# 61ST CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGION

*Kuala Lumpur, Malaysia*
*7 – 11 September 2026*

AGENDA ITEM 5: AVIATION SECURITY AND FACILIATION

# RECOMMENDED MITIGATION EFFORTS FOR UNMANNED AIRCRAFT SYSTEM THREATS AT AIRPORTS

(Presented by United States)

**INFORMATION PAPER**

**SUMMARY**

This paper outlines low-cost or no-cost recommended mitigation practices, based on the U.S. Transportation Security Administration's (TSA) experience, for addressing unauthorized unmanned aircraft systems (UAS) operations at civilian airports. The practices are derived from TSA's operational insights across four mission areas: policies and procedures, physical security, outreach and education, and training. The solutions are designed to reduce risks posed by careless, clueless, reckless, or negligent drone operators, enabling airport stakeholders to better focus resources on potential nefarious actors. For more information, refer to Appendix A of this Paper.

# RECOMMENDED MITIGATION EFFORTS FOR UNMANNED AIRCRAFT SYSTEM THREATS AT AIRPORTS

## 1. INTRODUCTION

1.1 Unmanned Aircraft Systems (UAS), or drones, are fundamentally changing the security landscape and as the commercial drone market continues to expand, this technology – whether employed by careless, clueless, reckless, negligent, or nefarious actors – presents an increasing threat to aviation security globally. In June 2025, U.S. President Donald J. Trump issued two executive orders, *Restoring American Airspace Sovereignty*[1] and *Unleashing American Drone Dominance*[2], which established a comprehensive UAS policy framework designed to protect the United States from the threats posed by UAS. The *Restoring American Airspace Sovereignty* order provides that it is the policy of the United States to ensure control over the national airspace and to protect the public, critical infrastructure, mass gathering events, and military and sensitive government installations and operations from threats arising from the careless or unlawful use of UAS. As part of the United States' comprehensive response framework for persistent airport disruptions caused by drones, the Transportation Security Administration (TSA) conducts airport vulnerability assessments to improve airports' preventive posture against drone threats.

1.2 Airport operations vary widely from location to location, creating unique environments with complex stakeholder needs and interests. A one-size-fits-all solution is not readily available. The attached guide (see Appendix A) consolidates several years of operational insights to present mitigation practices that airport stakeholders can tailor to their specific operational needs.

## 2. SCOPE AND APPROACH

2.1 The attached guide focuses on low-cost and no-cost solutions to reduce UAS-related risks from careless, clueless, reckless, or negligent drone operators at civilian airports to allow airport stakeholders to better concentrate their scarce resources on pursuing potential nefarious actors. While drones can be launched from anywhere and typically originate from off-airport property, the mitigation practices presented focus on actions airport stakeholders can implement within their own operational environments while encouraging cooperation with off-airport stakeholders. Airports should recognize that technological solutions alone are insufficient. Airports should reconceptualize existing security practices and equipment to address gaps that drones can uniquely exploit.

2.2 Four mission areas have been identified for comprehensive risk mitigation: (1) policies and procedures; (2) physical security; (3) outreach and education; and (4) training. This framework does not address the complex topics of Counter-UAS (C-UAS) technologies or changes that may need to be considered to national legal frameworks to enable such activities.

## 3. MISSION AREA 1: POLICIES AND PROCEDURES

3.1 Any new threat, such as UAS, necessitates the development of sound policies and procedures to mitigate the threat.

3.2 *Synergize Response Planning Efforts*. Airport communities must work collaboratively to ensure collective efforts address each airport's unique operating environment and response plans require regular updates to reflect changes in capabilities and personnel. At a minimum, all response plans should address the purpose, concept of operations, roles and responsibilities, communications and reporting, incident response, and close-out procedures.

3.3 *Exercise Response Capabilities*. Once response plans are developed, they must be tested to identify where written guidance falls short and where procedures can be improved.

---

1 https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/
2 https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/

3.4 *Information Sharing and Incident Tracking*. Regardless of potential data sharing frameworks or lack thereof, local jurisdictions should implement simple solutions to improve information sharing and ensure deconfliction among airport stakeholders, including procedures for "white-listing" authorized drone operations. Coordination with the civil aviation authority and the air navigation service provider regarding authorized drone operations and related regulatory requirements may also be helpful.

3.5 *Formalize Mutual Aid Agreements*. Given that airports often depend on off-airport law enforcement agencies to locate drone pilots, airports should formalize cooperative agreements establishing information sharing protocols, response radius, and reporting procedures.

## 4. MISSION AREA 2: PHYSICAL SECURITY

4.1 Drone technology is often evolving faster than the ability to develop and deploy viable solutions to counter it. A holistic approach to drone mitigation efforts at airports should consider updating existing practices and infrastructure to address current gaps in parallel with pursuing technology solutions.

4.2 *Harden Airport-Owned Property*. Airports should better secure vacant or underutilized land beyond operational areas and perimeter fencing through improved fencing, vehicle access limitations, enhanced signage, or other low-cost measures.

4.3 *Implement Construction-Related Protocols*. Construction contracts between vendors and airports should include language addressing drone use in projects, including any pre-/post-flight coordination or notification requirements.

## 5. MISSION AREA 3: OUTREACH AND EDUCATION

5.1 A people-centric approach to reducing risk can be achieved by educating various airport populations via targeted drone safety campaigns.

5.2 *Airport and Airline Employees*. Airport and airline employees are well-positioned to support informal, multifaceted drone awareness programs. Many routinely interact with the traveling public – at ticket counters, for instance – and if well-informed, can serve as useful sources on how to conduct safe and lawful drone operations – such as the requirement to register certain drones, if one exists under national laws and regulations – which can help to mitigate the overall risk to airports.

5.3 *Traveling Public*. Airline passengers funnelled through screening checkpoints present opportunities for direct engagement, particularly with passengers traveling with drones in their cabin baggage.

## 6. MISSION AREA 4: TRAINING

6.1 Drone Awareness and Mitigation Training for all levels of airport employees is recommended and would provide essential knowledge and skills tailored to their specific roles and responsibilities, serving as a critical component of any airport security plan. Coordination with the civil aviation authority, the air navigation service provider, and other entities that may be involved in regulating drone operations at the national level is encouraged to maintain accurate and up-to-date training as States increasingly integrate drones into their airspace.

6.2 *Public-Facing Employees*. Public-facing employees (i.e., ticket and gate agents, flight crews, retail and screening professionals) required to complete regular training should receive incorporated drone awareness training that covers the rules and regulations governing safe operations.

6.3 *Non-Public Facing Employees*. Non-public facing employees (i.e., maintenance or catering professionals operating in airport operational areas) should receive the same baseline drone awareness training as public-facing employees, as well as receive training on reporting drone sightings during normal duties and properly responding to unauthorized drones discovered on airport property to protect employees and safeguard potential evidence.

6.4 *Law Enforcement*. Airport law enforcement must possess legal knowledge and training to interact with drone operators encountered on or near airport property and understand how to further civil and criminal prosecutions when appropriate. Law enforcement personnel may be able to repurpose existing optical equipment (i.e., binoculars, night-vision goggles, thermal devices) to support drone sighting confirmation. Law enforcement personnel should also form UAS working groups or task forces as mechanisms for agencies to discuss issues and operate under common frameworks for joint operations and real-time threat response.

## 7. CONCLUSION

7.1 The growth and evolution of drone technologies, coupled with increasing legitimate drone use at airports, presents real security challenges requiring continuous adaptation. The mitigation practices outlined in the guide represent practical, implementable solutions that airport stakeholders can tailor to their unique operational environments to improve security posture against unauthorized drones.

7.2 Continued international cooperation, regular information exchange, and collaborative problem-solving remain essential to maintaining global aviation security in the face of this dynamic and evolving challenge. To that end, at the Thirty-Seventh ICAO Aviation Security Panel of Experts (AVSEC Panel) meeting in April 2026, the Working Group on Guidance Material (WGGM) noted an interest in developing guidance material on C-UAS measures with the support of national experts and other relevant working groups, to include the Working Group on Innovation in Aviation Security (WGIAS). Consequently, the United States stands ready to engage with interested States and international partners to further develop and refine these mitigation approaches, including contributing to the work of the WGGM.

## 8. ACTION BY THE CONFERENCE

8.1 The Conference is invited to note the information contained in this Paper.

— END —

**APPENDIX A**

**U.S. Transportation Security Administration**
**Recommended Mitigation Efforts for Reducing Risks Associated with Unauthorized Unmanned Aircraft Systems Operating in the Aviation Sector**

## Introduction:

Unmanned Aircraft Systems (UAS), or drones, are changing the homeland security landscape. As the commercial market grows, this technology – whether employed by a careless/clueless, reckless/negligent, or nefarious actor – will only become a greater threat to homeland and aviation security.

Following the December 2018 Gatwick incident in the United Kingdom, and the January 2019 incident at Newark Liberty International Airport, the United States Federal government laid out a roadmap for responding to a *persistent disruption* at an airport. As a result, TSA was designated as the Lead Federal Agency for responding to this threat. As the operational element of TSA, the Federal Air Marshal Service (FAMS) has embraced this mission space to reduce the risks unauthorized drones pose to airports.

Airport operations can vary widely from location to location, making for unique environments. Given this reality – and the sometimes-competing needs and interests of various airport stakeholders – one must recognize that "one-size-fits-all" solutions to this problem are not always feasible.

Therefore, TSA has undertaken a variety of left-of-launch initiatives intended to reduce the risk that unauthorized drones pose to an airport. These efforts include vulnerability assessments, outreach and education, policy initiatives, training, and exercises.

The growth and evolution of drone technologies – coupled with the fact that drones are increasingly being used at airports for legitimate purposes – present real security challenges that must be addressed to keep pace with these facts on the ground. This publication brings together several years of operational insights to put forth mitigation practices and considerations that airport stakeholders can tailor to suit their needs, with the goal of improving an airport's security posture against unauthorized drones.

## Scope:

This publication is intended to highlight ways to reduce UAS-related risk at civilian airports through the implementation of low-cost, no-cost solutions aimed at the careless/clueless or reckless/negligent drones operating around airports. By reducing this population, airport stakeholders are better able to concentrate their scarce resources on the pursuit of potential nefarious actors. While a drone can be launched from anywhere and, typically, drone flights that impact an airport originate off airport property, the mitigation practices in this publication are focused squarely on what airport stakeholders can specifically do with respect to their own operational environments – namely, inside the bounds of airport property. This does not discount the imperative for airport communities to collaboratively work with stakeholders off airport property to effectuate change; it simply offers solutions that can be readily implemented at the lowest levels possible.

Based on these parameters, four mission areas have been identified: ***policies and procedures, physical security, outreach and education, and training.*** Within this framework, specific

recommendations for reducing risk are outlined, based upon the knowledge, training, and experience of TSA/FAMS counter-drone subject matter experts.

This publication does not seek to comment on complicated questions such as the employment of Counter-UAS (C-UAS) technologies or changes in national-level legislative frameworks. While C-UAS technology and legal frameworks play a critical role in developing domain awareness and potentially responding and disrupting malicious actors who can then be held accountable by law enforcement, these are complex and challenging topics that deserve their own dedicated discussion.

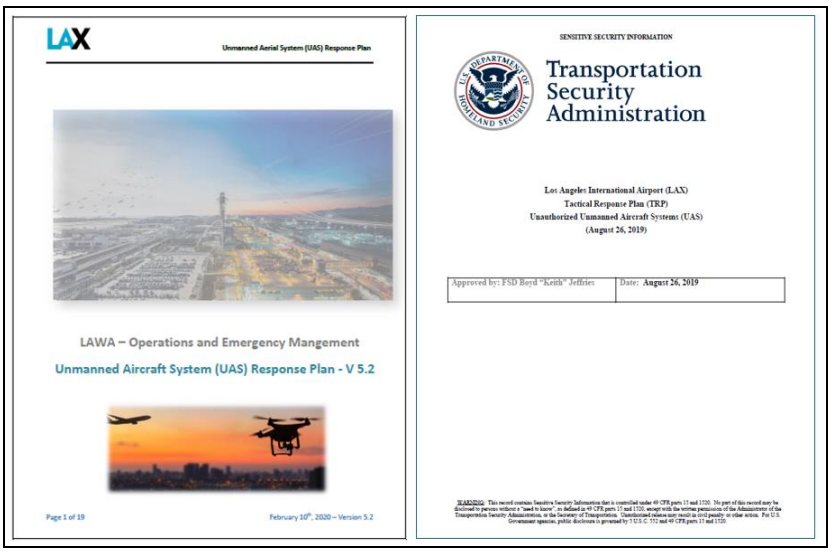
## **Mission Areas:**

### 1. Policies and Procedures

The advent of any new threat, be it a vehicle-ramming attack or active shooter scenario, necessitates the development of new policies and procedures that facilitate an organization's adaptation to its new environment. The UAS threat landscape is no different. It necessitates the development and implementation of policies and procedures that are tailored to deal with the unique issues pertaining to this threat.

#### *A. Synergize Response Planning Efforts*

A common refrain among airport stakeholders is that if you have seen one airport, you have seen one airport. Given how unique each airport's operating environment can be, airport communities must work together to ensure that their collective efforts address an airport's unique circumstances and are synced together to work in concert, not at cross-purposes. Furthermore, these policies and procedures need to be regularly updated to reflect changes in capabilities or personnel. Too often, response plans are not reflective of facts on the ground, have unresolved flaws, and do not align with agency-specific plans. At a minimum, all response plans should contain a statement of purpose, concept of operations, roles and responsibilities, communication and reporting procedures, incident response, and close-out procedures.




*Example: Drone Response Plans for Los Angeles International Airport*

#### *B. Exercise Response Capabilities*

Once airports have outlined their response planning efforts, those plans need to be put to the

test. Response capabilities should be exercised with the goal of highlighting where written guidance falls short. Initial exercises of this type should focus on table-top scenarios. The goal for these types of exercises should be to execute a practical exercise that tests all aspects of an inter-agency drone response in real time so that plans can be refined and reissued, as necessary.

### *C. Information Sharing and Incident Tracking*

Airports routinely deal with both technical and non-technical data sharing gaps. This problem may be further exacerbated for some states by the absence of national-level information sharing tools in this mission space, such as a national incident database, that provides this capability across areas of responsibility. While these concerns demand comprehensive solutions at the local, state and Federal levels, funding challenges and complex integration issues can be difficult to overcome.

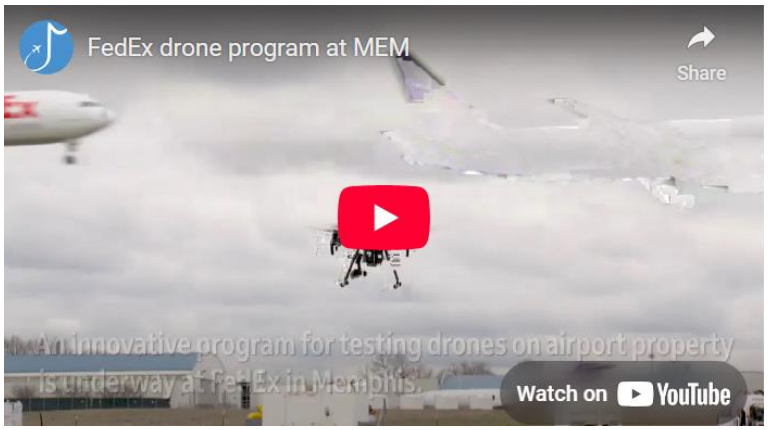
In the interim, local jurisdictions can implement simple solutions that improve information sharing and better ensure deconfliction among all airport stakeholders. This should include procedures for "white-listing" authorized drones operating near airports to eliminate miscommunication and the deployment of scarce resources to interdict approved operators.


Airport stakeholders have also embedded personnel in regional or state-level fusion centers to facilitate information sharing across agency domains. Examples include TSA/FAMS participation in regional fusion centers like the Delaware Valley Intelligence Center, where FAMS representatives are involved in UAS and C-UAS analytical and operational support functions. This work includes incident reporting and data sharing and analysis, support for intelligence and risk assessments, and special event coordination.

### *D. Formalize Mutual Aid Agreements*

Given the nature of the drone threat, airports are often dependent on the support of agencies operating off airport property to locate and interdict drone pilots. Airports, in consultation with surrounding law enforcement agencies, should agree upon information sharing protocols, response sectors and radius, and reporting procedures. The formalization of these cooperative agreements sets expectations and ensures accountability among stakeholders.

Since 2023, FedEx, in partnership with the Memphis International Airport, has been utilizing drones for various operations, including aircraft inspections, ramp security monitoring, and perimeter fence surveillance as part of the FAA's BEYOND Program. Innovative drone activities such as these require deconfliction and close coordination with airport stakeholders.




https://youtu.be/ShlJ6r_4CXs

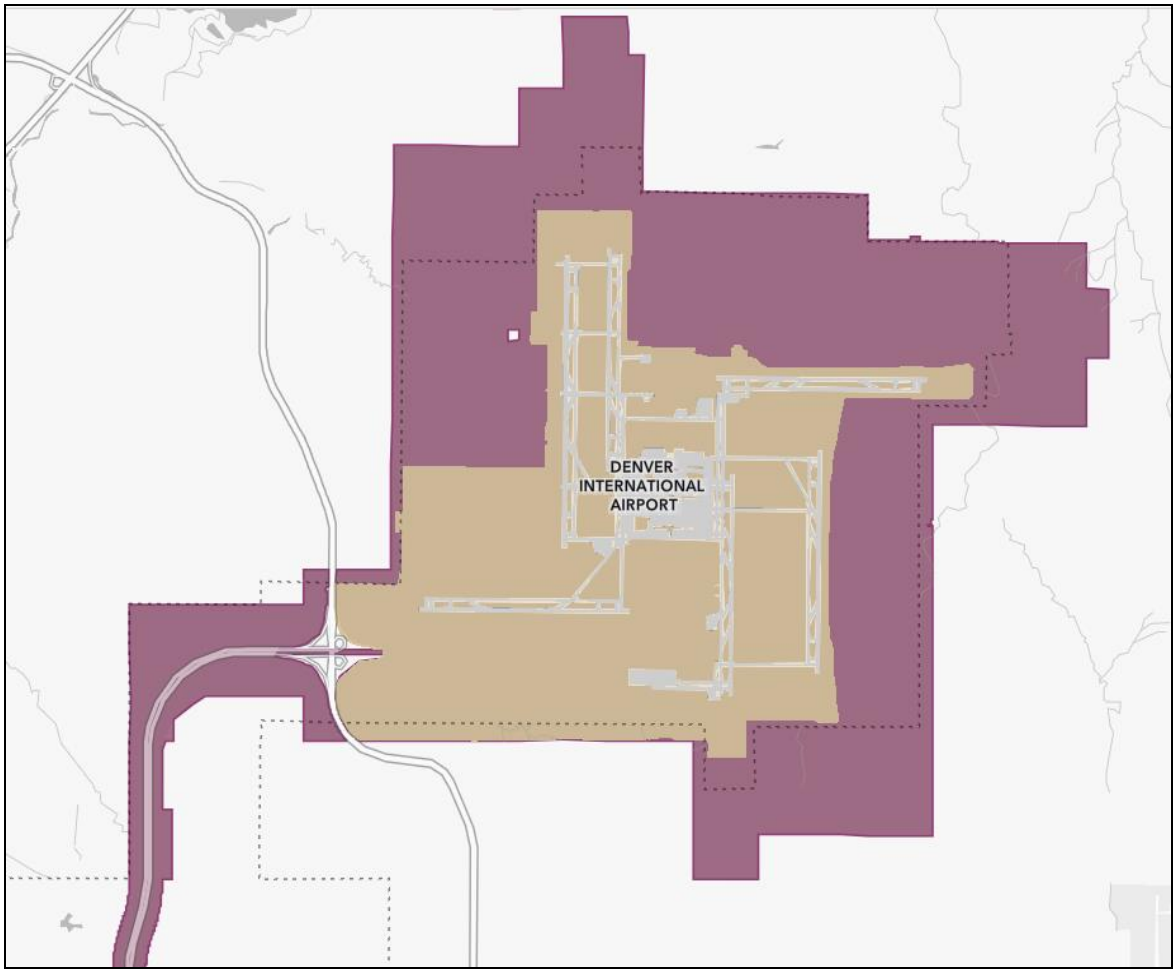
*Example: Memphis International Airport Collaboration with Airport Stakeholders*

## 2. Physical Security

Often drones are represented as a wholly unique threat that can only be mitigated through the implementation of sophisticated technological solutions. There is no question that technology continues to play a critical role in mitigating the threat drones pose to airports. However, airport stakeholders should recognize that there will always be a gap between the evolution of drone technology and the development of new equipment designed to counter drones. In addition to the pursuit of technological solutions consistent with applicable national law, airports should look at reconceptualizing existing physical security practices and equipment to address existing gaps that can otherwise be uniquely exploited by drones.

### *A. Harden Airport-Owned Property Against the Drone Threat*

Airports typically own large tracts of vacant or underutilized land beyond an airport's operations area. These areas may fall outside of the perimeter fencing that must meet specific national regulations to prevent unauthorized public access. These areas are not typically supposed to be publicly accessible, but they may seldom be visited by airport employees, and importantly, can offer excellent vantage points for aircraft viewing or other, potentially malicious, acts. Airports should look to better secure these areas to prevent them from being used by reckless or nefarious actors. These mitigation efforts can include improved fencing, vehicle access limitations, new or improved signage, and other low-cost countermeasures. Pushing unauthorized drone pilots farther out from an airport's critical nodes of operation reduces the amount of time a drone can cause an airport disruption. Increasing the amount of time it takes for a drone to reach airport property means that the drone has less battery life to sustain any unwanted activity.




*Example: Denver International Airport Operations Area (tan) vs. Airport Owned Property (purple)*

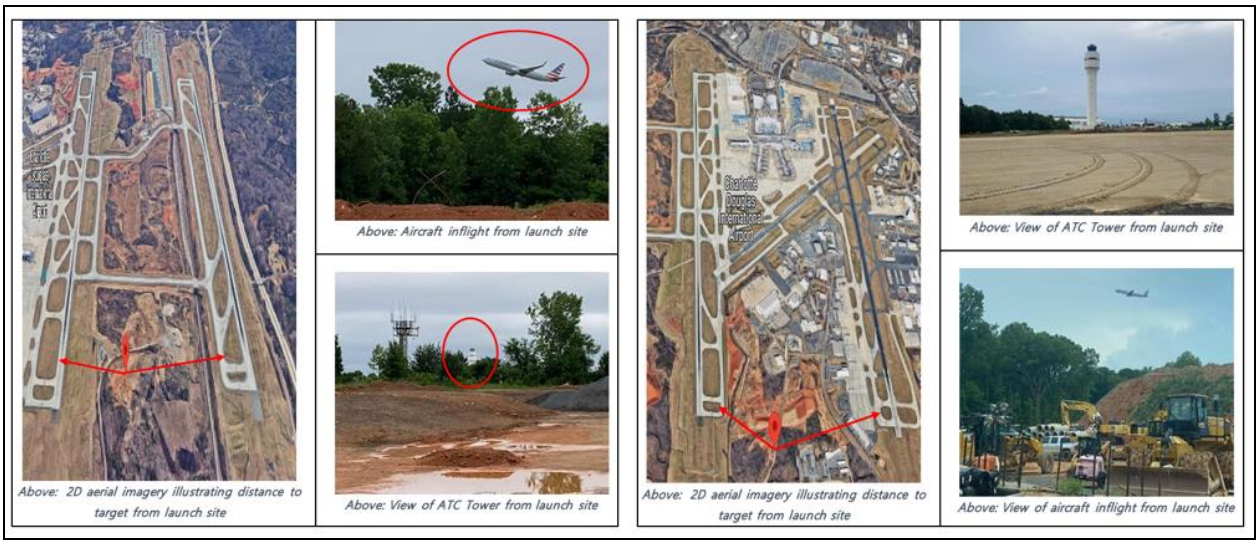

*Example: Security Vulnerabilities at a U.S. Airport*

*B. Implement Protocols for Construction-Related Efforts*

Airports routinely undergo construction that takes place adjacent to or inside the aviation operations area. These circumstances can introduce the need for UAS flights to monitor construction progress and/or facilitate operations. Any new construction contract between a

vendor and the airport should have language addressing the use of drones in their projects. Because most construction companies use UAS, a formal agreement between the airport and the vendor will establish a contractual obligation to ensure that any contracted operator abides by all current regulations and notifies all parties of their applicable relevant flight operations.

Additionally, as new or refurbished construction efforts are underway within the airport environment, buildings and infrastructure can be outfitted with basic physical upgrades to protect them from errant or malicious UAS. One example is the placement of anti-bird netting at observation areas or parking garages to prevent the launching of UAS from these locations.




*Example: Construction Projects or Accessible Staging Areas at an Airport*

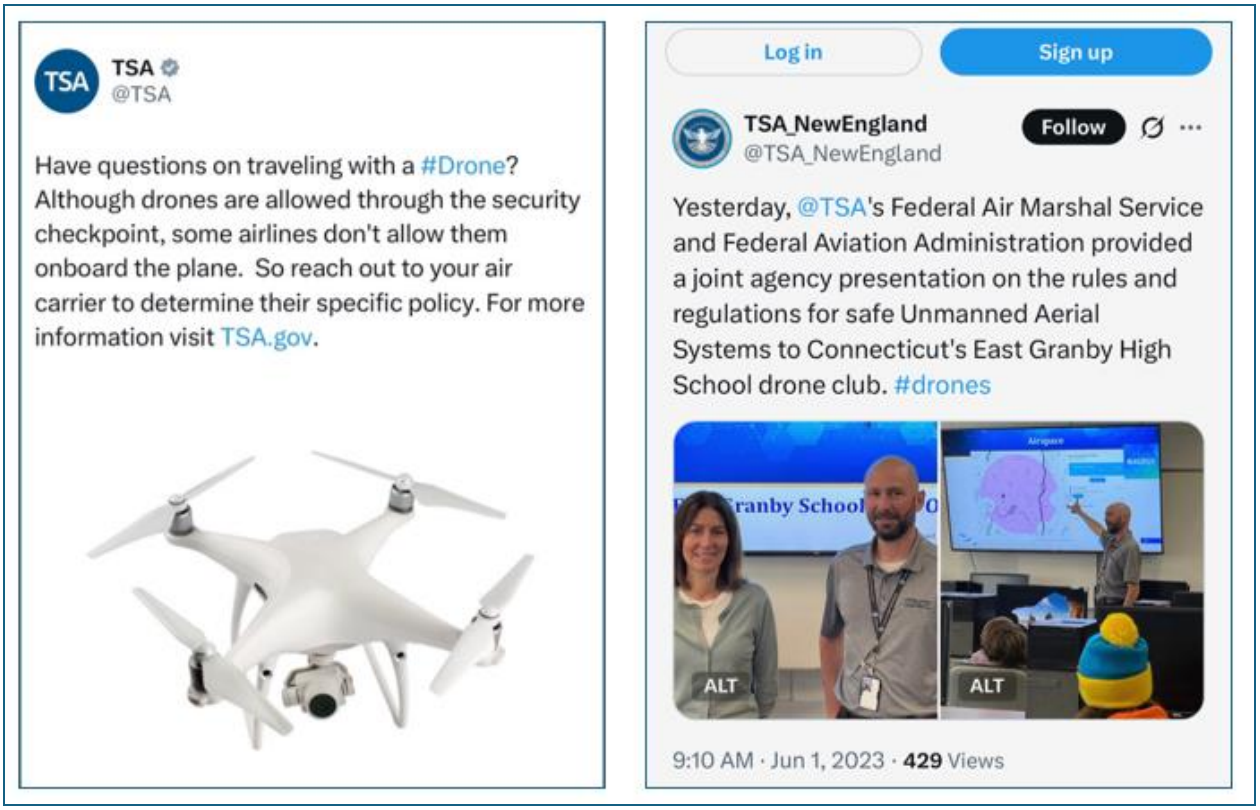
*Example: Anti-Bird Netting Deployed at Public Parking Garages*

### 3. Outreach and Education

A people-centric approach to reducing risk can be achieved by educating various airport

populations via targeted drone safety campaigns. These campaigns can broadly cover the rules and regulations governing drone use and employ a variety of tools to reinforce this message: no drone signage, social media campaigns, public service announcements, QR codes linked to handouts, press events, and even airport billboards. In addition to raising drone awareness around the airport, more focused information can be targeted to specific airport populations.


*Example: Common No Drone Zone Signage*




*Example: Social Media Outreach Efforts*

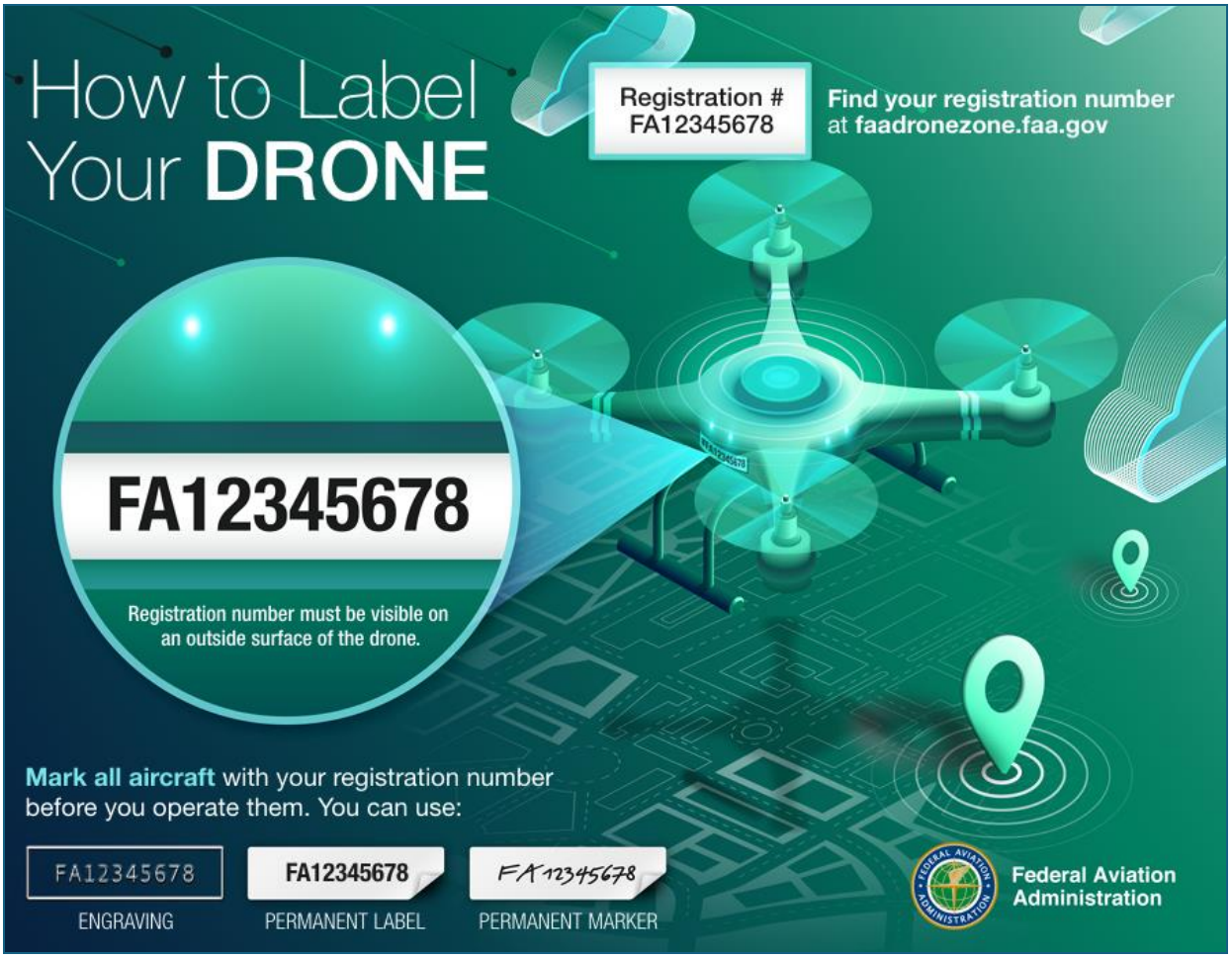

*Example: Miami Herald News Article Highlighting the Dangers of Spring Breakers Operating Drones Near Miami International Airport (2016)*

*A. Airport and Airline Employees*

Airport employees are well positioned to support all aspects of a multifaceted drone awareness and reporting program. Many airport employees routinely interact with the flying public and are uniquely positioned to be useful sources on this subject. Airline personnel, particularly pilots and crew who move around the country routinely, spend a great deal of time within an airport's broader ecosystem – hotels, restaurants, transportation hubs – and are uniquely situated to engage with and educate the public. Employees should be given access to briefing materials and handouts as well as feedback mechanisms that allow for questions to be asked and answered, particularly if they encounter unfamiliar situations. This could be in the form of a general email address, a specific point of contact at the airport, or coordination between the airport and a recognized expert from another government organization.

*B. Traveling Public*

Within the airport environment, the traveling public represents a captive audience primed to receive critical messaging on existing drone regulations and the importance of drone safety. In addition to the messaging formats outlined above, airline passengers are all funneled into one-on-one engagements at airline counters and screening checkpoints. This presents opportunities for direct engagements, particularly if passengers are traveling with a drone. These professionals can take the opportunity to engage in a targeted discussion – such as drone registration requirements contained in the State's national legislation or regulations – or more broad-based discussions on drone safety. All topics discussed can be referenced via QR codes or flyers posted in the immediate area to provide passengers with additional information.




*Example: U.S. Instructions on How to Label Your Drone (FAADroneZone Access - Register)*

**4. Training**

Dedicated training efforts that provide various employee groups with the tools they need to be effective within their unique roles and responsibilities are a key aspect to any airport's security plan. In this context, training efforts should cover broad-based objectives as well as targeted efforts that are specific to different employee populations. Many airports across the country have already begun to incorporate drone awareness training into their security preparedness programs.

*A. Public-Facing Employees*

Public facing employees who regularly interact with the flying public, such as ticket and gate agents, flight crews, retail and screening professionals, are all required to complete regular training requirements as a condition of their employment, similar to the Security Identification Display Area training requirement.

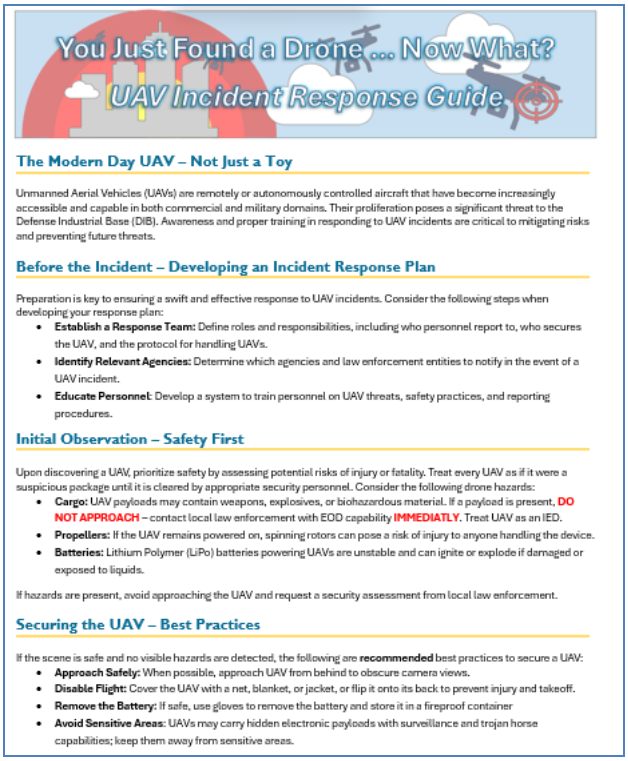
This training requirement should incorporate drone awareness training information, including the rules and regulations governing safe operations. In addition to this baseline information, public-facing employees should receive specialized training on how to interact with the flying public who may be traveling with drones, and how to report unsafe drone activity.

*B. Non-Public Facing Employees*

Non-public-facing employees, such as maintenance or catering professionals operating in the

airport operations area, are also required to complete regular training requirements, and should receive the same baseline drone awareness training as public-facing employees. In addition to this training requirement, non-public-facing employees should receive training on how to report drone sightings during the course of their normal duties, as well as how to properly respond to the presence of unauthorized drones they may find on airport property. This is an important aspect of protecting employees and safeguarding potential evidence.

*Example: Drone Discovered on an Aircraft Wing at a U.S. Airport by Maintenance Professionals*



You Just Found a Drone... Now What?

UAV Incident Response Guide

**The Modern Day UAV – Not Just a Toy**

Unmanned Aerial Vehicles (UAVs) are remotely or autonomously controlled aircraft that have become increasingly accessible and capable in both commercial and military domains. Their proliferation poses a significant threat to the Defense Industrial Base (DIB). Awareness and proper training in responding to UAV incidents are critical to mitigating risks and preventing future threats.

**Before the Incident – Developing an Incident Response Plan**

Preparation is key to ensuring a swift and effective response to UAV incidents. Consider the following steps when developing your response plan:

- **Establish a Response Team:** Define roles and responsibilities, including who personnel report to, who secures the UAV, and the protocol for handling UAVs.
- **Identify Relevant Agencies:** Determine which agencies and law enforcement entities to notify in the event of a UAV incident.
- **Educate Personnel:** Develop a system to train personnel on UAV threats, safety practices, and reporting procedures.

**Initial Observation – Safety First**

Upon discovering a UAV, prioritize safety by assessing potential risks of injury or fatality. Treat every UAV as if it were a suspicious package until it is cleared by appropriate security personnel. Consider the following drone hazards:

- **Cargo:** UAV payloads may contain weapons, explosives, or biohazardous material. If a payload is present, **DO NOT APPROACH** – contact local law enforcement with EOD capability **IMMEDIATLY**. Treat UAV as an IED.
- **Propellers:** If the UAV remains powered on, spinning rotors can pose a risk of injury to anyone handling the device.
- **Batteries:** Lithium Polymer (LiPo) batteries powering UAVs are unstable and can ignite or explode if damaged or exposed to liquids.

If hazards are present, avoid approaching the UAV and request a security assessment from local law enforcement.

**Securing the UAV – Best Practices**

If the scene is safe and no visible hazards are detected, the following are **recommended** best practices to secure a UAV:

- **Approach Safely:** When possible, approach UAV from behind to obscure camera views.
- **Disable Flight:** Cover the UAV with a net, blanket, or jacket, or flip it onto its back to prevent injury and takeoff.
- **Remove the Battery:** If safe, use gloves to remove the battery and store it in a fireproof container
- **Avoid Sensitive Areas:** UAVs may carry hidden electronic payloads with surveillance and trojan horse capabilities; keep them away from sensitive areas.

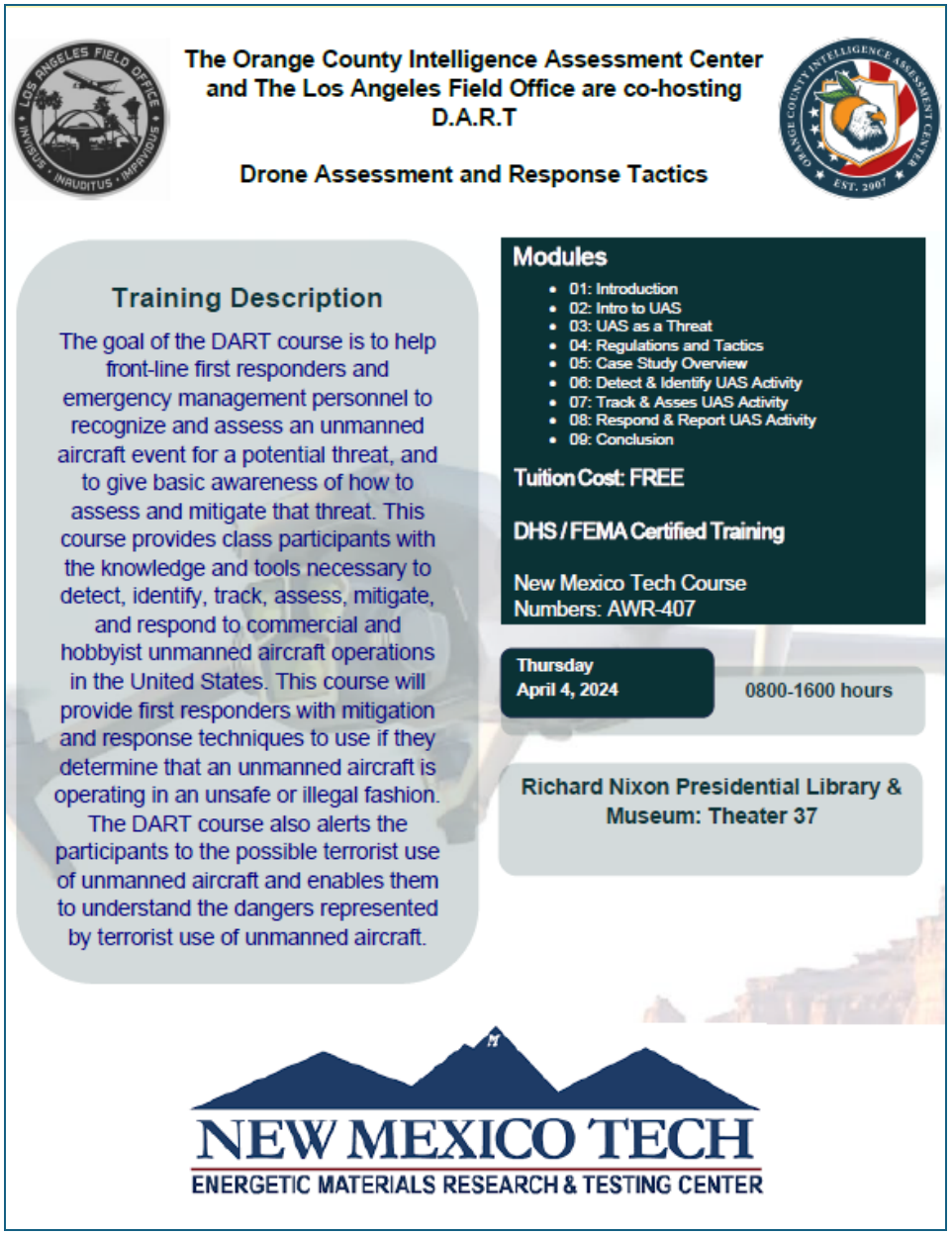
*Example: Organizational Briefing Material Outlining How to Safely Respond to a Pilot or Drone*

*C. Law Enforcement*

Law enforcement professionals working at airports are uniquely positioned to drive down the risk drones pose to aviation, particularly after they have been properly trained. In addition to receiving the same baseline information as other airport employees, law enforcement professionals must have a working knowledge of all national laws and regulations applicable to drone operations, such as remote pilot and aircraft registration requirements, drone-related operating requirements, and unsafe operation penalties. In addition to this legal framework, local law enforcement personnel must be familiar with specific local laws in their jurisdiction, like laws prohibiting the take-off or landing of drones from specific areas surrounding an airport, such as public parks.

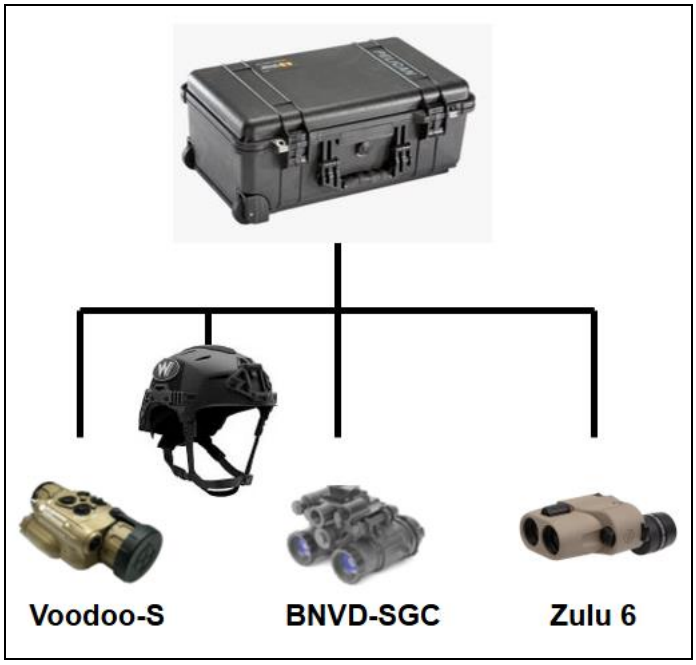

*Example: FAA Remote Pilot in Command Licensure*

Airport law enforcement must have the legal knowledge and training to interact with drone operators they encounter on or just off airport property and understand how to further civil and criminal prosecutions, when appropriate.




*Example: Federal Emergency Management Agency-Sponsored Drone Assessment and Response Tactics (DART) Training Held in Southern California*

Law enforcement personnel may also be able to repurpose existing optical equipment like binoculars, night-vision googles or thermal devices to support attempts to confirm reports of drone sightings. Effective utilization of this type of common law enforcement equipment, coupled with training about airspace awareness, deconfliction practices, observation tools and techniques – including effective ranging and reporting of confirmed sightings. To ensure proficient utilization of this type of equipment, officers should participate in practical training exercises to develop these capabilities.




*Example: FAMS' Optical Equipment Used to Support Visual Reporting Efforts*

Law enforcement personnel should also come together to form UAS working groups or task forces like the Federal Bureau of Investigation (FBI)-led C-UAS Task Force out of Los Angeles, California. The task force includes law enforcement participants from local, state, and Federal entities, including TSA/FAMS, FAA, United States Coast Guard, United States Secret Service, Los Angeles Police Department, and Los Angeles County Sheriff's Department.

*FBI C-UAS Task Force*

These types of groups provide a mechanism for agencies to discuss issues and come together under a common operational framework to conduct joint operations and address threats in real time. Regular interactions ensure that all agencies share a common understanding of the threat and mitigation resources available.

**<u>Conclusion</u>:**

The rapid proliferation of UAS presents evolving challenges to the security and operations of civilian airports. As demonstrated, a holistic approach – encompassing robust policies and procedures, physical security enhancements, targeted outreach and education, and comprehensive training – is an essential building block for mitigating the risks posed by unauthorized drones. While technological solutions and legislative measures remain important, airport stakeholders can take immediate, practical steps to address threats within their operational environments. By adopting the recommended practices outlined in this guide, airports can reduce the risk posed by certain drone operators, allowing resources to be focused on more serious threats. Continued collaboration, information sharing, and adaptation to this evolving threat will be critical to maintaining the safety and security of the nation's aviation sector in the face of this dynamic and persistent challenge.

**For more information, please contact your local TSA Representative.**

— END —