on pre-established criteria identified in the Incident Safety Plan
TSA/FSD	Federal Response	Develop National Policy and Guidance tools	Disseminate real time information to accurately assist with threat assessment	Security, deployment and operation of Federal Response if needed	Federal Investigation
Law Enforcement	Investigation	Review Incident Safety Plan, training and exercises,	Immediate response in Medium/ High Risk	UAS operator contact. Identify and mitigate hazardous situations. Stop and prevent unsafe acts	Investigation and prosecution

1.1.1 Airport Operators

The airport operator is the governing body over the airport's management and operation. Airport operators can take many shapes and are typically responsible for safe operations and security of the airfield and people. In an airport response to a UAS threat, it is the airport operator's responsibility to plan and coordinate the response effort.[2]

Airport operators typically do not have jurisdiction to restrict, mitigate, or prosecute operators of UAS that intrude into an airport's airspace or imaginary surfaces. Considering this, the airport operator needs to coordinate with local and federal officials in the event of a UAS threat.

The airport operator will likely be part of a response to unapproved UAS operators positioned on the airfield. This means the airport operator will need to establish a communication plan for events and establish common expectations for investigation and/or response. The airport operator will typically lead and sponsor all planning and training for responses, and will ensure the continuity of operations during and following the threat depending on severity.

For non-towered airports, it is recommended that the airport operator advise local air traffic through the Common Traffic Advisory Frequency (CTAF) to provide increased situational awareness of any present UAS threat. The airport operator should continue to monitor the threat and provide updates to pilots that are inbound, outbound, or in the airport's traffic pattern. The flow chart of a UAS threat lifecycle illustrated above can be utilized at non-towered airports, but it should be noted that the airport operator now plays the vital role of providing both local law enforcement and local air traffic with up to date information.

Airport operators also have a unique responsibility of community engagement. Most UAS threats to airports will not be created by nefarious actors or intentions. UAS have a low barrier of entry to the airspace, creating a need for local awareness and community training to safely fly UAS. By conducting local community outreach, and including city, county, or state agencies, the airport operator can decrease the potential for non-criminal UAS threats. See Section 1.5 for more information.

Title 14 CFR §139.325, Airport Emergency Plan, requires Part 139 certificated airports to have an AEP.[3] This is a logical place for a UAS threat response plan to be documented. Airport personnel responsible for maintaining the AEP should review it to analyze the levels of threat that UAS may pose, and the potential response efforts that may be necessary for instances when a UAS has the potential to collide with an aircraft. An AEP often incorporates an emergency alert classification and notification structure, which could include an alert level for a UAS threat and imminent aircraft accident.

---

[2] 49 CFR § 1542.215, Law Enforcement Support, states the following:

> Airport operators must ensure a law enforcement presence at the airport that is sufficient to address the evolving UAS threat to airports. Pursuant to 49 U.S.C. § 44903(c), TSA requires all airport operators holding certificates issued by the Department of Transportation to establish security programs providing a law enforcement presence and capability at the airport that is adequate to ensure the safety of passengers. The airport's security program must provide law enforcement personnel in the number and manner adequate to support the program. (49 CFR § 1542.215)
>
> Airport operators must ensure law enforcement personnel have authority to arrest, with or without a warrant, while on duty at the airport for violations of criminal laws of the state and local jurisdictions in which the airport is located, when committed in the presence of the individual or when the individual has reason to believe the suspect committed a felony. (49 CFR § 1542.217[b])

[3] FAA Advisory Circular 150/5200-31, Airport Emergency Plan, provides guidance to the airport operator in the development and implementation of an AEP.

1.1.2 Air Traffic Control

The primary purpose of Air Traffic Control (ATC) is to facilitate the safe and efficient flow of air traffic, and to prevent a collision involving aircraft operating in the NAS. ATC carries a critical role in mitigating the risks posed to manned aircraft by a UAS intrusion.

An airport in a dense urban area can have dozens of UAS sightings per day around its airfield. However, most UAS flights will not pose a risk to manned aircraft and thus not need an ATC response. ATC should be contacted about viable threats that would interfere with the safe operation of traffic at the airport, as ATC has the most immediate ability to advise pilots or direct them away from an area. ATC can divert manned aircraft when the UAS threat is credible and quantified.

In some situations, ATC will be the first to identify or be alerted of a potential UAS threat. In this instance, ATC will contact law enforcement and/or airport operations to begin responding to the threat. This will most likely also trigger a report to the Domestic Events Network (DEN). At that point, the threat assessment will take place and be led by the airport authority. ATC has an internal process for notifying other federal divisions and agencies of a UAS threat. This communication cycle should be outlined in the response plan and, if warranted, a letter of agreement should be developed between all applicable parties (see Section 1.1.9 for more information).

1.1.3 Transportation Security Administration

The TSA has overall federal authority in response to persistent UAS threats. Coordination with the TSA should take place through the local FSD. The Assistant FSD – Law Enforcement is charged with coordinating the federal law enforcement response to a significant UAS threat. TSA is the lead agency for the federal response to UAS threats, and TSA law enforcement is the sole group authorized to mitigate persistent credible threats. Having a TSA representative on the airport's UAS working group will assist in aligning and disseminating information, and getting the proper support when needed. Airports that do not have the capability or resources to have a UAS working group, should hold regular meetings with their local TSA contact.

As of the date of this report, the TSA is developing a national Concept of Operations (CONOPS) for the federal response at the Core 30 airports. TSA involvement in a response will begin with a credible and persistent detection of a UAS threat. The CONOPS will outline how the recovery and investigation of all UAS threats will involve federal agencies (see Legal Considerations).

1.1.4 Law Enforcement

Federal, state, and local authorities share the responsibility of protecting airports and their surrounding environments from UAS threats. Coordination between law enforcement partners will help ensure a unified and complete response. In the case of most UAS sightings and incidents at airports, it is the responsibility of the state and local law enforcement authorities assigned to protect airports to respond to a UAS in the first instance, and mitigate any impact on airport operations.

Local law enforcement is critical to responding to a UAS threat, and are most equipped to respond when the UAS operator is positioned off airport property. With their jurisdiction and training, local law enforcement will likely be the lead on operator engagement and investigation. Law enforcement has the jurisdiction to reprimand and prosecute nefarious actors, which makes them a critical part of community engagement. It is important to note law enforcement will likely not fully understand the threats and FAA regulations governing UAS without training and knowledge of available resources (such as the FAA's Public Safety and Law Enforcement Tool Kit). The airport authority should lead this training effort.

Airports that have on-site law enforcement are likely to have existing collaboration, training, and understanding in UAS matters. For airports without on-site law enforcement, conducting additional training and outreach will assist the law enforcement in responding effectively. Mutual aid agreements between local law enforcement and the airport can be utilized to outline the methods and plan for a response. Airports that have early response plans have found these agreements to be beneficial.

Training and direct communication between airport authorities and law enforcement are needed for effective responses. Airports without an on-site law enforcement presence, a regularly scheduled coordination meeting with local law enforcement is encouraged, along with their participation in an exercise where intervention is discussed. This will ensure consistent and successful collaboration.

The Law Enforcement Assistance Program (LEAP), run by the FAA's Office of National Security Programs and Incident Response, is designed to support state and local agencies by denying anyone access to the NAS that may pose a threat to national security. This office can take necessary regulatory enforcement actions against unlawful UAS operations or offer support to law enforcement agencies pursuing criminal prosecution of such operations. LEAP may be most valuable during training and after a threat incident, as opposed to during an incident. Additionally, under 49 USC § 114(q)(2), Federal Air Marshals (FAM) have authority to arrest UAS operators for violations of federal law and to seek and execute warrants for seizure of evidence, including evidence related to UAS.

1.1.5 Emergency Response

Emergency response to a UAS threat is different than to an accident, but can involve the same entities including ARFF, emergency medical service, public health, environmental health, public works, etc. These entities may be located on or off the airport. They are the same entities the airport coordinates with for other emergencies, and if an emergency is ultimately declared, the airport's established AEP should be followed. Since UAS threat information can originate from many different sources, the AEP should be tightly integrated with the plans from TSA, ATC, the local law enforcement organization, etc., to ensure a cohesive planning effort.

For airports with an Airport Communications Center or Emergency Operations Center, the response should be centralized utilizing existing infrastructure. Leveraging the airport-specific TSA Tactical Response Plan (TRP) and the *Unified National Level Response to Persistent UAS Disruption of Operations at Core 30 Airports* CONOPS, as appropriate, the process and time to contact emergency response entities for a UAS threat will likely be similar to other threats. Emergency response entities would typically be contacted after the threat is detected and a threat assessment has been completed. On-airport ARFF may warrant the earliest contact to be on high alert should they need to respond quickly if a collision with a UAS is imminent. All emergency response entities should be familiar with the alert notification and warning system in the AEP and TRP as it pertains to UAS threats, and understand the relevance to their respective operations.

1.1.6 State Transportation Agencies

State transportation agencies (i.e., Departments of Transportation) are not typically tasked with responding to individual airport threats, either from UAS or other sources. Post-incident contact may be appropriate to potentially identify patterns that may warrant the implementation of policy measures at the state government level. For smaller airports that are managed by a state transportation agency, the responsibilities outlined in Section 1.1 Airport Operators should apply.

1.1.7 Tenants

Tenants can include fixed-base operators, airlines, freight forwarders, flight schools, aircraft maintenance providers, etc. In responding to UAS threats, tenants contacted as part of the normal AEP process when the threat level is high and is germane to their operations. For example, a UAS threat to aircraft operations may have a high level of relevance to an airline operator but a very low level to an airport concessionaire. Tenants should be versed in the alert notification and warning system in the AEP as it pertains to UAS threats, and understand the relevance to their respective operations.

1.1.8 Aircraft Pilots

Pilots are the most likely to be impacted by UAS threats and often will be the first to report them to the ATC. It is then ATC personnel's responsibility to report such threats to other aircraft operating in the area and the responsible Airport Authority (typically Airport Emergency Operations or the Manager). If notification of a threat comes from outside the ATC system, then, based upon the threat level, it should be communicated to ATC, which would then disseminate the information to pilots in the area. The circumstances and flow of reporting can be agreed upon in MOUs.

When trends of non-threatening UAS operations local to the airport are identified, it is important to work with UAS operators, aircraft operators, and the proper air traffic control facility to provide situational awareness to aircraft operators. Providing the appropriate level of information about known or expected UAS operations can limit any non-threatening UAS being identified by pilots, and protect the safety of the aircraft operators.

1.1.9 Stakeholder Reporting Sequence

The UAS event reporting sequence typically begins with the pilot or ATC, because they are usually the first to see the UAS. If it is the pilot, it should be reported to ATC, and then ATC will take the appropriate action to communicate it to other pilots in the area. At this point, the event should be reported to the airport operator, law enforcement, and the DEN. For UAS events that are identified by the airport operator or law enforcement, ATC should only be contacted if the threat has been reasonably confirmed.

If warranted, a unified command should then be developed to coordinate a response. Members may include stakeholders such as, the airport operator, law enforcement, major tenants, and, if warranted, ATC and TSA. More information on reporting is included in Section 3.

Timely reporting is necessary to ensure prompt response by law enforcement and increase their chances of locating the UAS operator. The DEN reports the incident to FAA Security and Hazardous Materials Safety (ASH). ASH distributes a report to the TSA, FBI, Department of Defense, and DHS. The FAA, FBI, and other law enforcement agencies investigate the UAS incident. ASH follows up and facilitates the information exchange between the agencies involved. (Might, 2017)

1.2 Training and Exercises

Training and exercises are critical for an airport to be fully prepared for a UAS threat. Airport Authorities that have trained for UAS response have predominately taken one of two approaches:

1. Integration of UAS threats into the triennial full-scale emergency preparedness exercise
2. Independent coordinated training in the form of tabletop exercises

It is especially important to use these opportunities to integrate the responses of multiple decision-making entities and fine tune the airports coordination and communication processes.

Airports leveraging their full-scale triennial emergency preparedness exercise have a unique opportunity to go above and beyond the minimum requirements to satisfy criteria established by FAA and FEMA by incorporating UAS threats into the emergency scenario and testing additional capabilities.

Airports that leverage training for UAS threats or disruptions to airport operations in the form of routine tabletop exercises have the opportunity to test multiple unique scenarios, engage specific stakeholders, and keep up with ongoing technological advancements in the UAS market. These routine tabletop exercises foster a continuous improvement approach, as they take into account the proliferation of UAS and consider the advancements in technology, new risks, and opportunities to improve response plans or times. As airports prepare to utilize these training approaches, it is important to ensure all employees (i.e., all shift schedules) have an opportunity to participate, and that aspects of the training are incorporated into new hire orientation.

To be fully prepared for a UAS threat in and around the airport vicinity, the following components can be incorporated into routine training:

- Review of current UAS regulations
- UAS operating restrictions in the NAS
- Tracking and identification of a UAS
- Reporting UAS sightings and coordinating with involved stakeholders (e.g., ATC, ARFF, and local law enforcement)
- Threat assessment matrices

An example tabletop exercise has been included in Appendix A.

1.3 Leveraging other Resources

There are numerous resources airports can utilize to support developing and implementing a response plan to UAS threats. For planning purposes, airports should review their current community engagement methods, emergency procedures, training exercises, and letters of agreement to leverage existing materials and infrastructure.

Also, airports should utilize external resources, such as the FAA's Law Enforcement Toolkit, and their local law enforcement technologies and personnel. UAS threats can be wide area concerns that cross numerous jurisdictions and threaten other critical infrastructure and airports. Airports should communicate with local critical infrastructure operators, such as prisons, Air National Guard or military reserve units, and energy infrastructure that may have detection equipment and response protocols that can assist in the event of threat. The FAA has provided a Drone Toolkit and Remote ID Toolkit, which are also valuable resources for Airport Operators.

1.4 Public Policy Considerations

Local and state officials have begun to consider UAS-related legislation, with regulations that are primarily focused on privacy issues. Some airports have found ways to coordinate and lobby their local officials to support policies that would help protect airports from UAS threats. Examples include:

- Creating zoning restrictions around airports that limit areas from which operators can launch and operate UAS
- Utilizing community planning groups to set up permanent public notices for community awareness
- Developing mechanisms to report planned, authorized UAS operations to ensure airport operators are aware of potential UAS sightings

The FAA has developed a fact sheet for state and local regulations surrounding UAS usage. Examples of public policy include 49 USC §§ 114(f) and 114(p)(2); 49 USC §§ 44801, 44904, and 46314; 14 CFR § 107; and 49 USC § 44903 (j)(2)(D)(i). Other online resources for public policy information include AUVSI's policy map by state.

1.5 Community Awareness and Education

Since most UAS threats are not the result of nefarious intent, the best way to protect an airfield from a UAS threat is to educate the communities surrounding the airport on how and where to safely operate UAS.

There are numerous strategies to engage with the community. Most important is to make information and resources available for the local community to utilize. This could be in the form of a website with safe operation practices and locations, along with personnel to contact for questions about UAS policies at a local level. Additional strategies include holding community engagement events and educational lessons for schools.

Figure 2. Example of UAS Public Signage at DFW

Another impactful strategy is to work with local city officials to place "No Drone Zone" signs in places where UAS typically fly but are not supposed to (see Figure 2). Parks, attractions, and high density, family-oriented neighborhoods all lead to larger than normal UAS operations; signs with safe UAS operation tips can be placed in these areas. It is important to identify these high volume areas and put an emphasis on engagement at those locations. There are also times of year where UAS operations are more likely, for instance around the holiday season and summer. Engagement efforts should be increased during these times.

Examples of signage, derived from the FAA Community Engagement Toolkit, are provided in Appendix C. It is suggested to use these examples as a template to develop signage that has a localized focus. It is recommended that the airport place numbered "No Drone Zone" placards around the airport, so that members of the public who witness UAS operators nearby can contact the hotline listed to report the activity and reference the placard zone number. This enables local law enforcement to respond exactly to the location of observed activity.

During all community engagement efforts, it is important to promote safe operation within the NAS rather than discourage UAS usage.

1.6 Detection Systems and Technology

Effectively responding to a UAS threat is predicated on being able to detect the threat. UAS detection systems are being tested and becoming commercially available. Detection systems can utilize numerous different types of technologies such as radio frequency, optical, radar, and acoustic. Currently, there is no national standard for detection systems, but the FAA released a technical considerations sheet that includes descriptions of the main types of detection technology in early 2019, as well as additional information for airports that have or may install detection equipment. This information can be found here under "Guidance & Policy."

UAS detection systems are distinct from counter-unmanned aircraft system (C-UAS) technologies. C-UAS technologies are not permitted for airport operators' use as they have a mitigating aspect in addition to the detection component. Under the FAA Reauthorization Act of 2018, Sec. 383, Airport Safety and Airspace Hazard Mitigation and Enforcement, the FAA has been directed to test and evaluate technologies and systems that detect potential aviation safety risks posed by UAS at five airports. The sunset on this program is September 30, 2023.

Airports that are considering a response plan to UAS threats and deem a detection system necessary for their operations should begin planning for the potential infrastructure and cost requirements. The systems' sensors may require placement on top of existing infrastructure and in strategic locations around the airfield. Costs vary depending on the level of sophistication and customization of each detection system.

A UAS detection system should be designed with specific requirements to address threat assumptions. In a typical detect/identify/intervene process for protecting assets, the standard approach is to extend the detection perimeter to create more time to detect and identify possible threats. However, at a civilian airport, the area around the airport is likely populated and could contain many different activities, including UAS activity that is not a threat. For this reason, it may be useful to have a UAS detection system that is effective for commercial consumer-grade UAS. This may aid decision-makers by determining what is normal in the environment on a day-to-day basis to help distinguish unusual events.

Additionally, remote ID will soon be required on UAS. This will make available another layer of identification for airport authorities. However, it should be noted that detection systems for commercial consumer-grade UAS will not necessarily detect nefarious operators who deliberately operate without remote ID or using homemade UAS. Additional information on Remote ID can be found in Section 3.4.

Prior to installing a detection system, the airport sponsor will need to file Form FAA 7460-1: "Notice of Proposed Construction or Alteration." This allows for the FAA and the airport to coordinate on the detection system and take into account the radio frequency and physical disruptions presented by the technology. This should be supplemented by a CONOPS for use of the detection system.

SECTION 2: THREAT ASSESSMENT

When a UAS has been detected, a comprehensive threat assessment must be completed. While not all UAS sightings or detections are a significant threat to the airport and aircraft, they may present safety concerns that need to be identified and addressed. An example threat assessment matrix has been provided below. The airport and its stakeholders should develop a threat matrix tailored to their airfield and operations.

2.1 Threat Assessment Matrix

A standardized matrix should be used to assess the threat a UAS poses to the airport and its operations. This threat matrix should be developed in the planning stage and incorporated into the airport planning documents and training.

The factors that affect threat levels include but are not limited to:

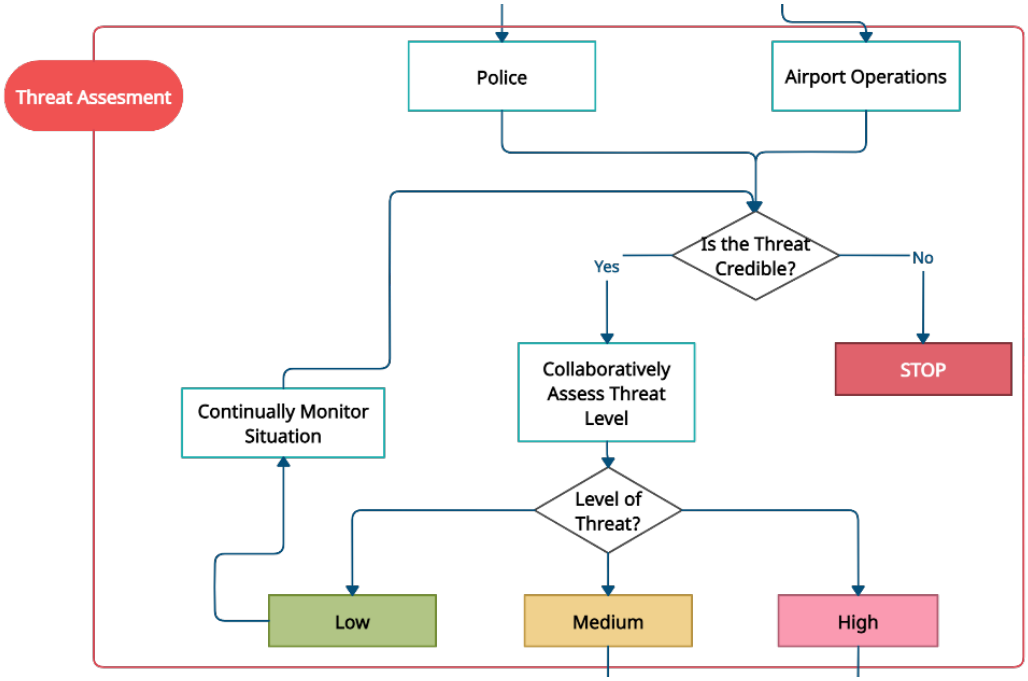
- Location
  - Distance from airport
  - Airport vicinity (airside/landside)
  - Land-use type (e.g., park where UAS are often seen)
- UAS size
- Number of UAS
- Time of day
- Length of detection
- Altitude
- Trajectory information
- Critical airspace intrusion
- Type of detection (credibility)

Low levels of threat would pose no interruption to airport operations, while high levels would be persistent, disrupt operations, and present a safety risk. That risk could be either to conventional aircraft or to people and property on the ground.

Threat assessment will be complicated by the fact the initial report(s) may come from the general public, and therefore may have some ambiguity or inaccuracies. This makes it especially important to have any reports quickly input into a methodical assessment process. Depending on the UAS location, visual sight or detection via technology should occur before reporting to air traffic.

It should be noted that assessing a UAS threat needs to be a collaborative effort between airport operations and airport or local police. The flow chart in Figure 3 (excerpted from Figure 1 in the Summary section) illustrates the threat assessment workflow in the event of a UAS threat detection or notification.

Figure 3. UAS Threat Assessment Workflow



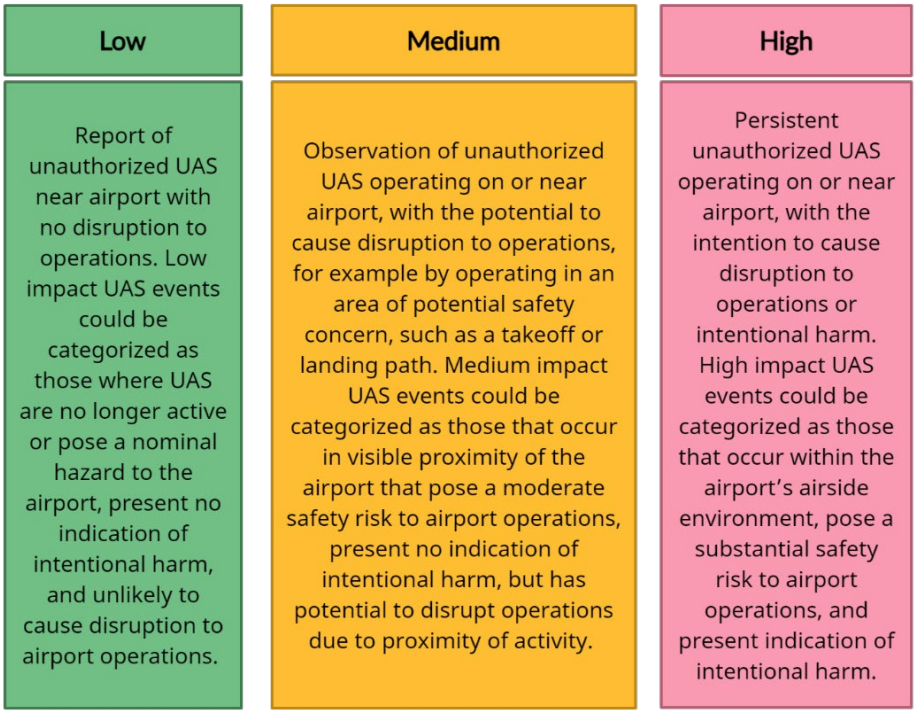
A threat level assessment should be made based on all available information and needs to be continually assessed as new information is provided. The level of threat will vary based on an individual airport's unique characteristics. A sample threat assessment matrix based on distance from the airport is presented in Table 2. It is essential for an airport to review the variety of factors listed above and develop threat assessment matrices unique to their own facility.

Table 2. Threat Assessment Matrix

Threat Level / Factor: Location	Level 1 Minimal	Level 2 Major	Level 3 Catastrophic
5–10 miles from airport	Low	Medium	Medium
2.5–5 miles from airport	Low	Medium	High
Less than 2.5 miles from airport	Medium	High	High

An example of threat levels developed by the Blue Ribbon Task Force (UAS Mitigation at Airports, 2019) is presented in Figure 4.

Figure 4. Blue Ribbon Task Force Threat Level Definitions



Airports can also utilize a scoring system to assign threat levels, as illustrated in Figure 5. In this example, a selection of high would correlate to a 3, medium 2 and low a 1. Adding together the corresponding numbers enables the airport to classify if the risk is high, medium or low. Location of UAS would indicate a high overall threat regardless of the outcome of the scoring exercise if it is on airport property.

Figure 5. Threat Assessment Scoring Matrix

Factor	Corresponding Risk: High (3)	Medium (2)	Low (1)
*Location of UAS	On Airport Property	Less than 2 miles away	Greater than 2 miles away
Number of UAS	Fleet (3+)	Pair/ Small Group (2-3)	Single (1)
Size of UAS	Medium/ Large (55 lbs. +)	Small (2 - 55 lbs.)	Micro (<2 lbs.)
Speed/ Trajectory	Erratic and Unpredictable	Slow Moving	Hovering
Controller Location	Hidden, Obscured or Spoofed	Unknown	Known
Frequency	Persistent	Unknown	Single Operation
Scoring System	High: 14-18 points	Medium: 11-14 points	Low: 6-11 points

*Note: *If the location of UAS is on airport property, it would indicate a "High" overall threat regardless of the outcome of the scoring exercise.*

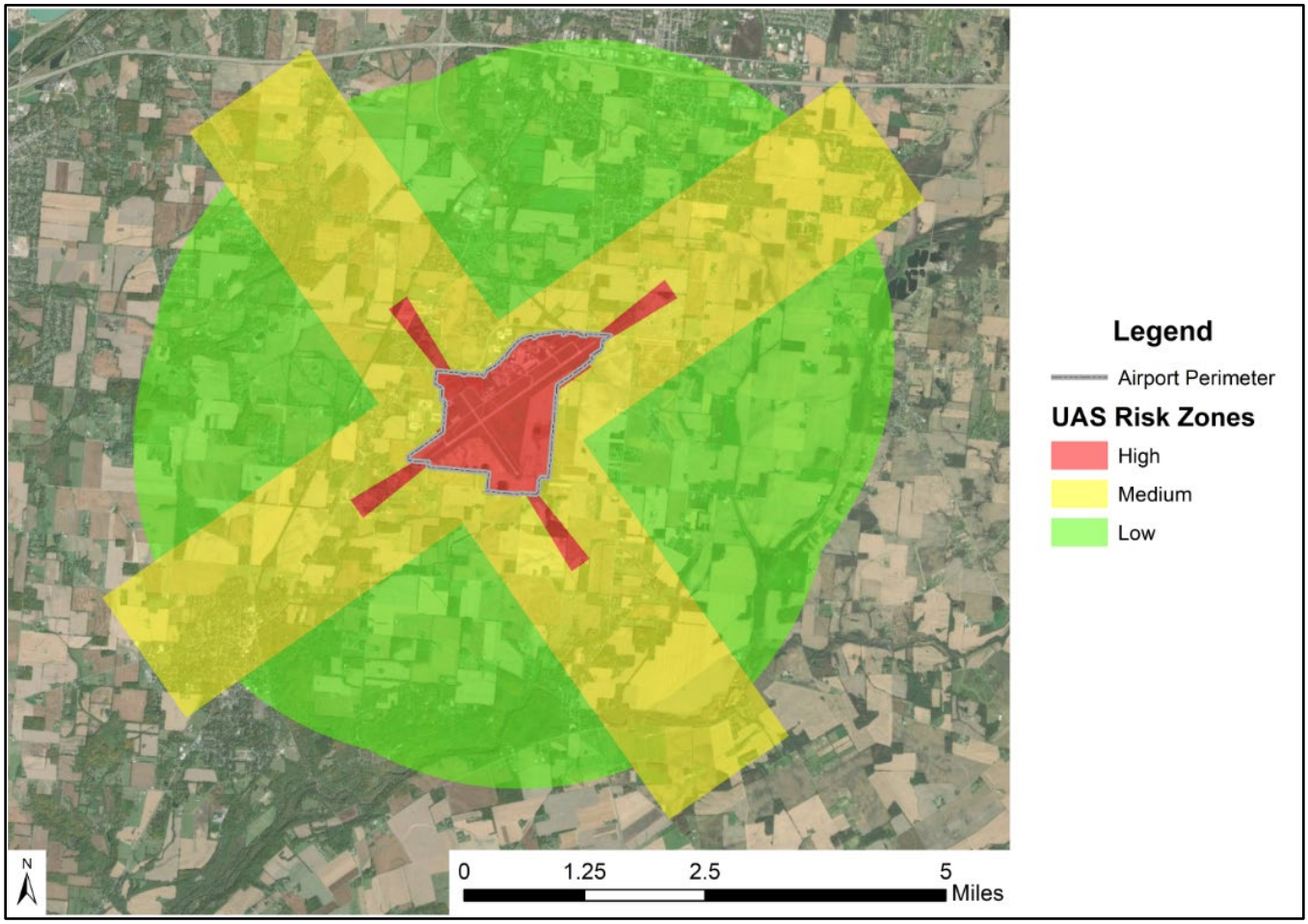
2.2 Threat Assessment Locations

Not all locations around the airport are considered high risk if a UAS is detected. Specifically, airport property and the approach/departure corridors present the highest risk. This is in accordance with a UAS pilot's ability to get authorization to fly in controlled airspace through the low-altitude authorization and notification capability (LAANC). LAANC allows UAS operators to fly in low-risk areas up to pre-determined altitudes in controlled airspace. ATC typically has LAANC authorization records, and third-party vendors are offering it to airports. Developing a risk zone map will assist in a timely threat assessment. UAS in a low-risk area will likely result in a limited response and monitor plan, while high-risk areas will trigger an immediate response.

Each airport's risk zones will be different. Altitude plays a critical role in determining risk to air traffic, and working with pilots, ATC and the community will assist in determining areas specific to the airport that present higher risk. Examples include known regular low-altitude helicopter operations that may not follow traditional approach/departure corridors.

Utilizing Part 77 surfaces can assist in creating natural boundaries for risk zones. Figure 6 shows an example of using these surfaces to develop a map for all stakeholders to reference. While a UAS in a low or medium risk zone may not warrant an immediate response, other attributes such as its altitude, trajectory, speed, and length of time flying can increase the threat.

Figure 6. Example Risk Zones



SECTION 3: RESPONSE

When a UAS is detected, a threat assessment should be conducted and a response initiated. The threat assessment will dictate the appropriate response required based on several criteria. The response should be airport specific, and should be based on threat level. For a response to be successful, numerous stakeholders must work together towards their respective goals (see Table 1, Section 1.1).

The most difficult challenge in conducting an efficient response is determining the location of the UAS and/or operator. Police are best equipped to begin the response centered on the operator, while airport operations can attempt to visually confirm and monitor the UAS while relaying information as described in Section 3.1. Because a UAS is difficult to see and can easily travel in any direction, it is important to quickly dispatch the closest resources but alert as many resources as possible.

Airports do not have the legal authority to eliminate or mitigate a UAS threat (Title 18). The FAA's guidance on responding to a UAS threat is to follow D.R.O.N.E (Law Enforcement Guidance for Suspected Unauthorized UAS Operations, 2018):

Direct attention to the incident and work to identify individuals involved

Report the incident to FAA and law enforcement

Observe the UAS and maintain visual contact

Notice attributes about the equipment and environment

Execute pre-determined policies and procedures

3.1 Information Dissemination and Notifications

If a UAS threat is detected by airport personnel, certain information should be immediately recorded for dissemination to ATC, law enforcement, and other pertinent entities. Specifically, a description of the UAS, including color, type, propulsion, and registration number, if viewable. If known, the location of the launch site, flight path, and any available information about the operator should be disseminated to law enforcement.

The initial reporting of a UAS sighting or detection can come from various parties. This creates a challenge in planning a response based on different information origins. Once the threat is defined, developing a unified command/communication center will assist in gathering information from all parties and effectively responding to both the operator and the UAS.

The timeliness and method by which information is conveyed is crucial to an effective response. Telephone or radio communication is the fastest way to disseminate information in real time, and should be used to begin the response whenever possible.

3.1.1 "Watch and Report" Programs

While the identification of a UAS is difficult, there are strategies to encourage public and employee participation in actively finding or reporting unauthroized UAS. Having a pre-established program that encourages people to search for and report location information can be invaluable during a response.

Through community engagement, airports can set-up a "watch and report" program on their website or a designated phone number that allows for community members to submit reports of a UAS operating near an airport. Sharing this tool with law enforcement can also quickly get reports directly to airport operations to begin a response if deemed necessary. A tool like this should be actively promoted throughout the community.

3.2 UAS Tracking and Locating Strategies

UAS can be difficult to find in the sky, especially if the system is a small off-the-shelf UAS. Strategies to find and track the UAS include:

- Divide the sky into grids and task multiple people with scanning the sky in small increments from top to bottom and side to side
- UAS are easier to spot on a cloud backdrop, so start your search there if possible
- Audible cues can also assist in determining the location
- If detection devices are used, information to help find and identify the threat are:
    - Positional information
    - UAS ID description
    - Time
    - Controller ID
    - Geofence penetration
    - Telemetry
    - Frequency

3.3 Operator Contact and Intrusion Mitigation

Local law enforcement, airport police, FAMs, and the FBI are the agencies best equipped to handle operator contact. Understanding the juristictional responsibilities of these agencies is critical to building a mitigation and communication plan. Information such as the location of the UAS, potential location of the operator, and best way to communicate those locations to law enforcment are important considerations for an effective response.

As discussed in Section 1.1.4, local law enforcement may not have a comprehensive understanding of FAA regulations and drone practices. For that reason, it is critical to engage with those law enforcmement agencies to provide training and information to help ensure an effective response when called upon.

Mitigation is a complex issue that is not in the purview of airports or local law enforcement. When necessary due to a credible persistent threat, a federal response can utilize mitigation techniques.

3.4 Remote ID

Remote ID is crucial for identifying a UAS that might be unlawfully operating in the NAS and vicinity of the airport. The concept allows for the reduction of careless/clueless operators near the airport by allowing the security personnel to easily identify the location of the UAS user; however, this does not address users with nefarious intent, who can use systems without remote ID capability. The Final Rule for remote ID became effective April 21, 2021. The latest information can be found here; a toolkit can be found here.

The remote ID concept comprises the following framework:

1. Owner registration of the UAS using the unique serial number assigned by the manufacturer
2. Broadcast and/or transmit remote ID data while operating the UAS
3. Remote ID UAS Service Suppliers (USS) will collect and store broadcasted/transmitted data from users on behalf of the FAA
4. Public access to data from Remote ID USS or through a personal device that can read a local broadcast

Remote ID can help the FAA, law enforcement, and federal security agencies track UAS by providing the following information:

- A unique identifier for the UAS
- The drone's latitude, longitude, geometric altitude, and velocity
- An indication of the latitude, longitude, and geometric altitude of the control station (standard) or take-off location (broadcast module)
- Time marks
- Emergency status (Standard Remote ID Drone only)

The current compliance date for manufacturers is October 21, 2022; for operators, the compliance date is October 21, 2023.

SECTION 4: RECOVERY

The level of effort necessary for recovery after a UAS threat is dependent upon the gravity of the incident itself. If the threat resulted in an accident, then the airport's accident recovery plan should be followed. This is typically detailed in the airport's AEP.

During recovery from a UAS threat, the most important element is to re-establish safe airport operations. For this to happen, the Aircraft Movement Area must be FAR 139 compliant (if applicable) and the AOA must be secure from any disturbances caused by the threat. The AEP should be followed at this stage, and updated in the next planning cycle to reflect necessary changes to address UAS threat recovery.

For the 2018 drone incident at Gatwick Airport, one of the hardest challenges was declaring an end to the threat and resuming normal operations. This was due to multiple factors, including inaccurate UAS reports from the public, an excitement level/malicious reports from the public, and a lack of detection capabilities. Even if an airport has detection systems installed, there likely will not be a complete system that can unequivocally ensure clear airspace and a neutralized threat. A sterile airspace per the detection system will just be one component of the decision to return to normal operations. The decision-making process for returning to normal operations is complicated, but airspace decisions will be led by the FAA with input from a unified command.

The recovery phase should also include detailed documentation of the event, including an incident report, damage assessments, and financial impacts. The UAS type, size, and operational characteristics should be documented, along with procedures taken to mitigate the impact of the threat.

4.1 Investigation

The airport's role in the investigation following a UAS threat will likely be assisting law enforcement in information gathering. The FAA asks that the following information be captured for investigation:

- Identity of operators and witnesses (name, contact information)
- Type of operation (hobby, commercial, public/governmental)
- Type of device(s) and registration information (number/certificate)
- Event location and incident details (date, time, place)
- Evidence collection (photos, video, device confiscation)

4.2 Communication Strategies

A UAS threat recovery decision should include appropriate stakeholders, as outlined in Section 1.1. These stakeholders should be provided a consistent set of threat assessment facts, and each should either concur or state their objection to returning to normal operations. The airport operator or central authority (if a unified command is established) will record the responses and declare a "situation normal" or "situation modified" position.

A process should be established for responding to requests for information regarding the incident from the public or the media. The public information officer should handle all interface with the media. The public information officer should disseminate information consistent with all other involved agencies.

4.3 Near Future Precautions

Following a UAS incident with criminal intent, secondary UAS may be deployed to cause further disruption. UAS incidents can also spur copycat actors inspired by the initial event. Directly following a UAS incident, it is important to remain vigilant of the area and take reports with a heightened preliminary threat level.

During this timeframe, which can vary depending on the level of public knowledge of the incident, there are additional precautionary measures that can be utilized. Examples include increasing the actionable range of detection systems, responding to all detected UAS sightings, and working with law enforcement and local media to ask for additional community participation in reporting suspicious UAS activity.

4.4 Community Involvement

Following an incident involving a UAS, it is important to take the lessons learned and impacts of the event to the community to better prepare for and lessen the likelihood of a future incident. Through social and local media, the incident can be used as a learning opportunity for the community to understand the implication of operating UAS near airports. The FAA developed a useful UAS Community Engagement Toolkit for this purpose.

4.5 Reflect and Review

After recovery from a UAS related threat, it is important for airport operators to foster an environment of continuous improvement by reviewing key phases in the UAS threat life cycle flowchart (Figure 1) and learn from their real world experience. All stakeholders involved in the incident should be engaged to identify lessons learned and areas of improvement. This should be used as an opportunity to update the AEP or UAS response plan and associated training materials to better prepare for future incidents.

SECTION 5: EXAMPLES AND CASE STUDIES

Some airports have taken steps in preparing a response plan for UAS threats. Two airports in particular, Tampa International Airport (TPA) and Dallas/Fort Worth International Airport (DFW) have led airports' preparedness to UAS threats. This includes developing working groups, conducting training and exercises, and installing detection infrastructure. The descriptions below include best practices from each airport collected through interviews and site visits.

5.1 Tampa International Airport

TPA has a robust response protocol to UAS threats. The airport installed a detection system, allowing them to view many commercial, off-the-shelf UAS flying in the airspace surrounding the airport. The airport has also developed training plans and held numerous tabletop exercises for their response plan.

In preparing for a UAS threat, the airport has broken its airspace into two areas. The first area is a monitor ring in which the airport will monitor any UAS reports and detections. The second area is an action ring in which a UAS presence will trigger a response. The operations manager will only call ATC if the UAS threat has been visually confirmed or the credible detection/report is above a preset altitude.

The airport has developed zoning and land-use rules for UAS operations. The airport uses heat mapping to identify problematic areas that see numerous UAS operations. To further prepare, the airport has worked with TSA and other stakeholders to train for UAS threats regularly. Commercial UAS operators in the area have been invited to participate in these exercises, furthering the airport's public engagement with the UAS community.

A response to an unauthorized UAS at TPA includes airfield operations and airport police. The TSA operations center is also notified of the response.

5.2 Dallas/Fort Worth International Airport

DFW has established a UAS working group, which meets four times per year for briefings and training. The group includes numerous key stakeholders: FAA, TSA, various airport departments, and airlines. The working group allows DFW to disseminate information and engage diverse perspectives in preparing for a response.

The airport also proactively installed UAS detection technology on the airfield, which the airport monitors to identify potential UAS threats. The airport has a documented response plan for UAS threats, and will respond to all unauthorized UAS threats within a specified detection zone. Each response differs depending on the threat level and location.

Each UAS detection within the specified detection zone is disseminated by the Integrated Operations Center to airport operations and law enforcement. The airport police have mutual aid agreements with local jurisdictions surrounding the airport that can assist with a response when needed. The ATCT is notified after the threat has been visually confirmed. To do this, the Integrated Operations Center dispatches airport operations and police personnel to search for the UAS and its operator. An investigation will be conducted on all unauthorized flights, and will include appropriate local, state and federal law enforcement agencies as needed.

DFW integrated UAS into their triennial exercise in 2018.

REFERENCES

Airport Safety and Airspace Hazard Mitigation and Enforcement (Section 383). FAA.gov. (2021). https://www.faa.gov/uas/critical_infrastructure/section_383/.

Berrick, Cathleen A. 2011. *Homeland Security: DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity.* GAO-10-106. Washington, DC: U.S Government Accountability Office.

Blue Ribbon Task Force. (2019). *UAS Mitigation at Airports*. https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf.

FAA, 2013. *PART 139 - Certification of Airports*. FAA, DOT, pp.533-534 https://www.govinfo.gov/content/pkg/CFR-2011-title14-vol3/pdf/CFR-2011-title14-vol3-part139.pdf

Google Maps. 2015. "McGhee Tyson Airport." https://www.google.com/maps/place/McGhee+Tyson+Airport/@35.810833,-83.993889,17z/data=!3m1!4b1!4m2!3m1!1s0x885c20e3d1be3533:0x2d8b24fc8a34c452

Gould, S., & Schroeder, M. (2004). *Man-Portable Air Defense System (MANPADS) Proliferation*. Fas.org. https://fas.org/programs/ssp/asmp/MANPADS.html.

Homeland Security Act of 2002. H.R. 5005, 107th Cong. (2002).

Long-term sustainability of current defense plans: Hearing before the Committee on the Budget, House of Representatives, 111th Cong., 1 (2009).

Might, C. (2017). *Unmanned Aircraft Integration*. Presentation, FAA.

Title 49: Transportation Part 1542—Airport Security Subpart C—Operations*, §1542.215 Law enforcement support*. Electronic Code of Federal Regulations (eCFR). (2021).

US Department of Transportation, Federal Aviation Administration. (2018). *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*.

APPENDIX A: EXAMPLE TABLETOP EXERCISE

The following tabletop exercise has been built using elements of a tabletop exercise provided by TPA.

Airport Background

- Airfield Infrastructure
  - 10,000 ft Runway 18/36L
  - 8,500 ft Runway 18/36R
  - Control Tower (Class B Airspace)
- Terminal Infrastructure
  - Terminal Building, landside access and parking located between parallel runway configuration
- Support
  - Airport Police immediately available
  - County Police available ad hoc
  - Airport Communications Center
  - Airport Operations personnel – Airside & Landside
  - ARFF

Initial Report

- **7:30 am:** Air traffic control is notified by a departing aircraft of a UAS maintaining its position at an altitude of 175 ft, approximately 800 ft west of Runway 18/36R. ATC, using binoculars, can see the UAS lights but is unable to recognize its type. ATC is unaware of any authorized UAS operations on the airfield or within the controlled LAANC (Low Altitude Authorization and Notification Capability) airspace.
- **Domestic Event Network (DEN) is activated**
- **ATC Advises Airport Operations and Airport Police**
  - What makes up a successful report?
  - Does ATC publish a NOTAM?
  - Discuss what Airport Operations asks/does
  - Discuss what Airport Police asks/does

Initial Report

- **7:46 am:** In the interest of safety, ATC suspends all arrivals and departures until the UAS hazard can be resolved. All landing aircraft are placed in a holding pattern, and aircraft waiting for departure on taxiways are directed to hold. As the suspension of operations is executed, the UAS is observed to no longer maintain a stationary position, and appears to be moving at a high rate of speed along Runway 18/36R.
- **7:55 am:** Airport Operations personnel performing a routine fence line inspection are able to get a better visual on the UAS. Airport Operations identifies the UAS as a white, hobby grade, multi-rotor platform with a single camera as a payload. The UAS operator is nowhere to be seen. Airport Operations personnel attempts to maintain a visual on the UAS and initiates a search for its operator on airport landside and airside facilities.
- **7:58 am:** Neither ATC nor Airport Operations personnel have visual of the UAS.

Initial Report - Discussion

- Who is responsible for directing the establishment of a command post at an airport during a UAS event? What organizational entities should be included as part of this multi-jurisdictional response effort? At what point would these entities be included?
- Discuss what local resources are available at and around the airport for deployment in response to a UAS event.
- What authorities currently exist to allow state or local personnel to actively defend against or interdict a UAS?
- Who communicates with the ATC to determine if the intent of the UAS is apparent? Discuss differences given a variety of the UAS's operational considerations – threatening aircraft in the air, on the ground, near buildings, or just loitering?

Response

- **8:30 am:** Airport Operations, ATC, TSA, and Airport Police have established a joint unified command.
- **8:35 am:** Local Police department joins the search for the UAS and the operator. The search is ongoing, but there have been no sightings of the UAS since 7:55 am.
- **8:55 am:** With no confirmed sightings for 60 minutes, local stakeholders agree that an "all-clear" may be called and direct to return to normal air traffic operations. Law enforcement remains in place in case the UAS returns.

Response - Discussion

- Who has the authority to announce an "all-clear" and how does the airport implement/ communicate the resumption of normal airport operations?
  - Is there a checklist to determine the "all-clear"?
  - Define the methodology
- How are interagency stakeholders engaging at the national level at this point?
- Can local law enforcement utilize the airspace above and/or near the airport following a full ground stop to search and interdict UAS operations?

Response - Continued

- **9:00 am:** As ATC is in the process of resuming normal operations, a UAS appears from the north and flies erratically at a high rate of speed over the terminal building. Airport Operations personnel determine that this UAS is a different system than the previous one. Airport Operations can only confirm that this UAS is orange, and is significantly smaller than the previous UAS identified.
- **9:05 am:** ATC suspends all departures again and issues a ground stop for all arrivals. Existing inbound aircraft are diverted to nearby airports, and departing aircraft on taxiways are directed to return to the terminal and to disembark passengers.

Response - Discussion

- What can be inferred from a second UAS appearing at the airport within minutes of operations resuming? How can/could this be mitigated?

Operational Recovery

- **9:30 am:** The DEN establish a discussion with TSA TSOC (Transportation Security Operations Center) to identify ripple effects on the rest of the national airspace system, and consider the need for national level action.
- **9:45 am:** Neither UAS are visible, but local stakeholders decide to keep operations suspended until further notice.
- **10:30 am:** Social media posts regarding the airport shutdown have gained momentum and pressure is being applied to the state and federal government to resolve the UAS disruption.
- **12:00 pm:** In a joint discussion between the Airport Operator, TSA, local law enforcement, industry, ATC, and TSOC, the decision is made to re-open the airport and begin operations as normal. Radio chatter on ATC frequencies increases as actions are underway to re-open the airport. This likely happens via the ATCSCC (FAA Command Center) as they connect all parties for an info-share/collaborative decision.

Operational Recovery - Discussion

- How will media, political, and economic influences impact the response to a UAS event?
  - How is this handled?
  - Define communication protocols with governmental entities – city mayor/ governor
- How long should key local, state and federal resources remain engaged and on scene after the return of operations from a persistent UAS disruption?

Ongoing Issue

- **1:30 pm:** ATC observes two UAS coming onto the airfield from the northeast. Using binoculars, they identify the UAS as the white and orange systems observed earlier in the day.
- **1:35 pm:** ATC once again suspends all departures and arrivals at the airport. The FAA discusses with local and national-level stakeholders to ensure that threatening UAS activity is not resumed.
- **2:00 pm:** Law enforcement can determine that the UAS are not operating from a fixed location and the operators appear to have access to airport communications. The group establishes potential mitigation activities and a POC for each action.
- **4:00 pm:** Local officials reconvene and determine that they have exhausted all possible means to locate the UAS operators to prevent further disruptions. TSA and other field staff determine that locally based response efforts have been exhausted. As the situation has not been resolved, TSA proposes in the TSOC discussions that national-level response is needed—specifically, currently approved UAS mitigation capabilities (C-UAS).

Ongoing Issue

- **4:30 pm:** No sighting of the UAS, but the airport remains closed until currently approved C-UAS equipment arrives.
- **5:35 pm:** One of the two UAS previously identified appears from the southeast and is hovering near the ATC tower. This platform is once again identified as a white, hobby grade, multi-rotor platform with a single camera as a payload.
- **5:45 pm:** Federal authorities arrive onsite with C-UAS equipment. Once set up and activated, the local TSA representatives or Federal Air Marshal takes action to mitigate the UAS operating near the tower and is successful!
- **6:00 pm:** With no additional sightings of the second UAS, ATC moves to resume to normal operations. Federal authorities are standing by with C-UAS equipment.

Hot Wash

- What are some key takeaways from today's discussion that should be considered for action?
- How will DHS, DOE, DOD, and DOJ be compensated for deploying and operating C-UAS technologies and services?
- What additional authorities are needed at the local and federal levels to enhance response efforts?
- How can we better support joint interoperability between federal, state, and local law enforcement and key operational stakeholders?
- The current Federal CONOPS is projected to exist for 6–12 months, unless renewed. What document will supplement this guidance to ensure the airport continues to refine their local response efforts as UAS technology keeps advancing?

APPENDIX B: RECURRENT TRAINING TEST

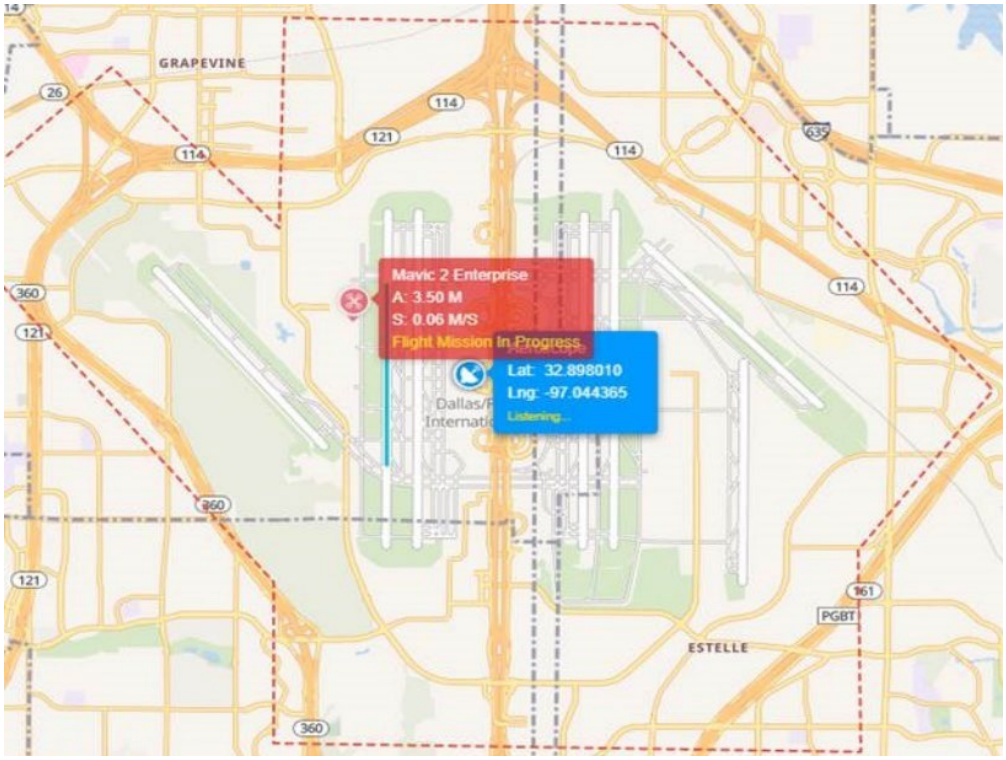
The following recurring training test is based on successful test of strategies conducted at DFW during the development of this guidebook.

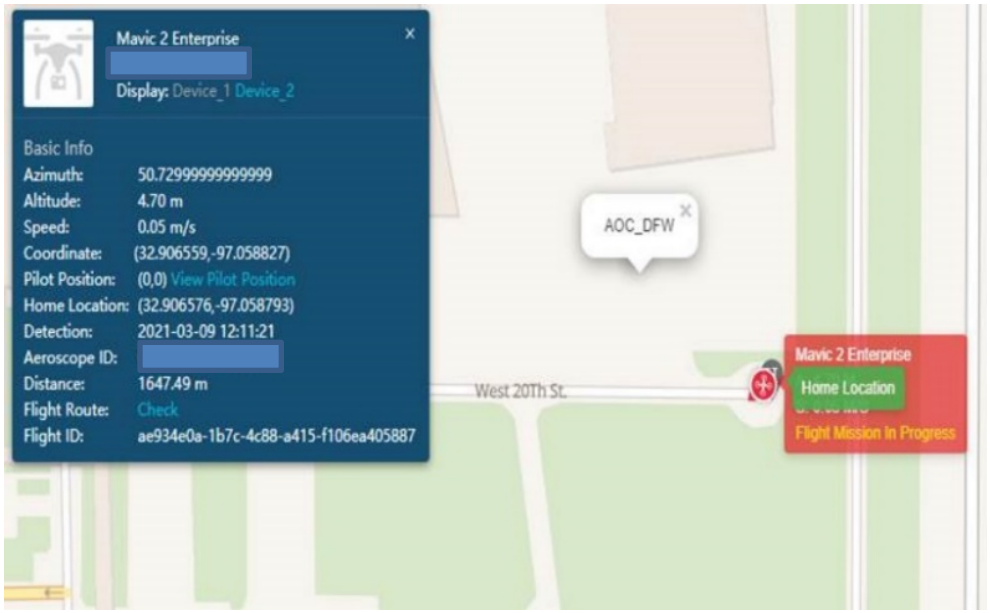
- Set a date and time to conduct the training. Obtain airspace authorization from the FAA to conduct the training. You should inform all necessary stakeholders of the testing, including ATC, pilots via a NOTAM, airport security, police, and operations. To ensure a successful training, this notification should not include specific details on the time and location of the test.

- Select and travel to the location. Have observers both at the UAS location and with key stakeholders, such as inside the airport communications center.

- Lift the UAS to a minimal height following all appropriate rules.

- If a detection system is installed, the UAS deployment should trigger a detection and response. If not, report a UAS sighting to the airport communication center.

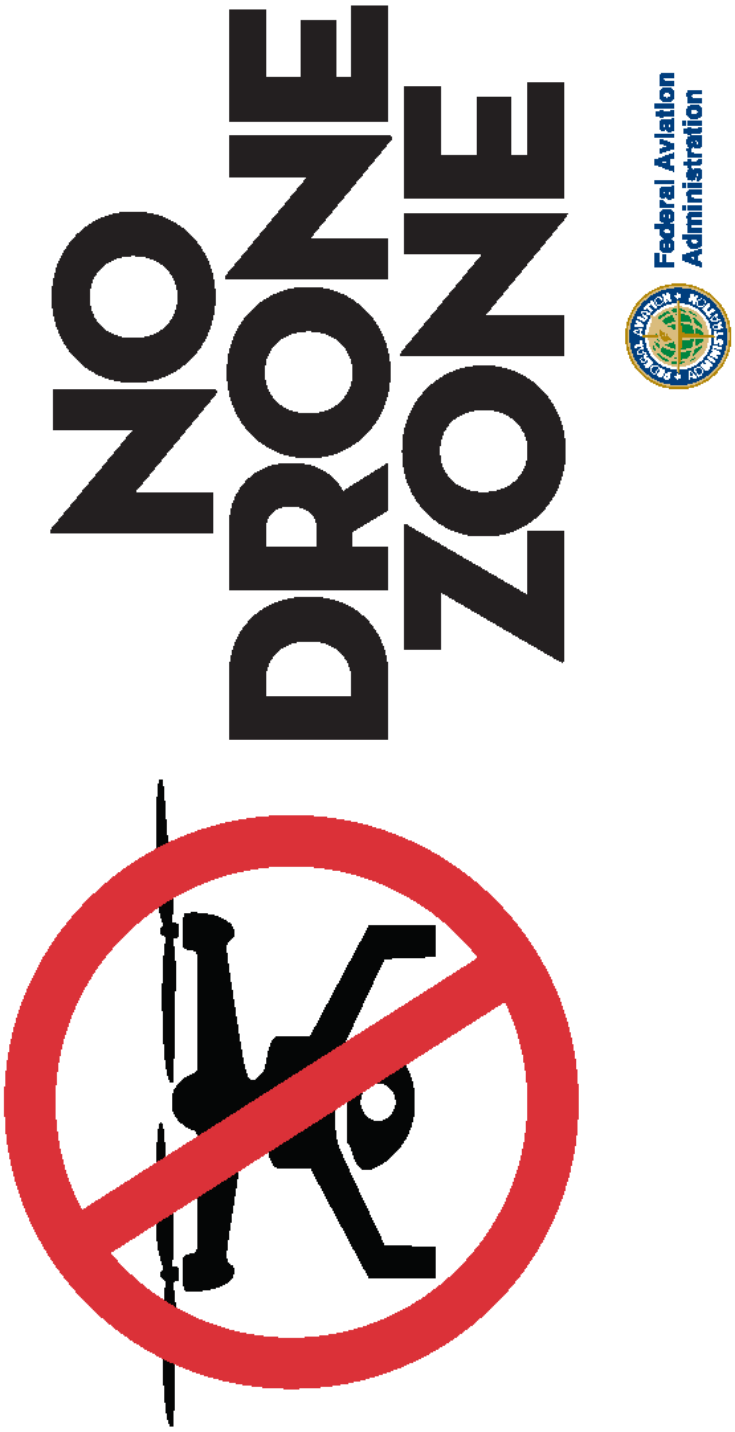




- Track the time and efficiency of the response. Key items to track include the time and type of information that is disseminated, the length of time until a confirmation of the threat, and the total number of responding personnel.
- Once the training is complete, land the UAS.
- Conduct a debrief and lead a lessons-learned conversation.
- Repeat this training for different personnel and scenarios.

APPENDIX C: COMMUNITY ENGAGEMENT SAMPLES

Federal Aviation Administration


NO DRONE ZONE
Federal Aviation Administration