



ICAO

International Civil Aviation Organization  
North American, Central American and Caribbean Office  
INFORMATION PAPER

NACC/DCA/14— IP/14  
15/05/26

**Fourteenth Meeting of the North American, Central American and Caribbean  
Directors of Civil Aviation (NACC/DCA/14)  
St. George's, Antigua and Barbuda, 1 to 5 June 2026**

**Agenda Item 5: Every Flight is Secure**

**RECOMMENDED MITIGATION EFFORTS FOR UNMANNED AIRCRAFT SYSTEMS THREATS AT AIRPORTS**

(Presented by the United States)

**EXECUTIVE SUMMARY**

This paper outlines low-cost or no-cost recommended mitigation practices, based on the U.S. Transportation Security Administration's Federal Air Marshal Service (FAMS) experience, for addressing unauthorized unmanned aircraft systems (UAS) operations at civilian airports. The practices are derived from FAMS 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 information paper.

<i>Strategic Objectives:</i>	<ul style="list-style-type: none"><li>• Every Flight is Safe and Secure</li></ul>
<i>References:</i>	<ul style="list-style-type: none"><li>• ICAO Annex 17 – Aviation Security</li><li>• ICAO Doc 8973 – Aviation Security Manual</li></ul>

**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. As part of the United States' comprehensive response framework for persistent airport disruptions caused by drones, the Transportation Security Administration (TSA) Federal Air Marshal Service (FAMS) 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 guide (*see Appendix*) 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 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 legislative fixes.

## 3. MISSION AREA 1: POLICIES AND PROCEDURES

3.1 Any new threat, such as UAS, necessitates the development of new 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.

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.

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

#### **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 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 authoritative sources on how to conduct safe and lawful drone operations – such as the requirement to register certain drones – which can help to buy down the overall risk to airports.

5.3 *Traveling Public.* Airline passengers funnelled through screening checkpoints present opportunities for direct engagement, particularly when traveling with drones in carry-on luggage.

#### **6. MISSION AREA 4: TRAINING**

6.1 Counter-UAS and Drone Awareness Training for all levels of airport employees provides essential knowledge and skills tailored to their specific roles and responsibilities, serving as a critical component of any airport security plan.

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

6.3 *Non-Public Facing Employees.* Non-public facing employees (maintenance or catering professionals operating in airport operational areas) should receive the same baseline drone awareness training as public-facing employees and 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 can repurpose existing optical equipment (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 represents 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. The United States stands ready to engage with interested States and international partners to further develop and refine these mitigation approaches.

-----

## APPENDIX

### 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 the aviation sector.

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.

Given this reality, FAMS 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 – presents 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 across the country 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 action 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 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 legislative fixes. While C-UAS technology and legal structures 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 discussion.

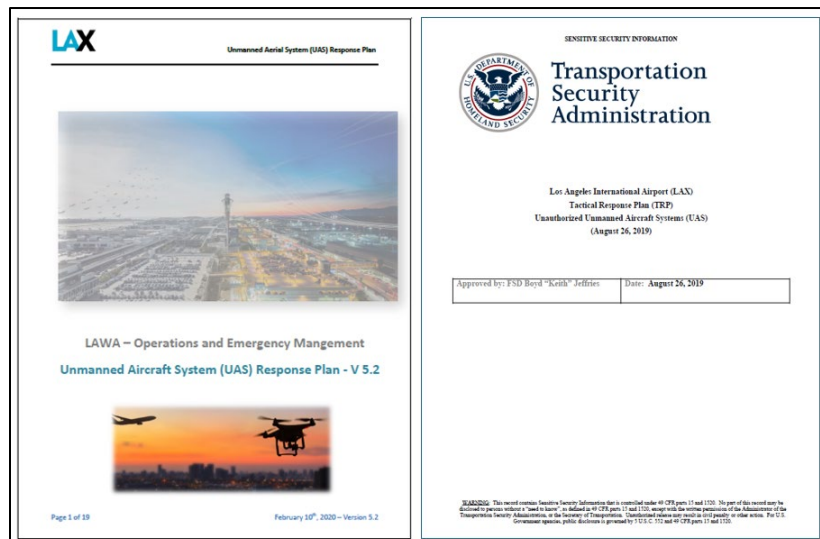
**Mission Areas:**

**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 which help to facilitate an organization’s adaptation to their new environment. The UAS threat landscape is no different. It necessitates the development and implementation of dedicated policies and procedures that are crafted 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’ve seen one airport, you’ve 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.



## 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 the eventual organization of a practical exercise that tests all aspects of an inter-agency drone response in real time so that plans can be refined and reissued.

### C. Information Sharing and Incident Tracking

Airports routinely deal with both technical and non-technical data sharing gaps. This problem is further exacerbated 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 in close proximity to 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 the FAMS’ participation in regional fusion centers

like the Delaware Valley Intelligence Center, where FAMS representatives are involved 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.



To differentiate between the Federal Aviation Administration (FAA) authorized drone operators and unauthorized drone violators, Massachusetts State Police set up a workflow for authorized operators to email their flight operation plan directly to [dronereport@mass.gov](mailto:dronereport@mass.gov). This simple information sharing mechanism allowed stakeholders to differentiate being legitimate and illegitimate operations until real-time access to FAA data became widely available. In September 2025 FAMS developed a geospatial tool to operational its access to FAA’s Drone Information Safety, Compliance, Verification and Reporting (DISCVR) Tool which was subsequently made available to state and local fusion center users. Work arounds of this type highlight the importance of creative solutions to complex, multi-agency problems until technological or legal fixes can be implemented.

### D. Formalize Mutual Aid Agreements

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.



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.

BWI Unsafe or Unauthorized UAS/Drone Response Management System			
Airport Policies	Airport Operations Risk Management	Airport Safety Assurance	Airport Safety Promotion (Culture)
<ul style="list-style-type: none"> <li>MD Code Transportation Title 5- Aviation Subtitles 10 and 11</li> <li>MDTA Police – AA County MOU (add drone assistance discussion TBD) 4-mile radius response</li> <li>MAA UAS / Drone website PSA?</li> <li>ACM AEP FAA LawCert Alert 21-04 Responding to unauthorized UAS operations</li> <li>ASP Response Protocol (SSI)</li> </ul>	<ul style="list-style-type: none"> <li>BWI – FAA Operational and/or Ground Stops</li> <li>Security breaches</li> <li>FAA Alerts I, II, III</li> <li>Campus-wide situational awareness using FAA BWI UAS Authorization database, visual inspections and approved technologies</li> <li>Incident tracking and trend analysis</li> <li>Continuous threat assessments</li> </ul>	<ul style="list-style-type: none"> <li>Daily safety and security compliance audits</li> <li>Monthly stakeholder SMS meetings</li> <li>2021 FAA Part 77 Aeronautical Study / Operational Implementation Approval / UAS Technology</li> <li>BWI safety, security and crime prevention efforts</li> <li>Safety &amp; Security Congressionally Mandated Joint Vulnerability Assessments</li> <li>FAA LEAP Training / Videos</li> <li>FAMS Training Partnerships</li> <li>JTTF FBI Partnership</li> <li>ASP, AEP, NTSB, etc. mutual aid response training</li> </ul>	<ul style="list-style-type: none"> <li>Public safety partnership initiatives Federal, State, and Local transportation community members*</li> <li>UAS / Drone Public safety briefings at BWI Marshall Airport and at community meetings*</li> <li>Public safety campaigns, See-Say Something, brochures and visual displays*</li> <li>Social media / signage PSAs*</li> </ul> <p>* <b>Community-wide initiatives</b></p>

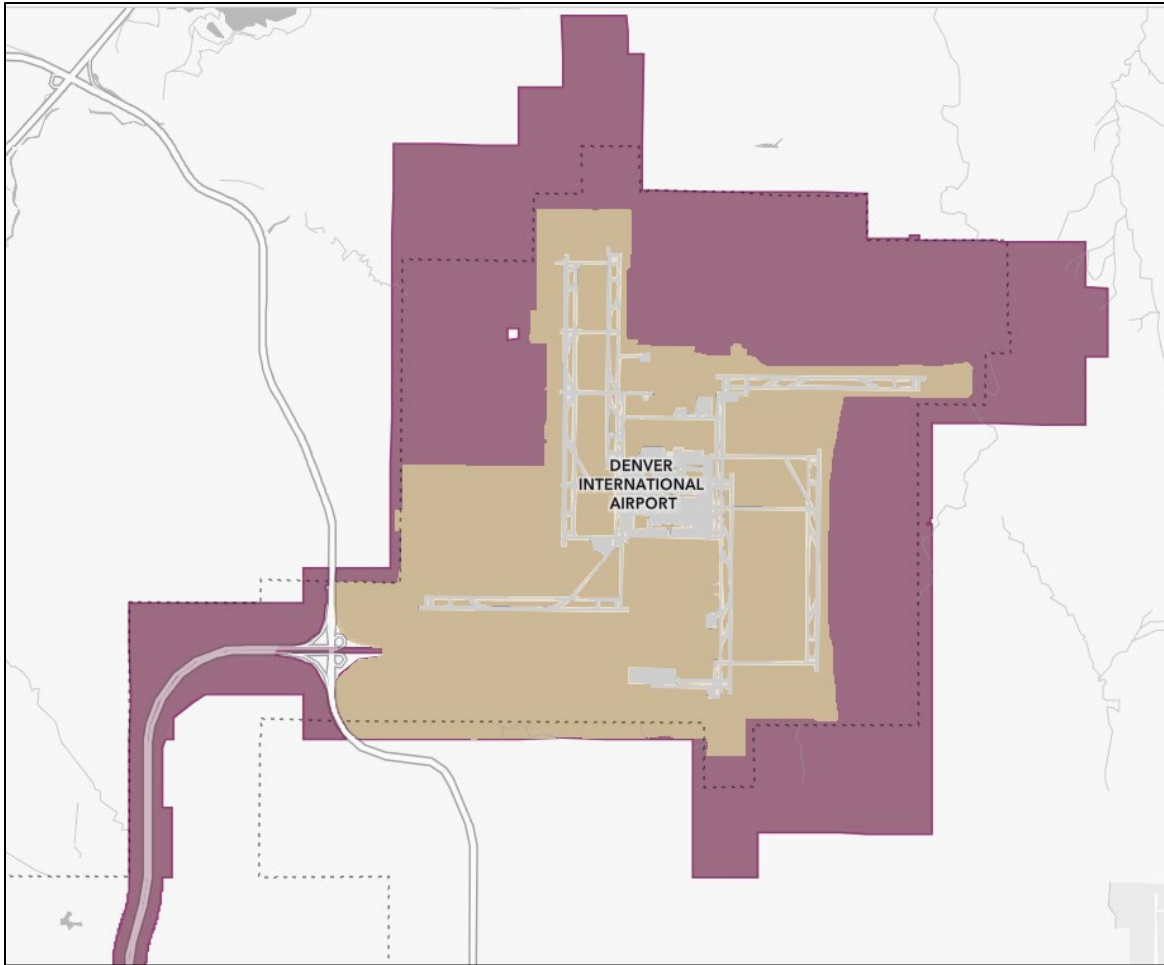
**Baltimore Washington International Airport Unsafe or Unauthorized UAS/Drone Response Management System**

## 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, 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 fall outside of the perimeter fencing that must meet specific federal 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 worse. Airports should look to better secure these areas from being utilized 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 a time a drone can cause an airport disruption. Increasing the amount of time it takes for a drone to reach airport property means that drone has less battery life to sustain any unwanted activity.



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



**Locked gate that still allowed pedestrian access**

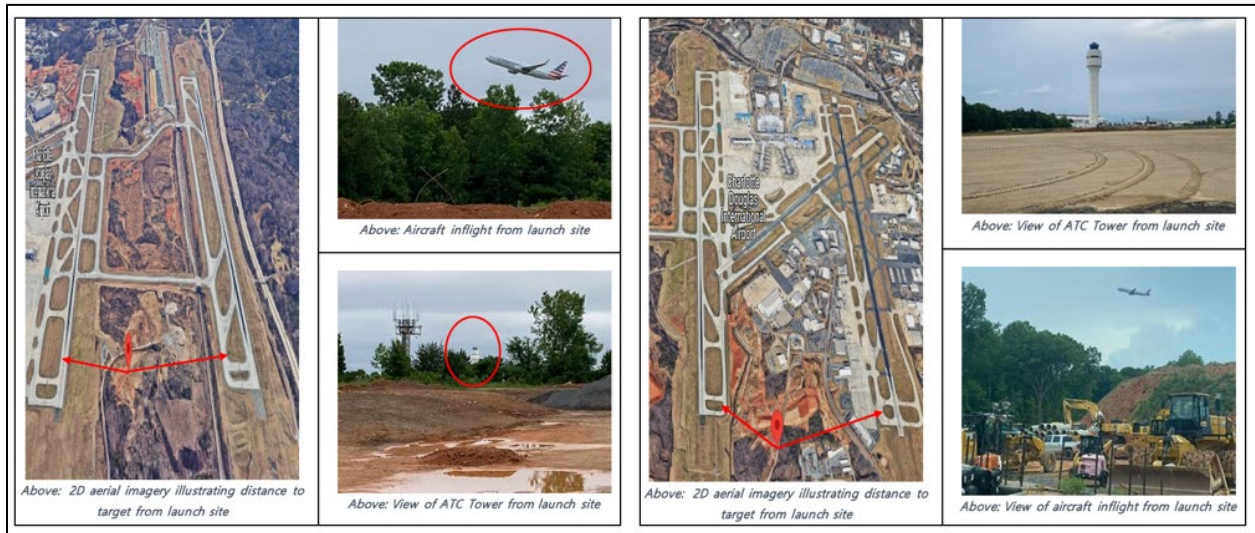
**Daisy-chain locking system in use at an airport-owned property gate**

**Examples of 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 contracts between a vendor and the airport should have language addressing the use of drones in their projects. Most construction companies use UAS and having a formal agreement between the airport and the vendor will establish a contractual obligation to ensure any contracted operator will abide by all current regulations and notify all parties that they are conducting 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 placing of anti-bird netting at observation areas or parking garages to prevent the launching of UAS from these locations.



**Examples of Construction Projects or Accessible Staging Areas at an Airport**



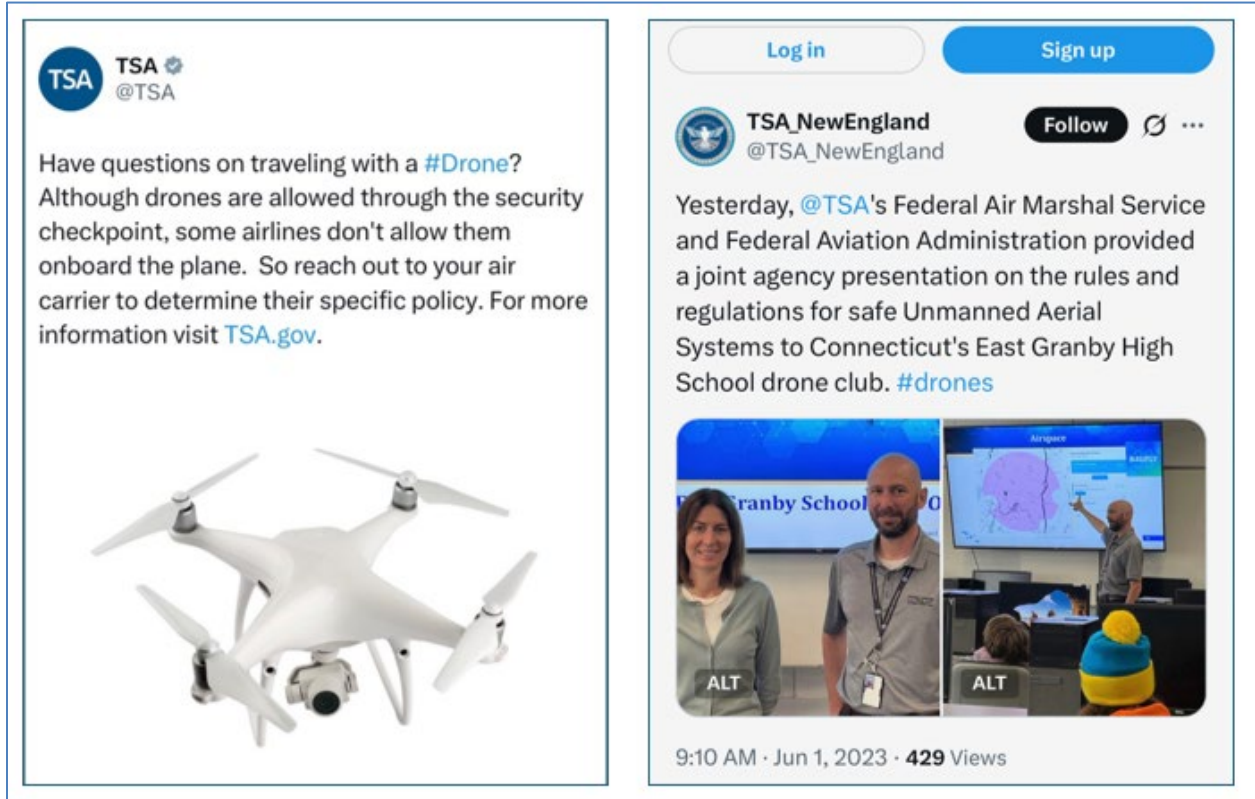
**Anti-Bird Netting Deployed at Public Parking Garages**

**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.



**Examples of Common No Drone Zone Signage**



**Examples of Social Media Outreach Efforts**



**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 multi-faceted drone awareness and reporting program. Many airport employees routinely interact with the flying public and are uniquely positioned to be authoritative 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 the domestic requirement to register any drone over 0.55 pounds with the FAA – 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.



**Instructions on How to Label Your Drone:** [FAADroneZone Access - Register](#)

#### 4. Training

Dedicated training efforts that provide various employee groups 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 on 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 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.



**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 EDD capability **IMMEDIATELY**. 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.

## Organizational Briefing Material Outlining How to Safely Response 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 professional must also be familiar with all federal laws and United States Code pertaining to drone operations, such as remote pilot requirements, aircraft registration laws, 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 like public parks.



**UNITED STATES OF AMERICA** XI  
DEPARTMENT OF TRANSPORTATION • FEDERAL AVIATION ADMINISTRATION

IV NAME  
XXXXXXXXXXXXXXXX

V ADDRESS  
XXXXXXXXXXXXXXXXXXXX  
XXXXXXXXXXXXXXXXXXXX

VI NATIONALITY USA  
VII D.O.B. XXXXXXXX

SEX HEIGHT WEIGHT HAIR EYES  
X XX XXX XXXXX XXXXX

IX HAS BEEN FOUND TO BE PROPERLY QUALIFIED TO EXERCISE THE PRIVILEGES OF

**REMOTE PILOT**

XI CERTIFICATE NUMBER XXXXXXXX  
XII DATE OF ISSUE XXXXXXXX

XIV *[Signature]*  
XV ADMINISTRATOR



**TRUST**

The Recreational UAS Safety Test (TRUST)  
Completion Certificate

Name:  
Thomas Cruise

Authentication Token:  
AAAAXXXXXXXXXXXX

Issued by:  
X on Month Day, Year

**Federal Aviation Administration Remote Pilot in Command Licensure Examples**

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.

**The Orange County Intelligence Assessment Center and The Los Angeles Field Office are co-hosting D.A.R.T**

**Drone Assessment and Response Tactics**

**Training Description**

The goal of the DART course is to help front-line first responders and emergency management personnel to recognize and assess an unmanned aircraft event for a potential threat, and to give basic awareness of how to assess and mitigate that threat. This course provides class participants with the knowledge and tools necessary to detect, identify, track, assess, mitigate, and respond to commercial and hobbyist unmanned aircraft operations in the United States. This course will provide first responders with mitigation and response techniques to use if they determine that an unmanned aircraft is operating in an unsafe or illegal fashion. The DART course also alerts the participants to the possible terrorist use of unmanned aircraft and enables them to understand the dangers represented by terrorist use of unmanned aircraft.

**Modules**

- 01: Introduction
- 02: Intro to UAS
- 03: UAS as a Threat
- 04: Regulations and Tactics
- 05: Case Study Overview
- 06: Detect & Identify UAS Activity
- 07: Track & Assess UAS Activity
- 08: Respond & Report UAS Activity
- 09: Conclusion

**Tuition Cost: FREE**

**DHS / FEMA Certified Training**

**New Mexico Tech Course Numbers: AWR-407**

**Thursday**  
**April 4, 2024**      0800-1600 hours

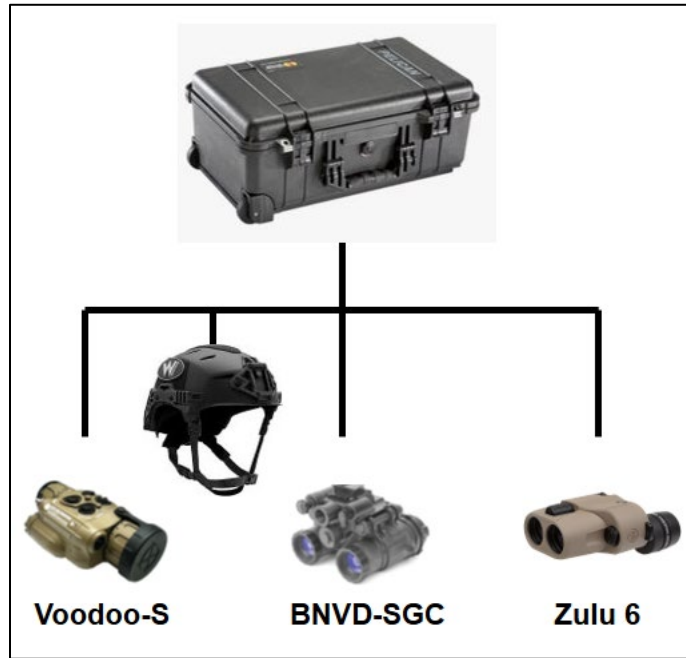
**Richard Nixon Presidential Library & Museum: Theater 37**

**NEW MEXICO TECH**  
 ENERGETIC MATERIALS RESEARCH & TESTING CENTER

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

Law enforcement personnel can also repurpose existing optical equipment like binoculars, night-vision goggles 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, observations 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.



**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-led C-UAS Task Force out of Los Angeles, California. The task force includes law enforcement participants from local, state, federal, and entities – to include FAMS, Federal Aviation Administration, 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.

**Conclusion:**

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, enhancements to physical security, targeted outreach and education, and comprehensive training – are essential building blocks for mitigating the risks posed by unauthorized drones. While technological solutions and legislative measures remain important, immediate, practical steps can be taken by airport stakeholders to address the threats within their operational environments. By adopting the recommended practices outlined in this publication, 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 reach out to the FAMS’ Counter Unmanned Aircraft Systems Unit at TSA Headquarters at [fams\\_cuas@tsa.dhs.gov](mailto:fams_cuas@tsa.dhs.gov)**