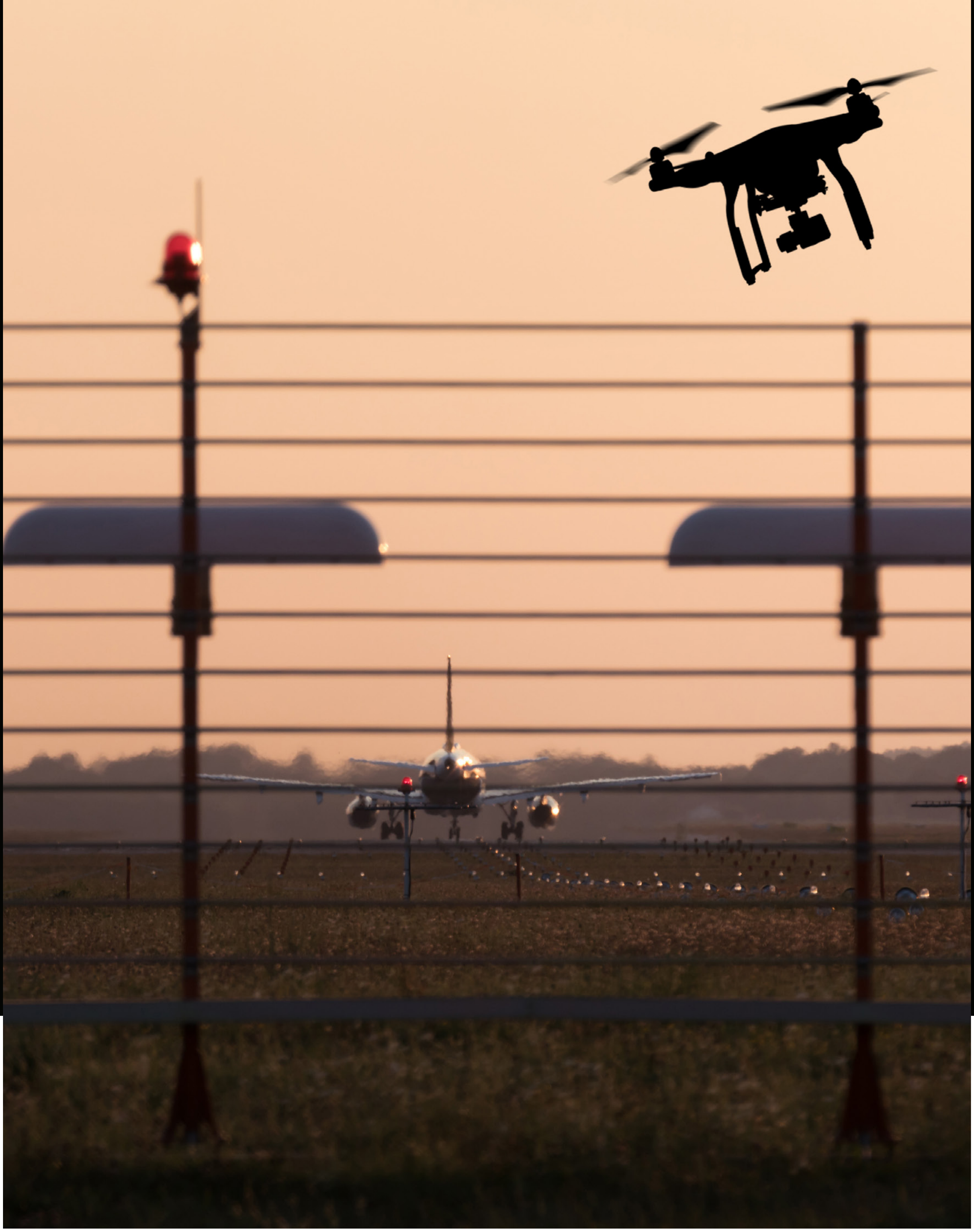
BLUE RIBBON TASK FORCE
ON UAS MITIGATION AT AIRPORTS

FINAL REPORT
OCTOBER 2019



BLUE RIBBON TASK FORCE
On UAS Mitigation at Airports

www.uasmitigationatairports.org

TABLE OF CONTENTS

INTRODUCTION

The Association for Unmanned Vehicle Systems International (AUVSI) and Airports Council International-North America (ACI-NA) commissioned the Blue Ribbon Task Force on UAS Mitigation at Airports (BRTF) in April 2019 to study the issue of Unmanned Aircraft Systems (UAS) integration, detection, identification, and mitigation in and around airports. The BRTF was charged with providing recommendations to airports and the U.S. and Canadian governments regarding UAS mitigation at airports–including but not limited to reviewing UAS and counter-UAS (C-UAS) technology, airport protocols for addressing UAS incursions, and the policy framework around UAS integration and mitigation in and around airports.

Through robust conversation across diverse stakeholders from the aviation community, the BRTF has been able to make significant progress in providing recommendations for the necessary policy framework to manage UAS mitigation at airports. Whether the origin of the incidence is carelessness, cluelessness, or maliciousness, the escalating frequency of drone-related incidents present a security, operational, and economic challenge to North American airports. The Final Report encapsulates the work conducted over past six months by BRTF to advance aviation and airport safety and security and builds off of the Interim Report that was released by the BRTF in July of 2019. The Interim Report included lessons learned from London Gatwick's December 2018 UAS incursion incident, a UAS detection and mitigation technology review, as well as over twenty recommendations to industry and government on steps that should be taken to safeguard airports from UAS incursions.

Commercial UAS applications continue to create new opportunities and add significant value to airport operations, but, unfortunately, also continue to represent a major challenge in and around the airport environment. Airports and their tenants benefit greatly from current UAS use in perimeter security, facility surveying and inspection, equipment inspection, and emergency response support. Equally significant are the concerns unauthorized UAS operations cause at or in the vicinity of airports. Unauthorized UAS have great potential to disrupt operations and the threat of intrusions introduces substantial risk highlighting the need for solutions that can safeguard airports from rogue UAS.

> **"**
> **THE FUNDAMENTAL ISSUE AT THE ROOT OF THESE CHALLENGES AND LACK OF SOLUTIONS IS THE CURRENT UAS REGULATORY AND LEGAL FRAMEWORK."**

The fundamental issue at the root of these challenges and lack of solutions is the current UAS regulatory and legal framework. Remote Identity (ID), a foundational regulation needed for technological solutions to work and the basis for other important rulemaking, is again delayed by the United States Federal Aviation Administration (FAA). This regulatory hurdle continues to block progress on opportunities for the safe and successful integration of UAS into the national airspace. Providing airports, law enforcement, and government with a critical tool that can identify and distinguish authorized UAS from those that may pose a safety or security threat greatly advances their ability to respond to and prevent potentially dangerous situations. The majority of incidents stem from the group of operators categorized as "careless or clueless." For every one of these operators who is identified, countless others cause disruptions or other incidents but remain unknown and without education or consequences. The importance of the ability to remotely identify and track these operators cannot be understated, as it would significantly reduce UAS incidents caused by the largest group of violators.

Distinct from the careless and clueless operators are the operators with potential criminal intent. Similar to the regulatory hurdles that limit stakeholder response to the careless and clueless, the legal framework also poses great challenges for authorities' response to criminal operators. Despite the clear proliferation of advanced technology and the increased risk that errant UAS present to airports and their surrounding communities, a regulatory and funding framework that empowers local authority to respond to threats by UAS is lacking. This creates a potential security gap and leaves the aviation community in the difficult position of balancing potential a security threat with the reality of limited funds and authority to effectively respond to that threat.

In the United States today, only four federal agencies have the authority to engage in counter-UAS actions, and this authority generally does not allow for persistent C-UAS coverage at airports. The situation is very similar in Canada. Broadening these agencies' scope of authority, however, would not alone address the unique issues at airports. The fast-paced operational nature of airports necessitates real-time responses that could only come from local authorities for successful outcomes in response to an unauthorized UAS. Extending authority to engage in UAS interdiction to trained local law enforcement tasked with safeguarding airports is the critical next step for government, one that can be accomplished while protecting civil liberties and statutory limitations.

Reports of arrests and other enforcement actions continue to make headlines—showing progress being made and underscoring the need to reduce barriers for future responses. This report seeks to address these threats with recommendations to policymakers and industry on ways to aggressively move forward to safeguard airports from the threat of UAS while simultaneously ensuring that safe integration of UAS operations into airports can proceed. Included in the report are recommendations on roles and responsibilities in UAS detection, authorities for countering UAS that pose a threat in an airport environment, and guiding principles for airports seeking to draft a UAS incursion response playbook. The report also contains feedback on the United States Transportation Security Administration's (TSA) draft Tactical Response Plan (TRP) for UAS incursions at airports.

Combined with the interim report from July, this report represents a set of recommendations that, if implemented, would help to ensure UAS safety and security moves forward in a timely and risk-based fashion to ensure the industry can continue to grow with compliant operations and airports remain safeguarded from careless, clueless, or criminal UAS operators. Recognizing the complexity and urgency of this new frontier for all stakeholders involved, the BRTF recommends a framework of shared responsibility with clear roles and responsibilities as the aviation community takes on this evolving challenge.

The Final Report provides recommendations and insights consistent with the objectives of the mission of the BRTF:

✓ Identify roles of key airport stakeholders in UAS spotting and reporting, including guidelines for reporting process.

✓ Provide recommendations to the federal agencies and Congress as they study the issue of delegation of authority in engaging C-UAS.

✓ Provide recommendations for additional law and policy to empower state and local authorities to respond to offenders.

✓ Make recommendations to airports on best practices for preparing and responding to authorized and unauthorized UAS missions on or in the airport vicinity.

✓ Explore the issue of safe operational integration of UAS in airspace under 400 feet.

✓ Looking forward, address evolving mission capability of UAS, including EVTOL package delivery.

"

RECOGNIZING THE COMPLEXITY AND URGENCY OF THIS NEW FRONTIER FOR ALL STAKEHOLDERS INVOLVED, THE BRTF RECOMMENDS A FRAMEWORK OF SHARED RESPONSIBILITY WITH CLEAR ROLES AND RESPONSIBILITIES AS THE AVIATION COMMUNITY TAKES ON THIS EVOLVING CHALLENGE."

TASK FORCE MEMBERS

MICHAEL HUERTA

CO-CHAIR
FORMER ADMINISTRATOR OF THE FEDERAL AVIATION ADMINISTRATION

Michael Huerta is the former Administrator of the Federal Aviation Administration of the United States of America. Huerta was sworn into office on January 7, 2013, for a five-year term. Huerta was responsible for the safety and efficiency of the largest aerospace system in the world and oversaw a $15.9 billion budget and more than 47,000 employees.

DEBORAH FLINT

CO-CHAIR
CHIEF EXECUTIVE OFFICER, LOS ANGELES WORLD AIRPORTS

Deborah Flint was appointed Chief Executive Officer of Los Angeles World Airports (LAWA) in June 2015, with oversight of Los Angeles International (LAX) and Van Nuys (VNY) airports. LAX is currently the fourth busiest airport in the world. Flint leads the team responsible for creating a world class airport that is a modern reflection of today's global society.

JOHN PISTOLE

FORMER ADMINISTRATOR, TSA & FORMER DEPUTY DIRECTOR, FBI

John S. Pistole is the former administrator of the United States Transportation Security Administration (TSA) and a former deputy director of the Federal Bureau of Investigation.

TRISH GILBERT

EXECUTIVE VICE PRESIDENT, NATIONAL AIR TRAFFIC CONTROLLERS ASSOCIATION

Trish Gilbert has served as the National Air Traffic Controllers Association's seventh executive vice president since she was first elected in September 2009.

RICH DAVIS

FORMER MANAGING DIRECTOR OF GLOBAL SECURITY, UNITED AIRLINES

Rich Davis spent 23 years in the Corporate Security department at United Airlines, where he directed the broad range of aviation security issues surrounding the airline and the airports through which United operates.

MARK LAROCHE

PRESIDENT AND CHIEF EXECUTIVE OFFICER, OTTAWA INTERNATIONAL AIRPORT AUTHORITY

Mark Laroche has been the President and Chief Executive Officer of the Ottawa Macdonald-Cartier International Airport Authority since March 1, 2013. Prior to this, he worked as the President and Chief Executive Officer of Canada Lands Company Limited.

HUNTLEY LAWRENCE

DIRECTOR OF AVIATION, PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Huntley Lawrence is responsible for managing one of the world's largest airport systems, comprised of John F. Kennedy International (JFK), Newark Liberty International (EWR), LaGuardia (LGA), Teterboro (TEB) and New York Stewart International (SWF) airports.

CATHY LANIER

SENIOR VICE PRESIDENT OF SECURITY, NATIONAL FOOTBALL LEAGUE

Cathy Lynn Lanier was the chief of the Metropolitan Police Department of the District of Columbia (MPDC). In 2016, Lanier was named Senior Vice President of Security for the National Football League.

SCOTT BROCKMAN

PRESIDENT AND CEO, MEMPHIS-SHELBY COUNTY AIRPORT AUTHORITY

Scott Brockman joined the Memphis-Shelby County Airport Authority in June 2003. He was appointed President and CEO on January 2, 2014 after having served as Executive Vice President and Chief Operating Officer.

CHAD MAKOVSKY

EXECUTIVE VICE PRESIDENT, OPERATIONS DIVISION AT DALLAS/FORT WORTH INTERNATIONAL AIRPORT

Chad Makovsky serves as the Executive Vice President for the Operations Division at Dallas/Fort Worth International Airport where he leads DFW Airport's Department of Public Safety, Environmental Affairs, and Operations functions.

MARILY MORA

PRESIDENT/CEO RENO-TAHOE AIRPORT AUTHORITY

Marily Mora is responsible for leading and directing the Reno-Tahoe International Airport (RNO), and the Reno-Stead Airport (RTS), with an operating budget of $46 million.

NEIL WILSON

PRESIDENT AND CEO, NAV CANADA

Neil R. Wilson is President and CEO of NAV CANADA, as of January 1, 2016. He served as Executive Vice President, Administration and General Counsel for the Company from 2013-2016, responsible for all Legal and Corporate Services.

JAMIE RHEE

CHICAGO DEPARTMENT OF AVIATION (CDA) COMMISSIONER

Jamie Rhee is the Chicago Department of Aviation (CDA) Commissioner where she manages one of the world's busiest airport systems, comprised of O'Hare and Midway International Airports, which serves more than 100 million passengers each year.

UAS DETECTION: A SHARED RESPONSIBILITY

In the interim report, the BRTF noted that it would continue to explore the issue of availability of federal funding to help industry test, acquire, deploy, staff, and maintain detection, tracking, and identification (DTI) technology. The BRTF also pledged to examine how the role of federal governments might evolve in UAS traffic management (UTM) to address the growing mission capability of UAS, including the integration of electric vertical takeoff and landing (eVTOL) package delivery services and ride sharing.

The premise behind these questions is rooted in the position of the FAA and other U.S. federal agencies that the government does not have the authority, capital, or human resources to invest in and operate UAS detection systems on and near airports. The situation is very much the same in Canada. This has led some airports to take on UAS detection in order to fill the void left by the lack of current involvement by federal governments. **The BRTF takes the position that airports should not be burdened with undertaking this operation alone.** Instead, as with many other operations at airports, such as airport security, **UAS detection should be a shared responsibility between airports and federal governments.** Further, many airports simply have no ability to engage in the monitoring of UAS activity—the process for deploying UAS DTI technology is complicated and expensive and beyond the scope of many airports' resources and capacity. **Without a robust federal role, an unacceptable security gap will continue to exist at many airports across the U.S. and Canada.**

As the popularity and utility of UAS continue to expand, and new technologies come online, including eVTOLs, airports are not authorized to and cannot reasonably be expected to engage in UAS air traffic management. The position of the U.S. federal government is that UAS "must be authorized in the airspace because FAA air traffic control is responsible for managing the safety and efficiency of controlled airspace." In Canada, air traffic services are funded directly by existing aviation customers. UAS operators are not currently paying fees but would be the primary beneficiary of future UAS services. **The federal governments of both the U.S. and Canada are then responsible for engaging in safety measures to monitor UAS traffic.** This includes the detection and identification of compliant and non-compliant UAS, and the actions required for both types of operations to ensure safety and security in and around airports.

The BRTF recommends that Congressional action must be taken to give the FAA the appropriate resources on a consistent basis to engage in the lead role of monitoring UAS traffic in and around airports. The urgency for congressional action is underscored by the fact that the FAA is understaffed, underfunded, and subject to government shutdown. We are not suggesting or recommending that air traffic controllers solely take on the responsibility for detection and identification of compliant and non-compliant UAS. Multiple offices within the FAA need be a part of the solution, including the Air Traffic Organization (ATO), Law Enforcement Assistance Program (LEAP), UAS Integration Office, in addition to sharing responsibility with airport operators. For UAS detection at airports to be successful, however, Congress must additionally authorize and appropriate the necessary funds for the FAA to ensure adequate testing, acquisition, deployment, staffing, and maintenance of DTI technology in the airport environment. Other federal agencies, including the TSA, Federal Communications Commission (FCC), Department of Justice (DOJ), and Department of Defense (DOD), also have roles in monitoring compliant and non-compliant UAS in and around airports, and must also be appropriately funded and encouraged to work with airport operators and the FAA in this shared safety and security responsibility.

In the interim, however, the BRTF suggests a conditional approach for airports seeking to test, acquire, deploy, staff, and maintain DTI technology themselves, as some are already integrating this technology. Some airport operators are moving forward with the deployment of UAS detection technology in the absence of federal action; **therefore, there is an urgent need for the FAA and Transport Canada to establish UAS detection system standards.** Having standards in place is important both as a verification of the technology and as a prerequisite for Airport Improvement Program (AIP) eligibility for UAS detection and mitigation systems as authorized in the FAA Reauthorization Act of 2018. The BRTF recommends that the FAA work to standardize approaches to UAS detection technology integration at airports with further testing, work toward uniform standards, and provide more straightforward guidance to airports seeking to deploy DTI technology. In Canada, TC has not provided any guidance to airports on this matter as of June 2019 but must do so as soon as practicable.

The BRTF recommends Congress in the U.S. and Cabinet in Canada also consider new funding sources for airports to test, acquire, deploy, staff, and maintain DTI technology. The AIP grant program in the U.S. and the Airports Capital Assistance Program (ACAP) in Canada are already underfunded to support the infrastructure needs of airports today. Given the many competing priorities for use of AIP and ACAP funds, it would be prudent to develop additional dedicated funding sources so that airports and the FAA and Transport Canada do not have to choose between equally critical projects and expose themselves to undo liability.

"THE BRTF RECOMMENDS THAT CONGRESSIONAL ACTION MUST BE TAKEN TO GIVE THE FAA THE APPROPRIATE RESOURCES ON A CONSISTENT BASIS TO ENGAGE IN THE LEAD ROLE OF MONITORING UAS TRAFFIC IN AND AROUND AIRPORTS."

UAS MITIGATION: A ROLE FOR STATE AND LOCAL LAW ENFORCEMENT

As part of the FAA Reauthorization Act of 2018, Congress directed the Executive Branch to report back with recommendations to Congress on future delegation of C-UAS authority beyond the limited authority granted to the four federal agencies currently with C-UAS authority. The BRTF believes the following information can serve as a valuable resource for Congress and the federal agencies studying this issue.

DHS and DOJ have expertly and successfully demonstrated C-UAS capabilities on a temporary basis during large-scale events with lead time and extensive planning. However, federal authorities alone simply do not have the resources or manpower to accomplish this mission on a daily basis at airports across the country. Furthermore, the authority granted to the four federal agencies is narrowly tailored to specific events and facilities; the daily operations at airports remain outside the scope of that authority. The U.S. and Canadian federal governments recognize state, provincial, and local law enforcement as first responders to unauthorized UAS events. In fact, federal authorities will not deploy resources to an airport until local law enforcement resources are exhausted. The FAA notes, “When the full weight of local resources are unable to resolve a credible risk from errant or malicious UAS operations, assistance from federal authorities and supporting resources may be available upon request.” Local law enforcement, however, lacks both the authority and the resources to mitigate UAS in real time, effectively ensuring the response will fall short and require federal action that will unlikely be timely enough to actually mitigate the threat. This presents a major security gap and a vulnerability to our respective national securities that must be addressed.

During the June 2019 U.S. Senate hearing on drone security, Senator Edward Markey remarked that first responders are “caught in no-man’s-land” for protecting against urgent UAS threats and

highlighted the imbalance between responsibility and authority, noting, “we need a balance that is struck here, and right now, I don’t think we have a full balance.” Senator Markey further acknowledged this imbalance by indicating it is time for Congress “to think about modifying that authority so that we deal with this tsunami of threats which are going to be out there and allow for there to be additional protections which are provided to the public.”

The increase in UAS sightings at airports, airspace disruptions, and threats of UAS use by activist groups drive demand for change in how responsible authorities respond. It is no longer acceptable for a lack of legal framework, understanding of technology, or authority to be the reasons airports remain at risk of a serious UAS event. It is time consideration be given to balancing response capabilities with continually evolving UAS threats.

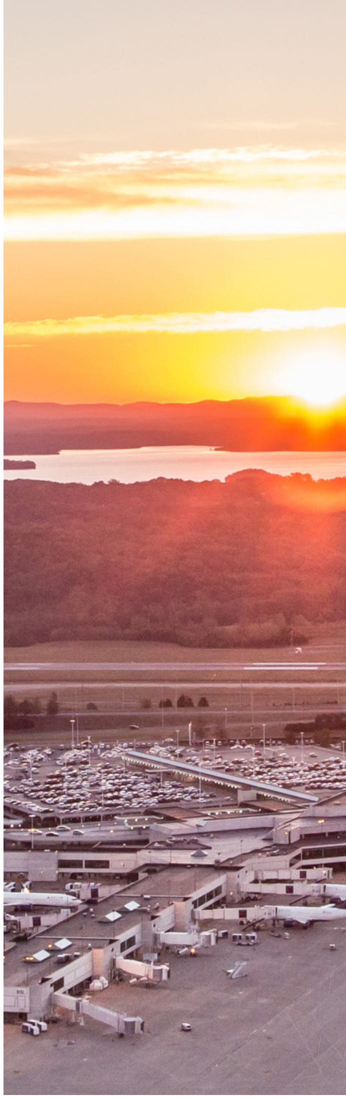
The BRTF agrees with the FAA that public safety agencies, such as local and state law enforcement agencies, including airport police authorities, are in the best position to deter and investigate unauthorized or unsafe UAS operations and “while drones can serve as a useful tool, these agencies also have an important role in protecting the public from unsafe and unauthorized drone operations.” **The BRTF recommends Congress in the U.S. and the**

Cabinet in Canada extend authority to engage in UAS interdiction—kinetic or electronic—to trained state and local law enforcement in the U.S. and the Royal Canadian Mounted Police (RCMP), provincial, and local law enforcement in Canada tasked with safeguarding airports and the immediate surrounding areas. Interdiction should always be a last resort—to date, most UAS incursions have been halted when the UAS operator is identified and told to land the errant UAS. Nevertheless, local and state law enforcement working in and around airports, including flight pathways, need to have the ability to use interdiction technologies should the risk circumstances absolutely require that course of action.

The BRTF suggests that the deputation of C-UAS authority to state and local law enforcement should begin with a pilot program overseen by DOJ, in consultation with DHS, in the U.S. and DOJ and Public Safety in Canada (PSC), to establish protocols, training, and practice exercises. This pilot program would require authorization from Congress, which the BRTF suggests is an action that Congress should undertake straightaway. The pilot program would bring airports, federal agencies, state, provincial, and local law enforcement together with private sector entities that manufacture UAS, detection systems, and mitigation technology. The pilot program should be open to no less than six participating airports in order to gather information on different operating conditions, organizational models, and local law enforcement relationships.

The program would help governments create a second narrowly tailored grant of authority to state, provincial, and local law enforcement and provide critical information to the FAA and Transport Canada as they develop standards and issue rules. The program would be an instrumental case study in balancing roles and responsibilities, strengthening the partnerships between federal agencies and state, provincial, and local authorities, and accelerating the development of standards necessary for actionable next steps.

The BRTF recommends that training programs include not only the safe and effective use of various C-UAS technologies, but also the balance between privacy and safety. **The BRTF acknowledges the absolute importance of safeguarding personal information and the right to privacy.** The BRTF believes defending critical infrastructure and ensuring civilian safety is of paramount importance and can be done in a way that protects civil liberties. **Enforcement officers deputized with C-UAS responsibilities at and near airports should, therefore, have the same legal protections on privacy and liability issues afforded to federal agencies.**



"

**IT IS NO LO
A LACK OF
UNDERSTA
OR AUTHO
AIRPORTS
SERIOUS U**

ONGER ACCEPTABLE FOR
F LEGAL FRAMEWORK,
ANDING OF TECHNOLOGY,
ORITY TO BE THE REASONS
REMAIN AT RISK OF A
JAS EVENT."

TSA'S DRAFT TACTICAL RESPONSE PLAN **THE BRTF'S FEEDBACK**

U.S. and Canadian airport operators do a commendable job of keeping airports safe and secure for the traveling public. Assessing risks and mitigating threats in the airport environment are responsibilities of airport operators and are successfully and seamlessly accomplished on a daily basis. Those roles and responsibilities are well established in statutory and regulatory authorities, providing operators and federal agencies clear direction to carry out the joint responsibility of keeping airports safe and secure.

Yet, when it comes to the threat of unauthorized UAS in the airport environment, the fundamental problem remains at issue—currently defined federal roles are unclear, as are state and local law enforcement roles, and airport operators are statutorily and regulatorily constrained to mitigate unauthorized UAS. Since the publication of the BRTF's interim report in July 2019, the United States Transportation Security Administration (TSA) released a draft Tactical Response Plan (TRP) that provides a framework for a local response to an errant or malicious UAS at the airport. The TRP shows the progress of federal agencies beginning to define and clarify roles and responsibilities; unfortunately, however, the TRP exacerbates the fundamental problem of assigning responsibilities to airport operators that they have no authority (and insufficient resources) to carry out.

01

THE BRTF RECOMMENDS THE TRP BE MODIFIED TO REFRAME THE CURRENT ROLES AND RESPONSIBILITIES OF AIRPORTS AND FAA.

The FAA is responsible for airspace management and must have a clearly defined active role in UAS response plans. Detection of aircraft in airspace in and around the airport environment is a part of airspace management. The BRTF understands the TRP is an internal TSA SOP and recommends that it accurately reflect current roles and responsibilities for response plan development. The BRTF recommends modifying the TRP to appropriately reflect the airport as having a supporting and collaborative role in relation to the FAA and other federally authorized agencies, rather than the lead role.

02

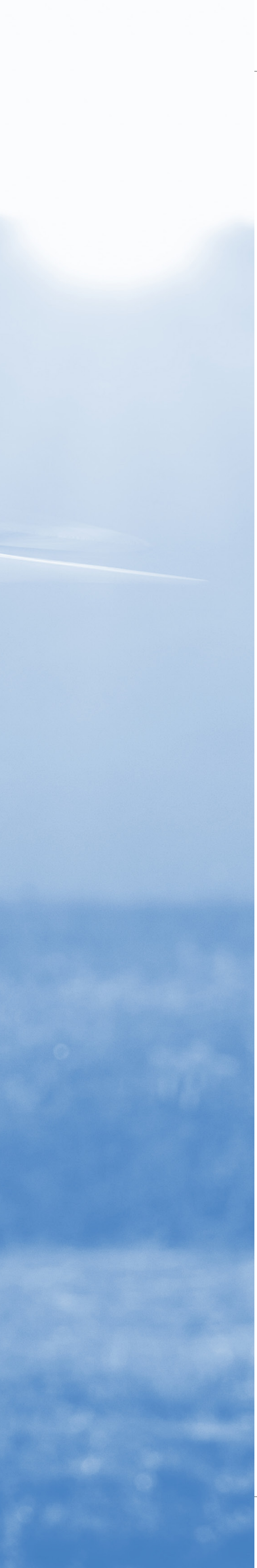
THE BTRF RECOMMENDS THE TRP BE MODIFIED TO EXCLUDE REFERENCE TO THE AIRPORT'S AIRPORT SECURITY PROGRAM (ASP) TO ADDRESS UAS THREATS UNTIL SUCH TIME THAT ROLES AND RESPONSIBILITIES ARE CLEARLY DEFINED AND CODIFIED.

Airports are required by regulation to establish air transportation security programs that provide law enforcement presence and capability that is adequate to ensure passenger safety. It is premature for TSA to assign airports the responsibility of ensuring their existing law enforcement is adequate to address UAS threats under these federal programs before roles and responsibilities are defined. Airports do not yet have the authority to carry out this responsibility and therefore the airport's security role should not be a requirement under their federally mandated ASP. Once roles and responsibilities are defined, the ASP could be an appropriate vehicle for requirements under a shared responsibility model.

03

THE BRTF RECOMMENDS FEDERAL AGENCIES PUBLISH A DOCUMENT CLEARLY DEFINING THE ROLES, RESPONSIBILITIES, AND AUTHORITIES OF LOCAL LAW ENFORCEMENT AGENCIES.

The BRTF acknowledges the FAA, DOJ, and TSA have provided some guidance; however, the information does not provide clear direction to law enforcement agencies to state with certainty what their role is within current legal, statutory, and regulatory limitations.



GUIDING PRINCIPLES FOR UAS INCURSION RESPONSE PLANNING AT AIRPORTS

As the BRTF noted in the interim report, industry, local law enforcement, and federal agencies should partner in developing airport community communications plans that would alert all stakeholders–including but not limited to air navigation service providers (i.e., the FAA Air Traffic Organization in the United States and NAV CANADA in Canada), airport and airfield operations, airport and local police departments, and airline control centers (to also notify pilots and ground crew)–to authorized UAS in the vicinity. This would help limit concerns about UAS operations in the airport environment and drive appropriate levels of response.

As part of the release of the BRTF Final Report, the BRTF has included a standalone attachment that provides a practical template for airports to develop a UAS Response Plan, which integrates the guiding principles provided below.

Below are a set of considerations airports should evaluate when deciding how to respond and are developing their own individual UAS response plans:

01

SCOPE

Scope considerations could include:

What types of unauthorized UAS events could occur at or near airport? Some examples are:

- Confirmed and active UAS
- Confirmed but no longer active UAS
- Unconfirmed UAS
- On airport property and inside a certain number of miles from airport perimeter fence
- Outside of specified number of miles from airport
- Activity that causes airport disruption
- Activity that causes airport closure and reopen

How are those events defined?

Any local details that make unique events likely at a particular airport?

For airports with authorized UAS operations, should response to unauthorized UAS be a part of standard operating procedure (SOP) for authorized operations or a separate plan?

02

COLLABORATIVE DEVELOPMENT

The TSA TRP indicates that the UAS Response Development Team (UASRDT) should:

Be led by the Federal Security Director (FSD) and Federal Air Marshal Service (FAMS) Supervisory Air Marshal in Charge (SAC)

Involve the Assistant Federal Security Directors for Law Enforcement (AFSD-LE), compliance, transportation security specialists-explosives (TSS-E), the airport coordination center, Federal Bureau of Investigation (FBI), local law enforcement, and, as applicable:

- TSA
- FAA
- Customs and Border Protection (CBP)
- Homeland Security Investigations
- State Fusion Center
- National Guard/Air National Guard
- City Police
- Township Police
- County Sheriff's Department
- Federal law enforcement agencies that serve a local jurisdiction, e.g., U.S. Park Police, Bureau of Land Management, etc.

Consideration should be given to identifying other stakeholders who should be involved in the planning and development. Other examples could be:

- Airport Operations
- Planning and Environment
- Airport Police Department
- FAA's Law Enforcement Assistance Program (LEAP) Agents
- Public Safety and Security Technology
- Legal Department
- Corporate Communications
- Airport/community public affairs
- Airlines

Don't assume federal agency personnel understand their roles and responsibilities even if written documentation and guidance is provided. Proactively provide clarity on roles and responsibilities for all levels of government since this regulatory area is constantly evolving

03

REVIEW REQUIREMENTS

Before any response plan or action is defined:

The development team should refer to all statutory, legal, and regulatory requirements, including:

- National policies
- FAA and Transport Canada regulations/guidance
- State /Provincial and local statutes/regulations
- Airport plans
- Concept of operations (Core 30 Airports)
- TSA tactical response plan (TRP)

This is particularly true for airports seeking to evaluate or deploy detection systems—as the FAA has indicated it cannot determine the legality of any detection systems and directed airports to consult legal counsel and/or the appropriate authorities

Current laws prohibiting non-federal counter-UAS operations to protect airports should also be reviewed

04

DEFINITIONS

Considerations for defining terms:

- Due to multi-stakeholder involvement in responding to a UAS incident, common terminology must be used
- Don't assume stakeholders define commonly used terms the same way
- Definitions and criteria must be clear, concise, and easily understood by all to avoid interpretation differences and support rapid response
- Refer to regulatory definitions when available/applicable
- Definitions could include, but are not limited to:
  - Locations
  - Facilities
  - Responsible individuals
  - Operations
  - Equipment
  - Disruption
  - Detection
  - Mitigation
  - Confirmed
  - Unconfirmed
  - Disruption to operations
  - Indication of intentional harm
  - Threat
  - Perceived threat

05

RESPONSIBILITIES

Considerations for determining and defining responsibilities:

The development team should consider the primary responsibility for each entity and each individual with mission responsibility. Key responsibilities to consider include:

- **Transportation Security Administration (TSA):** The Lead Federal Agency (LFA) for C-UAS response at an airport.
- **Federal Aviation Administration (FAA):** Responsible for control and routing of air traffic and determining whether a UAS is operating lawfully (for example, operating with a waiver), or unlawfully. Air Traffic Controllers are not required to provide ATC services, including separation, to unmanned aircraft; however, ATC generally provides advisory information from any pilot-reported or tower-observed activity, providing information on the UAS activity, position, distance, course, type of UAS, and altitude.
- **Federal Bureau of Investigation (FBI):** Responsible for the investigation of terrorist acts or violent crimes against aircraft.
- **Local Authority:** While state and local entities do not have authority to use counter-UAS technology to mitigate UAS, law enforcement responsibilities may include:
  (1) detecting UAS;
  (2) reporting incidents to Federal entities (for example, the FAA Regional Operations Center);
  (3) observing the UAS in flight;
  (4) identifying the type of device (e.g., fixed wing or multi-rotor) and the UAS size, shape, color, and payload;
  (5) locating the operator; and
  (6) executing appropriate police action to include, among others, obtaining evidence, identifying witnesses, and conducting initial interviews.
- Define the action for each responsible party upon a triggering event for each threat level
- Determine the playbook for operational disruptions such as option to land, temporary delay, closure, etc.
- Consider table-top exercises for multi-stakeholder planning in the event operational disruptions such as altered flight path, temporary delay, closure, etc

06

LIMITATIONS

Considerations for limitations:

- Document limitations on the airport's and individuals' authority to mitigate UAS even when the UAS creates a hazard to airport operations
- Document limitations on law enforcement's authority
- Include a statement that airport employees will defer to federal agencies' defined actions when mitigating risk of unauthorized UAS and their operators
- Review and check against any local policies regarding UAS and enforcement

07

DEFINE THREAT LEVELS

Considerations for defining threat levels:

Determining the appropriate number of threat levels. Generally, threat levels can be categorized by response type:

- Reporting and documentation
- Local enforcement
- National response

Additional considerations may include:

- Size of the UAS
- Number of UAS (one vs multiple vs swarm)
- Distance/proximity from airport/approach path, which usually should be limited to within 5 miles of airport property.

Identify the threat level at which there is likely disruption to airport operations and develop a response that considers the role of the TSA as the lead federal agency.

08

PROCEDURES

Procedural considerations include:

- Regardless of origin (pilots, airport employees, etc.), should all reports of unauthorized UAS activity should be routed through one entity for dissemination?
- How are procedures different if airport is equipped with detection technology?
- Should there be one or multiple notification paths, e.g., email, phone, etc.?
- How to determine notification tree—should notification be tiered based on threat level?
- What is the playbook for operational disruptions such as option to land, temporary delay, closure, reopen, etc.?
- Can external communications be helpful in real time or should they be avoided until event is over?
- Responses should be scaled to each defined threat level, how to pivot when threat level changes from one to another?
- Who are the individuals with decision-making authority?
- Create predetermined hotline/conference bridge phone numbers and access codes
- Create dedicated email address
- What is the best process to collect and share data, best practices, and lessons learned?

09

ACCIDENT/INCIDENT REPORTING

The FAA, National Transportation Safety Board (NTSB), and TSA may have regulatory reporting requirements that must be followed in the event of certain accidents and incidents involving UAS. It is advisable that airport operators are familiar with the essential elements of information (in accordance with the Tactical Response Plan) that federal agencies are responsible for documenting after an incident. These can be found in the UAS Response Plan Attachment.

APPENDIX A

UNMANNED AERIAL SYSTEM (UAS) RESPONSE PLAN TEMPLATE

Background

The potential safety hazards and security threats presented by errant or malicious UAS activity in the National Airspace System (NAS) and the evolving tactics used by hostile actors are provoking a growing number of efforts by public and private sector entities to address these risks. The potential for UAS activity to interfere with or halt operations at an airport is a known threat, demonstrated by recent disruptions to operations at Gatwick Airport in the United Kingdom (December 2018) and Newark Liberty International Airport (January 2019). TSA is working with federal agency partners, local airport operators, law enforcement officials, and industry to prepare, prevent, and respond to UAS threats to aviation security and airport operations. Additionally, airports are encouraged to develop local response plans to ensure a proper response to address unauthorized UAS operating on or near the airport.

Scope

Standard operating procedures for responding to unauthorized UAS activity at or near the airport. Considers protocol according to threat level presented by observed UAS:

Low

Report of UAS operating near the airport with no disruption to operations. Low impact UAS events could be categorized as those where UAS have been observed and reported but are no longer active; pose a nominal hazard to the airport; present no indication of intentional harm; and are unlikely to cause disruption to airport operations.

Examples:

- Confirmed but not longer active UAS. A drone was identified near airport property, usually through visual observation, but the drone is no longer active.
- Confirmed and active UAS. A drone has been identified near airport property, is still active, but poses no threats or potential safety issues to airport operations.
- Report of UAS operating without authorization on airport adjacent property (up to five miles), but not exhibiting threatening behavior.

***Response Type:** Monitoring, reporting, and documenting.*

Medium
Report of unauthorized UAS operating on or near airport, with the potential to cause disruption to operations, for example by operating in an area that presents a significant safety concern, such as in the path of aircraft taking off or landing. Medium impact UAS events could be categorized as those that occur in visible proximity of the airport that pose a moderate safety risk to airport operations, present no indication of intentional harm, but has potential to disrupt operations due to proximity to airport property, type of UAS operation, or direction of the UAS flight path.

Examples:

- Observation of a UAS in an area of potential safety concern, at the perimeter fence, or is persistent beyond the 20-30 minute battery life of the average UAS.
- Observation of one or multiple UAS above the airport perimeter or in the immediate vicinity.
- Off airport property, especially when UAS is conflicting with arriving or departing aircraft.
- Multiple UAS operating on or near the airport and are exhibiting persistent hovering behaviors.

***Response Type:** Reporting, documenting, and actively dispatch resources to track the UAS and locate the operator. Determine need to escalate threat level.*

High
Persistent unauthorized UAS operating on or near airport, with the intention to cause disruption to operations or intentional harm. High impact UAS events could be categorized as those that occur within the airport's airside environment, pose a substantial safety risk to airport operations, and present indication of intentional harm or intentional disruptions to airport operations.

Examples:

- Explicitly threatening behavior, such as hovering above a runway for a prolonged period.
- Knowledge of a weaponized drone on or in the immediate vicinity of airport property.
- A swarm of drones is observed operating on or near the airport.
- Attack by a drone on the airport or adjacent community.

***Response Type:** Reporting, documenting, and actively dispatch resources to track the UAS and locate the operator. Depending on the severity of event, request federal response. Recovery activities may follow.*

Definitions and Acronyms

- Unmanned Aircraft (UA): Any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board.
- Unmanned Aircraft Systems (UAS): An unmanned aircraft and the equipment required to control it remotely.
- Counter Unmanned Aircraft Systems (C-UAS): A system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system.
- UAS Sightings: First hand report of a drone that is within visual line of sight
- UAS Reports: First-hand observations of UAS that are reported to airport operations, or a notification that comes to airport operations through Air Traffic Control (e.g., a report that came to ATC from a pilot, etc.)
- Disruption: The negative impact of a UAS Of Interest (UOI) on an airport, resulting in the degradation of air traffic operations or other security, safety or efficiency impacts on the NAS. The negative impact may include any consequence of a response action.

- Mitigation: The action of reducing the severity of a UAS threat through enforcement or technology.
- UAS Detection, Identification, and Interdiction Technology (DTI): UAS detection involves the observation of UAS operations through technical means such as electro-optical/infra-red (EOIR), acoustic, radar, RF receivers, and/or networked surveillance using shared positional and identification data; identification involves the authentication of UAS operation based on the totality of the circumstances, including a highly reliable primary observation or some form of two-factor confirmation such as a UAS detection system backed by a first-hand visual sighting; interdiction involves radio-link jamming, GPS jamming, taking control of the drone (spoofing), lasers, electromagnetic pulses, and kinetic projectiles.
- Local Communities of Interest (COI): Those agencies based in, operating at, and/or responsible for an airport that participate in planning and response activities designed to address unauthorized UAS operations that impact airport operations. In addition to federal, state, and local entities, the local COI includes private sector actors, such as air carriers.
- Federal Security Director (FSD): TSA representative and person charged with overall responsibility for aviation related issues
- National Federal Response (NFR): National-level resources and command and control to halt persistent disruptive UAS operations at an airport.
- Lead Federal Agency (LFA): The agency responsible for C-UAS response at airport (TSA).
- Federal, State, and Local Entities (FSL): The federal, state, and local agencies that should be considered as part of a UAS response plan.
- Steady State Operations: Preparation for a potential UAS incident at an airport.
- Unified Command (UC): Designated individuals from TSA, Airport Operations, and Airport Police that will coordinate a response to a high-level UAS threat
- Threat: The reasonable likelihood that UAS or unmanned aircraft activity– if unabated – would:
  - Inflict or otherwise cause physical harm to a person;
  - Inflict or otherwise cause damage or harm to assets, facilities or systems;
  - Interfere with the operational mission, including movement security, or protection of a covered facility or asset;
  - Facilitate unlawful activity;
  - Conduct unauthorized surveillance or reconnaissance; or
  - Result in unauthorized access to, or disclosure of classified, sensitive or otherwise lawfully protected information.
- Credible UAS Threat: Intelligence indicates that there is a UAS threat to a specific airport, airline, or region, which has sufficient credibility to merit immediate response preparations.
- Essential Elements of Information (EEI): Key information that is documented by TSA after a UAS incident, including characteristics about the timing and activity, identity of the UAS, additional vehicle characteristics such as payload, UAS behavior, operator information, evasive actions that resulted from the incident, impact to flight operations, and media.

Supporting Partners and Agencies

Federal Responsibilities and Authorities

The UAS Response Development Team (UASRDT) at the airport, led by the FSD and Federal Air Marshal Service (FAMS) Supervisory Air Marshal in Charge (SAC), involves the Assistant Federal Security Directors for Law Enforcement (AFSD-LE), Compliance, Transportation Security Specialist-Explosives (TSS-E), and FSL law enforcement support. The UASRDT conducts at minimum yearly updates of the local UAS Plan. Federal supporting entities include:

Transportation Security Administration (TSA)

Mission Responsibilities: Responsible for the security of civil aviation. The Lead Federal Agency (LFA) for C-UAS response at an airport.

Federal Aviation Administration (FAA)

Mission Responsibilities: Responsible for control and routing of air traffic and determining whether a UAS is operating lawfully (for example, operating with a waiver), or unlawfully. Air Traffic Controllers are not required to provide ATC services, including separation, to unmanned aircraft; however, ATC generally provides advisory information from any pilot-reported or tower-observed activity, providing information on the UAS activity, position, distance, course, type of UAS, and altitude.

Federal Bureau of Investigation (FBI)

Mission Responsibilities: Responsible for the investigation of terrorist acts or violent crimes against aircraft.

Local Authority

While state and local entities do not have authority to use counter-UAS technology to mitigate UAS, law enforcement responsibilities may include:

(1) detecting UAS;
(2) reporting incidents to Federal entities (for example, the FAA Regional Operations Center);
(3) observing the UAS in flight;
(4) identifying the type of device (e.g., fixed wing or multi-rotor) and the UAS size, shape, color, and payload;
(5) locating the operator; and
(6) executing appropriate police action to include, among others, obtaining evidence, identifying witnesses, and conducting initial interviews.

In the case that the local law enforcement response is insufficient to stop the UAS operations at the airport, the Federal government may provide assistance through a National Federal Response (NFR) to mitigate the UAS, which may include the use of C-UAS technology. The execution of an NFR will normally not be considered for disruptions where the local community of interest (COI) has not exhausted its own resources to successfully resolve the UOI. Given the shared responsibilities and authorities of airports and FSL agencies in protecting airports, and the areas adjacent to airports, coordination between Federal and SLTT partners to address a specific UAS threat will ensure a unified and complete response.

[Insert: Relevant State Agencies]
[Insert: Relevant Local Law Enforcement Agencies]

Steady State Operations, Vulnerability Assessments, and Incident Preparation

Airport Operations maintains ongoing coordination with law enforcement and TSA to prepare for a response to a potential UAS incident. This includes understanding the C-UAS legal environment, technical capabilities of commercial UAS systems, and UAS operator behavior patterns; ensuring UAS awareness in airport community engagement and community outreach efforts; understanding response requirements and reporting Essential Elements of Information (refer to TSA UAS Tactical Response Plan) should an UAS incident occur; evaluate vulnerabilities, including potential UAS launch sites, around the airport.

Operational Responsibilities (by level of impact)

Low

Report of unauthorized UAS near airport with no disruption to operations. Low impact UAS events could be categorized as those where UAS are no longer active or pose a nominal hazard to the airport, present no indication of intentional harm, and unlikely to cause disruption to airport operations.

Airport Operations: When a UAS report comes in directly to Airport Operations, airport operations personnel will report relevant information to other relevant stakeholders such as airport police, ATC, and TSA. Documentation and reporting should include information pertaining to the UAS such as:

- Location, altitude, and direction of travel
- Description of UAS (color, size, lights, payload)
- Nature of UAS activity and/or interference with flight operations

In the event that there is pilot-reported or tower-observed UAS activity, ATC may alert airport operations with similar information.

Airport Operations and **Airport Police** may determine whether to push the report out to airport field staff for situational awareness and in an attempt to identify/track/monitor a UAS that may be within line of site of airport property.

Medium

Observation of unauthorized UAS operating on or near airport, with the potential to cause disruption to operations, for example by operating in an area of potential safety concern, such as a takeoff or landing path. Medium impact UAS events could be categorized as those that occur in visible proximity of the airport that pose a moderate safety risk to airport operations, present no indication of intentional harm, but has potential to disrupt operations due to proximity of activity.

Airport Operations: Airport Operations will execute protocol consistent with a low-level UAS threat. If UAS activity appears to be creating a potential safety hazard or there is persistent behavior characterizing the definition of a medium-level threat, Airport Operations will coordinate with ATC regarding possible deviations to flight operations. Additionally, Airport Operations may activate additional notification systems and alert public relations.

Airport Police: When an officer responds to a UAS incident within the APD jurisdictional boundary, possible responses may include:

1. Making a radio broadcast of the UAS sighting and include the following information:
   - Location, altitude, and direction of travel
   - Description of UAS (color, size, lights, payload)
   - Nature of UAS activity and/or interference with flight operations
   - Request additional unit(s) to conduct a search of the area for the UAS operator
   - Request Airport Operations to respond to the officer's location
2. Provide the FAA ATC Tower with the location, altitude and direction of travel of the UAS, and ask if the UAS has approval to fly in the area observed.
3. Continue to observe the UAS, provide status updates as necessary, and coordinate the search for the operator with responding unit(s).
   - Average UAS flight times are approximately 20-30 minutes, at which point the UAS will likely return to the operator or designated landing area for retrieval by the operator. It is important that officers track the UAS during the return flight and direct unit(s) to the landing area to identify the operator. The operator can be up to three miles away.
   - If it appears that the UAS operator is located outside the APD jurisdictional boundary, the officer shall contact the law enforcement agency that has jurisdiction over the location and request enforcement of applicable local municipal codes.
   - Enforcement options may include arrest, citation, confiscation of the UAS, and/or notification to FAA/DHS representatives for enforcement of applicable federal regulations.
   - Consideration for arrest and confiscation of the UAS should be given whenever it is determined that the UAS had interfered with manned aircraft flight operations.
4. If both the UAS and operator cannot be tracked or located, document the incident and note any interference with manned flight operations.

High

Persistent unauthorized UAS operating on or near airport, with the intention to cause disruption to operations or intentional harm. High impact UAS events could be categorized as those that occur within the airport's airside environment, pose a substantial safety risk to airport operations, and present indication of intentional harm.

Airport Operations: In a high-threat scenario, Airport Operations will work with Airport Police to exhaust all local resources. In the event that UAS activity has been escalated from medium to high-level threat, and all local resources have been exhausted in trying to identify and detain the UAS operator, Airport Operations will:

- Establish a Unified Command that involves TSA, FBI, Airport Police, and Airport Operations, and make determination for location of command post (relative to the UAS under observation) and communicate it to all agencies.
- Engage in regular conversation and coordination with ATC about any possibility for the need to alter flight paths
- Consider runway closures if the threat is so significant that it requires flight path alterations, for example if there is a UAS, or multiple UAS operating near the east perimeter of the airport at an altitude that conflicts with arriving aircraft, or a UAS operating on airport property with persistent threat to operations.
- If the event is determined to be a clear attack by a UAS on the airport, Airport Operations should work with Airport Police to drive traffic from affected areas and restrict access to authorized personnel.
- Airport Operations should liaise with Airport Police to document all essential information resulting from an incident.

Airport Police: Airport Police will follow the same protocol and response procedures for a medium-level threat. Law enforcement presence under a high-threat scenario may include increased patrols or surveillance at the potential launch locations, at major roads/highways, and requesting periodic aerial surveillance of potential UAS launch sites. Once all local resources have been exhausted, APD will defer to the federal entities as to next steps.

FSD: If the UOI causes a persistent disruption to an airport, and a local response is insufficient to mitigate the UOI, the incident may require a National Federal Response (NFR), governed by the draft CONOPS, Unified National Level Response to Persistent UAS Disruption of Operations at Core 30 Airports. Reference an airport specific TSA UAS tactical response plan for additional protocol.

Recovery

If a UAS incident results in halted air traffic operations, TSA will coordinate with the FAA, airport operations, airport police, and other interested entities to determine when to resume operations at the airport; this will be a joint decision between the Unified Command. To resume operations, Unified Command will require a high level of confidence that there are no other drones operating in the area. Airport Operations should work with ATC to resume operations.

TSA will use the Essential Elements of Information (EEI) checklist to track completion of immediate and follow-up actions and assist in collecting information. In coordination with all involved parties, the FSD will conduct an after action report to assess the response and actions taken.

Reference Documents

1. TSA Counter UAS Tactical Response Plan

Detection Equipment Procedures

[Insert distinguishing procedures, should detection equipment be introduced into the airport environment]

APPENDIX B

INITIAL RECOMMENDATIONS

Remote ID

- Remote ID technology is a critical component of the future UAS detection and identification landscape; the FAA and Transport Canada (TC) are unable to accomplish other regulatory advancements in UAS operations, such as small UAS operations over people and beyond visual line of sight (BVLOS) flights, until Remote ID is implemented. The BRTF urges the regulating authorities to expedite the publication of the Remote ID rule, and in the interim, the FAA and TC should find ways to incentivize voluntary compliance, such as with waivers for part 107 and 135 operations.
- Remote ID should be interoperable with ATC automation, and the Air Navigation Service Provider (NAV CANADA) in Canada, such that target information, including ID and position, can be passed to ATC automatically and is able to display designated UAS targets of interest (e.g., by a public safety official, in Remote ID) to ATC personnel. The Remote ID standards also must be interoperable internationally–a UAS purchased in one country must be visible in the system of another nation.
- Remote ID data also needs to be made available to airport operations and public safety professionals on a real-time basis to facilitate situational awareness and more effective identification of potential UAS threats and ultimately enable errant UAS to be directly associated with their registered operators.
- The BRTF further encourages the FAA and TC to require identification of all UAS rather than exempting hobbyists from Remote ID and to consider requiring retailers and manufacturers to include identification so that future UAS are not sold without Remote ID. Creating this commonsense regulatory requirement will be a valuable step forward in enhancing safety and security.
- The BRTF supports the FAA's work to make the LAANC system available to recreational flyers. The BRTF understands the FAA will expand LAANC to include recreational flyers on July 23, 2019 and recommends operators attend its live drone webinar on July 18. The BRTF will follow the FAA's progress on expanding the LAANC system.
- The BRTF encourages the FAA to partner with the LAANC-authorized USS through the InterUSS Platform as soon as possible to enable another level of known information in the airport environment, including to local law enforcement and airport operators.
- The BRTF supports new TC regulations that became effective on June 1, 2019, that apply to all Remotely Piloted Aircraft Systems (RPAS) operating in Canadian airspace, which requires owners/operators of RPAS to follow the requirements for operations in each class of Canadian airspace.

Communication & Response Planning

- Industry, local law enforcement, and federal agencies should partner in developing airport community communications plans that would alert all stakeholders–including but not limited to air navigation service providers (e.g., the FAA Air Traffic Organization in the United States and NAV CANADA in Canada), airport and airfield operations, airport and local police departments, and airline control centers (to also notify pilots and ground crew)–of authorized UAS in the vicinity. This would help limit concerns about UAS operations in the airport environment and drive appropriate levels of response.

- The prior observation notwithstanding, we understand that in the U.S., the Transportation Security Administration (TSA) is developing UAS incursion response plans both at the local level (in this report termed "tactical UAS incursion response plans") and on a national level (Unified National-Level Response to Persistent UAS Disruption of Operations at Core 30 Airports). In Canada, TC's RPAS Task Force is developing similar plans. The BRTF strongly recommends that response plans at both levels–the tactical and the national–be actively coordinated with airport operators and local law enforcement representatives starting at their earliest phases of development (especially tactical response plans) to ensure effective use of local resources and capabilities; effective coordination among federal, state, provincial, and local partners; and rapid and effective plan implementation.

Risk Assessment

- The BRTF notes that clear threat assessment processes, well-defined and pre-coordinated response roles and responsibilities, and well-enumerated and understood decision-making processes are critical elements of effective airport UAS incursion response plans. These elements should be considered by North American airport operators in close coordination with federal partners when crafting their own UAS incursion response plans–something every airport should have in place. As the FAA recently noted and the BRTF concurs with, "A collaborative approach promotes responsible and effective decisions for how to respond to errant or malicious UAS operations."[2] The BRTF urges the federal governments, including the TSA and TC, to move rapidly forward in its work to develop airport security protocols for UAS incursions.
- North American airport operators, local law enforcement, and their federal partners should work together during response plan development on site survey planning to map high-risk areas for UAS launches and incursions in and around airports. The site planning will provide understanding for law enforcement to respond in the search for an errant UAS operator by first targeting the most likely launch sites.

Response Management

- Preparing for various UAS incursion scenarios–such as a long-term airport closure and the humanitarian, logistical, and communication plans required to effectively manage such a situation–should be part of the regular disaster response planning and training airports undertake.
- With respect to the reopening of an airport and the airspace after a UAS incursion, an airport recovery protocol should be standardized to define recovery and reopening practices with specific lines of authority (transnational, federal, local, airport operator), with characteristics unique to each individual airport determined locally.
- While it is not the position of the BRTF that the detection of UAS in the airport environment should necessarily default to airport operators, at the present time, some airports are moving forward with this mission given the absence of federal action. Therefore, the BRTF suggests that airports and the FAA work together to create an "interim standard" for AIP eligibility for the leasing/purchasing, deployment, staffing, and maintenance of Detection, Tracking, and Identification (DTI) equipment.

Standardization, Testing & Data

- The FAA and TC must work to standardize their approach to UAS DTI technology integration at airports. The most recent guidance from FAA to airports (May 7, 2019) was a step in the right direction, but it leaves the entire burden on individual airports to seek independent legal guidance to confirm the legality of a potential UAS detection system. This approach subjects a single UAS detection system to multiple, potentially inconsistent, legal interpretations in various jurisdictions rather than taking a standardized approach under a uniform regime. This is not an efficient framework for airports or the FAA. The BRTF recommends that the FAA work to standardize approaches to UAS detection technology integration at airports with further testing, work toward uniform standards, and provide more straightforward guidance to airports seeking to deploy DTI technology. In Canada, TC has not provided any guidance to airports on this matter as of August 2019, but must do so as soon as practicable.

- More testing and data collection of DTI and C-UAS technology is required, and federal authorities must work together on a pathway for DTI and C-UAS technology evaluation in commercial settings such as airports, with the ultimate goal of producing performance standards.
- Understanding the extent and nature of UAS intrusions in the airport environment is a key factor in developing mitigation strategies. Individual agencies and operators are working to capture data; however, a combined unified effort could produce more valuable and usable results. The BRTF recommends federal agencies and industry collaborate to create a single UAS reporting system that will capture reports of suspected and confirmed sightings, intrusions, outcomes, etc. In Canada, the Civil Aviation Daily Occurrence Reporting System (CADORS) could be used as the recording system.
- The BRTF believes that manufacturers should share in the responsibility for helping to restrict access to sensitive flight locations, including airports, except for those authorized for approved UAS missions, with the incorporation of geofencing technology.

Education

- More should be done to inform careless and clueless UAS operators about the risks and penalties associated with unauthorized or unsafe UAS operations near airports. Airports should work with local media, government officials, and law enforcement on high-profile public awareness campaigns about the dangers and prohibitions related to operating a UAS at an airport. Signs should be posted in and around airports, including high-probability launch points, with warnings and information on law enforcement action for violating airspace rules.
- UAS knowledge tests for new UAS pilots should include questions to test potential pilots on the rules of operating at airports.

Enforcement

- Laws prohibiting UAS operations in restricted areas, including airports, must be strictly enforced. The BRTF recommends more resources be allocated to the swift and public prosecution of criminal actors. Robust enforcement will also serve as a deterrent to future would-be criminals. The BRTF will also study the issue of whether new laws are required at the federal, state, provincial, and local level to ensure that criminals are stopped and fully prosecuted.

APPENDIX C

REVIEW OF CURRENT POLICY LANDSCAPE & CHALLENGES FACED BY AIRPORTS AND C-UAS INDUSTRY

As the fastest growing segment of aviation, UAS operations continue to rapidly increase in number, technical complexity, and capability. The growth in popularity and use of these new aircraft has presented a number of regulatory and technical challenges for the government, industry, and other stakeholders. The safe and efficient integration of UAS into the NAS requires resolving key challenges to enable evolving technology to safely achieve its full potential. Several of these challenges are related to UAS operations in the airport environment.

In July 2018, the FAA released guidance on UAS detection and countermeasures technology to airport operators pointing to remote identification requirements to be more effective and cost efficient to address airports' concerns around UAS operations; yet the applicable regulatory framework and its effectiveness remain undetermined. Later in 2018, Congress passed an FAA Reauthorization that extended C-UAS authority to additional federal agencies but did not address state and local law enforcement or the TSA–agencies that ultimately will be called on to protect the public from UAS-related threats in and around airports. On May 7, 2019, the FAA published additional guidance to airport operators interested in evaluating, demonstrating, or otherwise installing UAS detection systems that helped to clarify some questions from the airport community, but, like the previous guidance, raised many additional questions that must be addressed. On June 1, 2019, new regulations became effective in Canada for RPAS that are 250 grams to 25 kilograms and include operating the RPAS within the pilot's visual line of sight (VLOS). Beyond visual line of sight (BVLOS) requirements are expected to be developed next in Canada.

Given the continued proliferation of UAS operations and the seriousness of the risk posed, airport operators must have protocols and mitigation strategies in place to manage errant or malicious UAS activity until a permanent framework is implemented. The industry continues to work with government partners on remote identification and tracking rules, but more needs to be done in the meantime. Some in industry are not waiting on government and are taking a proactive approach to mitigating potential UAS risk to critical infrastructure, such as airports, from careless (or clueless) operators. Steps such as installation of Remote ID, geofencing, ADS-B receivers, and knowledge quizzes can go a long way toward eliminating risk through deterrence and education.

Beyond these UAS manufacturer-installed tools, North American airports are interested in UAS detection technology but are taking a measured and informed approach to understanding the technology, any associated risks, and the regulatory framework.

The BRTF will focus on developing UAS mitigation strategies at airports, including a policy and regulatory framework that may also be adaptable to implement outside the airport environment. The BRTF will offer templates for Threat Response Protocols to immediately improve an airport response after intrusion by an unauthorized UAS, determine how best to mitigate this threat, and recommend forward-looking policies.

All stakeholders appreciate the tremendous value of UAS within the airport environment to conduct operationally efficient missions. The safety and security risks, however, cannot be overlooked. The BRTF is seeking to advance aviation and airport safety and security as well as deepen the understanding of, and conversation among stakeholders in order to make significant progress on the necessary policy framework of the future.

Approved UAS Operations at Airports

UAS can add tremendous value to airports by increasing operational efficiencies, improving safety, and adding economic opportunities within the airport environment. Types of operations will continue to evolve and should not be hampered by a lack of policy that supports legal use of UAS.

Memphis-Shelby County Airport Authority (MSCAA) is one of the lead participants in the U.S. Department of Transportation's Unmanned Aerial Systems Integration Pilot Program (UAS IPP). MSCAA has been successfully demonstrating for nearly a year how approved UAS operations can be safely integrated into the airport environment to increase safety, security, and efficiency. Dozens of successful UAS flights have been conducted, with missions including aircraft inspection, airport perimeter fence inspections, and security monitoring of ramps and use in logistics warehouses.

The goal of the UAS IPP is to conduct advanced UAS operations in selected airspace to generate data and knowledge for future UAS policymaking. MSCAA is fulfilling its mission by working to "develop operational procedures, assess potential impacts, develop airport and team member communication protocols, and determine the operational reliability of small UAS that could be used on the Memphis International Airport (MEM) airfield."[3] The DOT and FAA are to be commended for selecting Memphis-Shelby County Airport Authority as a lead participant in the UAS IPP and for bringing government and the private sector together to accelerate safe UAS integration.

Other airports, including Dallas Fort Worth International, Seattle-Tacoma International, Atlanta Hartsfield Jackson International, and Los Angeles World Airports are also developing processes and procedures for using UAS to support emergency response, site survey, wildlife mitigation, and aerial photography missions. Several airport tenants–particularly airlines–have expressed interest in or have started actively utilizing UAS to support their missions, albeit frequently in controlled environments such as inside aircraft hangars.

In Canada, Ottawa International Airport (YOW) became one of the first airports to propose a draft intervention plan, incident protocol, and response approach to TC to assist in the occurrence of a drone incursion within close proximity to their aerodrome. YOW also led the organization of a successful drone tabletop exercise, which was cohosted by TC. Several potential scenario were presented and discussed among participants, and viable approaches were proposed. Available mitigation technology was also addressed. Outcomes from the exercise included: the need for a clear national protocol to deal with RPAS incidents; the adoption of a standard process for addressing RPAS sightings; defining roles and responsibilities; compiling and maintaining data related to RPAS incidents; having a strong media relations network among stakeholders when an RPAS incident occurs and establishing a common communications approach; considering both the economic impact and the potential physical threat of an incident; the expectations on airport authorities; and the education of the public required in the new regulations.

Remote ID and LAANC

The FAA and TC are charged with safely integrating the new UAS class of aircraft and their operators into their respective NAS. The FAA has taken several regulatory steps to increase the safety of UAS operations, including registration requirements and, more recently, the NPRM on the Operation of Small UAS over People, an ANPRM on the Safe and Secure Operations of Small UAS, and an Interim Final Rule on an External Marking Requirement for Small Unmanned Aircraft. One important rule yet to be published–Remote Identification for UAS–is a foundational part of full integration in responding to UAS intrusions in the airport environment. TC has also recently introduced regulations that went into effect on June 1, 2019, which include UAS registration requirements.

Often compared to a digital license plate for UAS, Remote ID will help airport operations teams, law enforcement, and other authorities to quickly identify airborne UAS along with their operators, thereby separating approved UAS operations from errant or illegal ones. Importantly, the FAA intends to create remote identification requirements that will make certain data–including the location, direction, speed, and altitude of an in-flight UAS, as well as the location of the UAS pilot and the UAS's registration information–available to authorized officials on a real-time basis for airborne UAS. The FAA's UAS-ID Aviation Rulemaking Committee (ARC) recommended in 2017, "The UAS ID and tracking system should interoperate with the ATC automation, such that target information from the ID and tracking ground system, including ID and position, can be passed to ATC automation."[4] The BRTF concurs with this recommendation and the additional recommendation from the ARC that "FAA automation and the UAS ID and tracking system should be able to display designated UAS targets of interest (e.g., by a public safety official, in the UAS ID and tracking system) to ATC personnel."[5] The BRTF suggests that the Remote ID standard also must be interoperable internationally–a UAS purchased in one country must be visible in another nation.

Information collected by Remote ID will allow the FAA, TC, NAV CANADA, law enforcement, airport operations teams, and other public officials to instantly identify a specific UAS by a broadcast unique identifier and learn information about the operator, which is critical in an airport environment. This capability gives the authorized individuals access to important data to make an informed determination about the threat level of the suspect UAS. As the Homeland Security Advisory Council's Emerging Technologies Subcommittee noted in its interim report from May 21, 2019, "This will assist security agencies, law enforcement, and aviation regulators to ensure that authorized UAS operations do not pose safety and security threats and to distinguish and focus attention on potential bad actors operating without authorization." The information produced by Remote ID is vital for law enforcement and airport operators to determine how and where to intervene most effectively and also establishes a system for some accountability to be attached to the anonymity of UAS operations.

Remote ID will also require airborne UAS to provide identification information that can be received by other authorized parties to facilitate more advanced operations for UAS and support future UAS Traffic Management (UTM) efforts, which are extremely important to the future of airport operations. Remote ID is vital for the realization of UTM, which would work in conjunction with the existing air traffic control (ATC) system to reduce barriers to innovation and improve security of the national airspace.

Finally, Remote ID will provide airports, law enforcement, and federal authorities a new level of insight on UAS operations–data that can be used to improve aviation safety and approved-UAS integration and unapproved-UAS incursion planning.

The BRTF encourages the FAA and TC to expeditiously publish the Remote ID rule. The BRTF further encourages the FAA and TC to require identification of all UAS rather than exempting hobbyists from Remote ID and consider requiring retailers and manufacturers to include identification so that future UAS are not sold without Remote ID. Creating this commonsense regulatory requirement will be a valuable step forward to enhance safety and security.

While the FAA is working to publish a Remote ID NPRM, the successful Low Altitude Authorization and Notification Capability (LAANC) program offers great potential as a Remote ID solution. Under the Part 107 small UAS rule, operators can fly in controlled airspace under 400 feet as long as airspace authorization is obtained from the FAA. The manual process to apply for authorization is laborious and protracted, but LAANC significantly decreases the wait time and provides greater flexibility in operational planning. LAANC provides automatic FAA authorizations for flights under 400 feet in controlled airspace and accepts applications for authorization to fly above a designated altitude on a UAS Facility Map. LAANC is an innovative collaboration between government and private industry and the first partnership under the FAA UAS Data Exchange.

In this partnership, certain UAS Service Suppliers (USS) are authorized by the FAA to provide LAANC service, and the authorizations are obtained through USS digital platforms. In support of Remote ID benefits until a rule is in effect, the InterUSS Platform software has been developed to allow communication between the various USS during UAS operations. Through partnership with the FAA, information concerning the UAS operator's identity can be validated in the event of a UAS incursion, thereby scaling the response. With this data exchange, airport operators and law enforcement could quickly establish a trusted set of facts and information about the person operating the intruding UAS. The InterUSS Platform provides other benefits, such as event history record, privacy protections, accountability, increased UAS operations, and accident prevention. LAANC is already a success, covering nearly 600 airports, but the full potential of the program is not yet fully realized.

This partnership and remote ID solution could be implemented immediately without additional policy framework, regulations, or technology. The BRTF encourages the FAA to partner with the LAANC-authorized USS through the InterUSS Platform as soon as possible to enable another level of known information in the airport environment, including to local law enforcement and airport operators. The BRTF also supports the FAA's work to make the LAANC system available to recreational flyers. In Canada, Remote ID technology is also available; however, the recently published RPAS regulations do not address this capability, so it is unclear if the regulations would require a revision.

Steps to Full UAS Integration in the NAS

Although Remote ID is an extremely important tool in UAS mitigation at airports, more must be done to protect the safety and security of airports from the risk of hostile and errant UAS operations. Remote ID will allow for quick action against UAS pilots who are operating carelessly or recklessly and emitting an RF signal; however, a UAS operator who has nefarious intent will not likely not be broadcasting a signal that could be detected and tracked. More must be done to ensure aviation safety and the safety and security of airports from the risk of hostile "dark drones."

In the U.S., the FAA and other federal agencies have not indicated a willingness or ability to invest in and operate UAS detection systems on and near airports. Indeed, ATC towers are already frequently understaffed, underfunded, and subject to government shutdowns. In the recent publication of the FAA's Exception for Limited Recreational Operations of Unmanned Aircraft, the FAA reinforced the point that, although the FAA will not engage with UAS detection, the aircraft are operating in FAA-controlled airspace: “Small unmanned aircraft operations do not receive air traffic services, but they must be authorized in the airspace because FAA air traffic control is responsible for managing the safety and efficiency of controlled airspace.” The situation is very much the same in Canada.

This has led some airports to assume that they must fill the void left by the lack of involvement by the federal government. Indeed, stakeholders must be permitted to take steps to better understand the threats in their jurisdiction through detection and tracking. Unfortunately, however, an unclear and uncertain path lies ahead of airports seeking to evaluate, demonstrate, or otherwise install or deploy UAS detection systems. Importantly, the BRTF takes the position that this is not a mission airports should be burdened to undertake.

The FAA issued updated information regarding UAS detection systems at airports in a memorandum dated May 7, 2019. This memorandum, included in Attachment A of this Interim Report, places the burden on individual airports to seek independent legal guidance to confirm the legality of a potential UAS detection system. This approach subjects a single UAS detection system to multiple legal interpretations in various jurisdictions rather than a uniform framework resulting from a standardized approach; this result is due in part to the complexity of the DTI technology and how it changes in each individual airport environment. The guidance also cautioned federally obligated airports that deploying detection technology could be in conflict with their grant assurances, again creating opportunity for different results at airports around the country. The BRTF has identified this as an area requiring further exploration. The BRTF recommends that the FAA and TC work to standardize their approach to UAS detection technology integration at airports with further testing and work toward standards to provide more straightforward guidance to airports seeking to deploy DTI technology.

The BRTF will explore the question of what federal funding is available to help industry test, acquire, deploy, staff, and maintain DTI technology to offset what is otherwise, in essence, an unfunded mandate to airports from the federal government. The BRTF suggests that airports and the FAA work together to create an “interim standard” for Airport Improvement Program (AIP) grant eligibility for the leasing/purchasing, deployment, staffing, and maintenance of DTI equipment. Given the urgency for more knowledge about threats and appropriate mitigations from policy, law enforcement, and C-UAS perspectives, this is an instance where, for the sake of progress, the perfect should not be the enemy of the good.

From an SMS perspective, knowledge of a safety hazard requires action. Airport operators use SMS principles to identify hazards in their operations, assess the risk, and mitigate if a threat exceeds acceptable levels. The risk posed by unauthorized UAS is no different–it requires assessment and mitigation. However, once the risk is assessed, airport operators are limited in mitigation strategies and constrained by laws. Some airports have already begun developing Standard Operating Procedures (SOPs) related to UAS intrusions through SMS, but the mitigation component is missing. The FAA has issued orders and published guidance materials for airports on how to implement a voluntary SMS; this information may be helpful to the FAA and industry to collaborate in building a safety framework for UAS mitigation.

Roles, responsibilities, and flow of information are all a part of response procedures after a UAS incursion in the airport environment. For airport operators, however, guidance remains unclear. Local law enforcement is not authorized to engage in UAS mitigation; therefore, it is likely that federal assistance will be required to address identified UAS threats. The process for making and responding to the request are still under development, leaving airport operators vulnerable to a lack of timely federal assistance.

In addition, following an airport or airspace closure, the recovery protocols for reopening must be defined. The

BRTF recommends that airport recovery procedures be studied further and a protocol should be standardized to define recovery practices with determined authorities, with certain characteristics unique to each individual airport to be determined locally.

The May 7, 2019, guidance further reiterated the FAA's position that it does not support the use of C-UAS by entities other than the federal agencies with specific statutory authority to use the technology. Moreover, besides the FAA's lack of support for the use of C-UAS, significant legal obstacles that restrict most public and private entities from testing, evaluating, or using countermeasures against UAS, including:

United States Criminal Code

- Title 18 contains multiple sections prohibiting acts that implicate UAS mitigation strategies. These sections include prohibitions against damaging or destroying an aircraft; willful or malicious interference with U.S. government communications; and intentional or malicious interference with satellite communications.
- Title 18 has sections under the Computer Fraud and Abuse Act (CFAA) that could be triggered by gaining access to computers without authorization or exceeding authorized access. These acts are crimes even if the unauthorized access is for the purpose of countering or preventing the unauthorized activities of others.
- Title 18 wiretap laws prohibit the intentional interception of communications or disclosing or using the contents of such communications. Recent exemptions from this prohibition only pertain to certain federal agencies under specific circumstances.
- The Aircraft Sabotage Act under Title 18 prohibits damage or destruction of aircraft and could be violated by interference with the flight path of a UAS or some other type of disruption or destruction of a vehicle.
- The Pen Register Act under Title 18 is another protection of electronic communications. It generally prohibits the installation or use, without a court order, a device that "records or decodes" signaling and other information transmitted by electronic communications, or any device capable of identifying information that identifies the source of an electronic communication.
- In Canada, the legal framework for the usage of C-UAS technology has not been discussed with airports, which are awaiting federal guidance on this matter.

The Communications Act of 1934

- Title 47 contains several sections with requirements and prohibitions pertinent to UAS mitigation. These sections require radio transmitter operators to be licensed or authorized; prohibit the manufacture, importation, marketing, sale, or operation of (except by the U.S. government) any unlicensed jammers; and prohibit willful or malicious interference with radio communications of any station licensed, authorized, or operated by the U.S. government.

United States Code – Transportation

- Title 49 prohibits "seizing or exercising control of an aircraft . . . by force, violence, threat of force or violence, or any form of intimidation, and with wrongful intent."

Aviation regulations

- Section 107 under Title 14 requires anyone controlling a UAS to be the designated pilot in command with a remote pilot certificate or a person under his or her immediate supervision. This requirement raises the question of whether a person conducting a C-UAS mission would also be required to hold a remote pilot certificate.

Although Congressional action will be necessary to overcome most of these hurdles, working through the policy framework for delegating and/or expanding C-UAS authority to other entities is a valuable exercise.

Ascertaining intent is another critical area that informs decisions related to both detection/tracking/identification as well as mitigation. Determining whether an operator is clueless or careless versus criminal is an important factor in response and mitigation. Remote ID coupled with DTI data can paint a fairly informative picture of the operator's intent–certainly enough for first responders to determine what level of mitigation to deploy. Information and data will enhance the precision of responses and avoid overreactions. Research and stakeholder meetings to date indicate that most detections fall within the clueless and careless classification. The BRTF believes C-UAS measures would rarely be deployed but should be available under a clear and established process in the event they are needed.

The federal government must rapidly finalize and practice a defined plan for how to respond to a UAS incursion at an airport. The current federal position, which is that "the U.S. Government is working to develop the federal response to a persistent UAS disruption at a major airport," is insufficient and leaves airports vulnerable. The recent work of a federal interagency task force to establish protocols to address a persistent UAS disruption at an airport is a step in the right direction. More needs to be done, however, to rapidly develop and practice specific plans for how to respond to a UAS incursion at an airport, with multiple scenarios as part of the planning process.

Education

The overwhelming majority of UAS and small unmanned aircraft systems (sUAS) operations are flown safely by responsible pilots. Nevertheless, in the interest of constantly improving aviation safety, the BRTF recommends that more be done to educate UAS operators on the dangers of operating around airport environments. Airport area public awareness campaigns on "Authorized UAS Only" are an important and effective tool to warn UAS operators about restricted flight areas. Airports, in coordination with federal, state, provincial, and local law enforcement, should seek to map high-risk areas around airports to gain an understanding of where UAS flights may be launched and to post warnings in those areas.

Some UAS manufacturers are now requiring new operators to pass a short, user-friendly "knowledge quiz" before operating a new UAS. The BRTF supports the concept of a user-friendly test for new pilots to ensure understanding of flight safety and encourages manufacturers to include questions related to the dangers of operating near airports on such tests. Further, manufacturers must educate new UAS operators about the dangers of flying beyond visual line of sight (BVLOS), especially when other aircraft are present in the area. Data from a study published in 2019 by Embry Riddle Aeronautical University showed that more work must be done to educate and warn pilots flying their sUAS beyond their line of sight, because the percentage of flights BVLOS in the study was unacceptably high. Clearly, BVLOS poses a substantial risk in an airport environment.

APPENDIX D

LEARNING FROM LONDON GATWICK'S DECEMBER 2018 UAS INCURSION

On December 19 and 20, 2018, a reported series of repeated UAS incursions resulted in London Gatwick Airport (LGW) being closed for more than twenty-seven hours. In what officials believe was a deliberate attack on LGW, a UAS operator (or operators) was alleged to launch a UAS intermittently from multiple sites around the airport to fly and hover on or near airport property for more than twenty-four hours. The timing of the repeated launches is believed to have been a deliberate effort to prevent the airport from reopening after its initial closure. The radio frequency (RF) signal from the UAS was not transmitting, meaning the UAS and its operator's identity and location were obscured from RF detection. The UAS's lights were on at night, however, to ensure it would be visible by sight, resulting in the airport remaining closed. The persistent UAS threat and the subsequent closure of the airport and airspace created large-scale disruptions throughout Europe and resulted in more than 160,000 passengers missing their flights and connections. The total economic loss is projected to be in the tens of millions of British pounds.

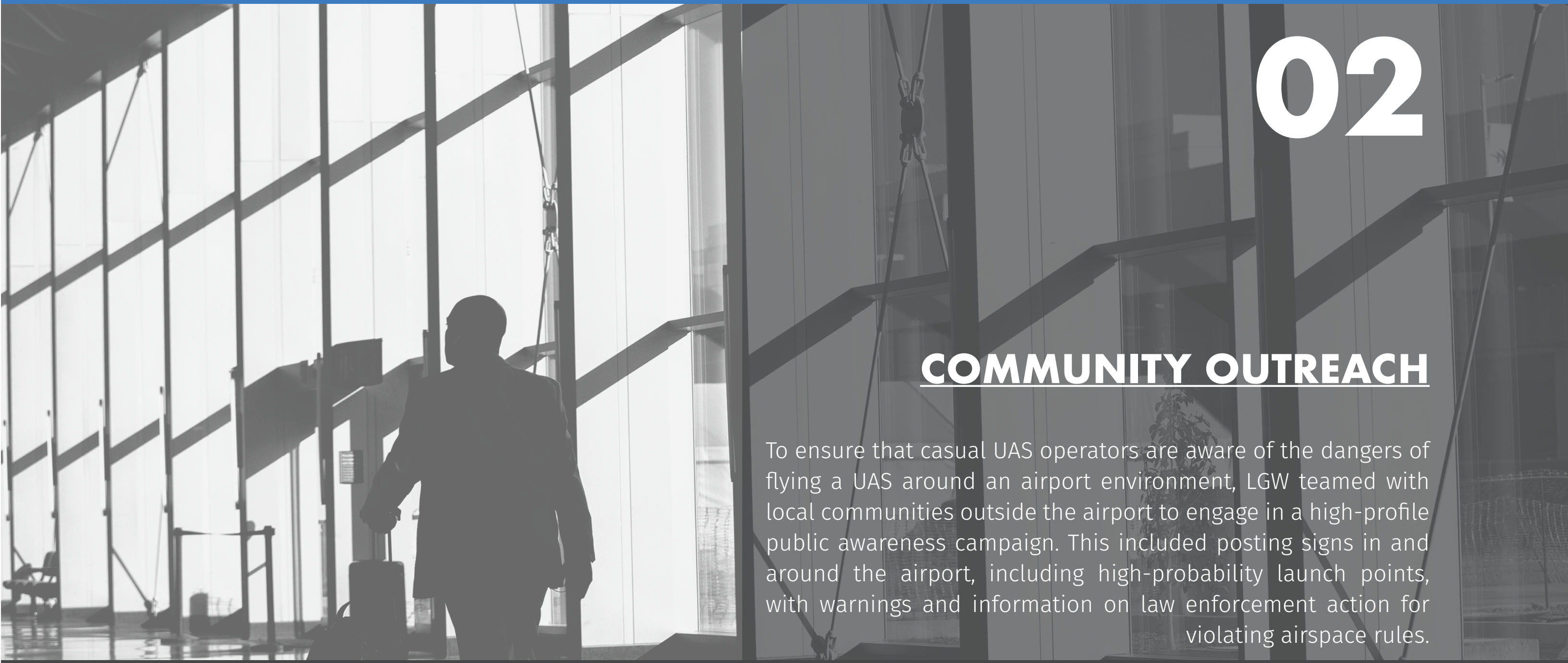
Below are lessons learned from the attack at London Gatwick Airport that can be applied to North American airports as they engage in UAS incursion response protocol planning and exercises:

01

THREAT RISKS AND FUTURE UAS INCURSIONS

LGW undertook a detailed site survey around the airport to understand its threat risks and prepare for future UAS incursions by identifying likely launch points. This understanding allowed police to respond in the search for the UAS operator by first targeting the most likely launch sites.

This site survey planning is an activity that North American airport operators, local law enforcement, and their federal partners, including the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and in Canada TC and the Royal Canadian Mounted Police (RCMP) could work together on now.

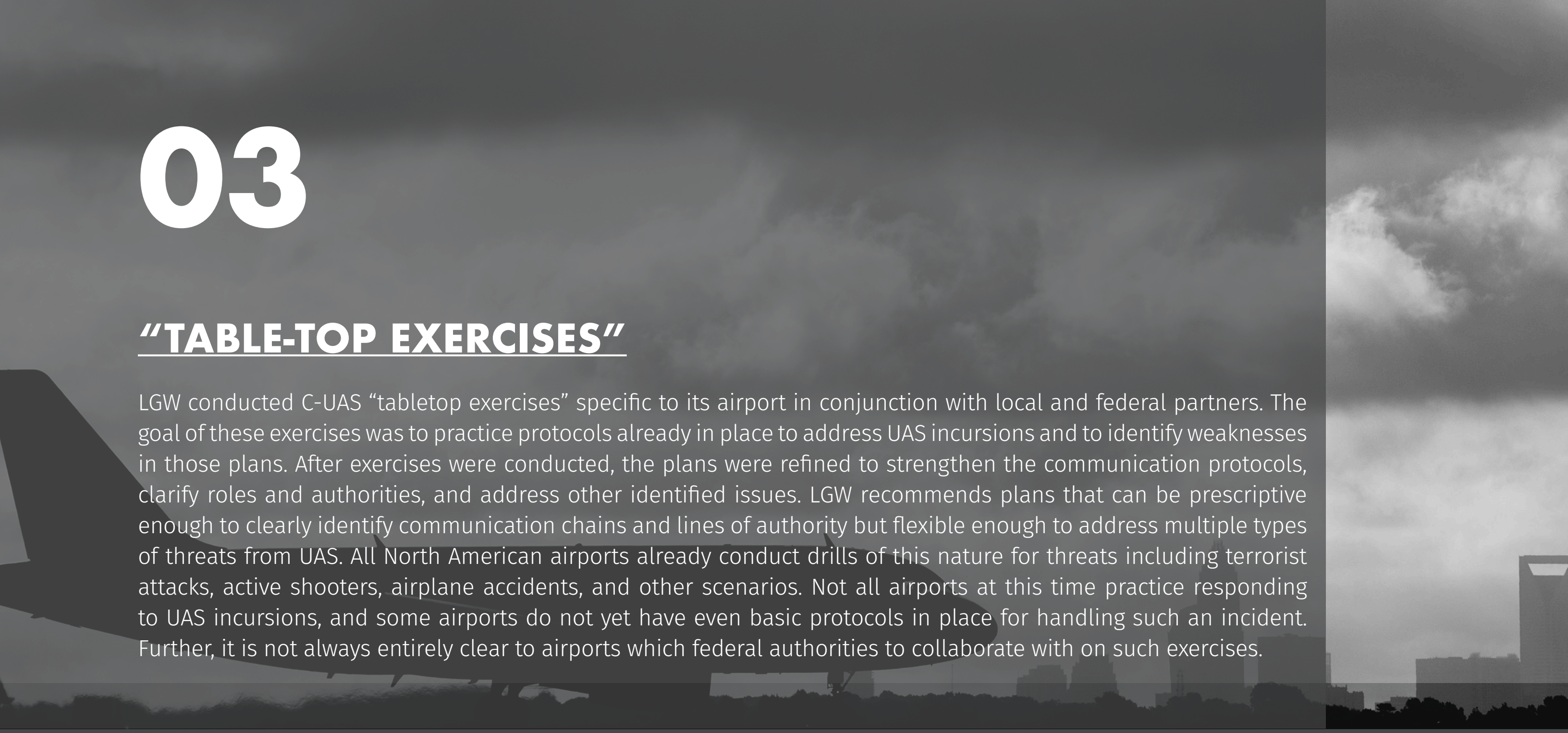


02

COMMUNITY OUTREACH

To ensure that casual UAS operators are aware of the dangers of flying a UAS around an airport environment, LGW teamed with local communities outside the airport to engage in a high-profile public awareness campaign. This included posting signs in and around the airport, including high-probability launch points, with warnings and information on law enforcement action for violating airspace rules.

North American airports are already engaged in public awareness campaigns, but more should be done to inform casual and clueless UAS operators about the risks and penalties associated with operating in and around an airport.



03

“TABLE-TOP EXERCISES”

LGW conducted C-UAS “tabletop exercises” specific to its airport in conjunction with local and federal partners. The goal of these exercises was to practice protocols already in place to address UAS incursions and to identify weaknesses in those plans. After exercises were conducted, the plans were refined to strengthen the communication protocols, clarify roles and authorities, and address other identified issues. LGW recommends plans that can be prescriptive enough to clearly identify communication chains and lines of authority but flexible enough to address multiple types of threats from UAS. All North American airports already conduct drills of this nature for threats including terrorist attacks, active shooters, airplane accidents, and other scenarios. Not all airports at this time practice responding to UAS incursions, and some airports do not yet have even basic protocols in place for handling such an incident. Further, it is not always entirely clear to airports which federal authorities to collaborate with on such exercises.

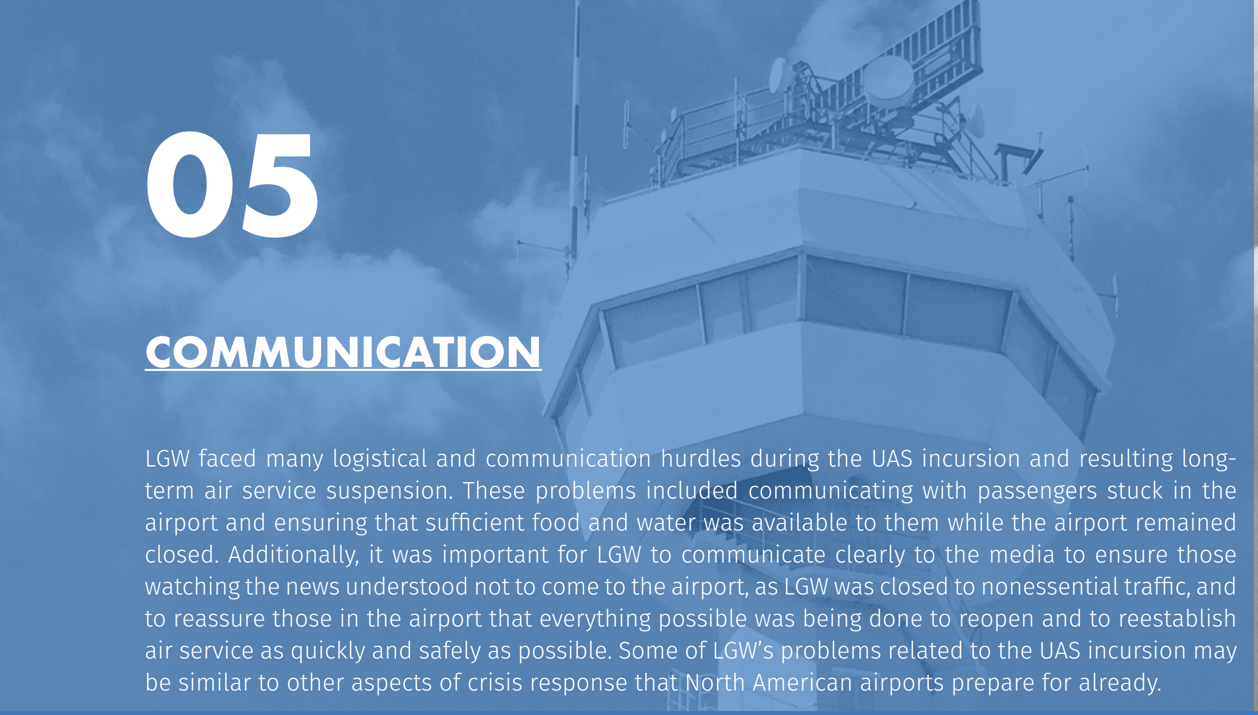
The BRTF will make recommendations in a future report on the basic command and control building blocks airports should have in place to respond to UAS incursions and how best to coordinate and work with transnational and federal authorities.

04

FEDERAL PARTNERS

LGW worked closely with federal partners, including the Royal Air Force, MI5, and the Defense Science and Technology Laboratory on the UAS incursion response.

The BRTF recommends that airports in the United States and Canada similarly work with their respective governments on mitigation plans. Response plans at the tactical and national levels should be actively coordinated with airport operators and local law enforcement representatives starting at their earliest phases of development (especially tactical response plans) to ensure effective use of local resources and capabilities; effective coordination among federal, state, provincial, and local partners; and rapid and effective plan implementation.

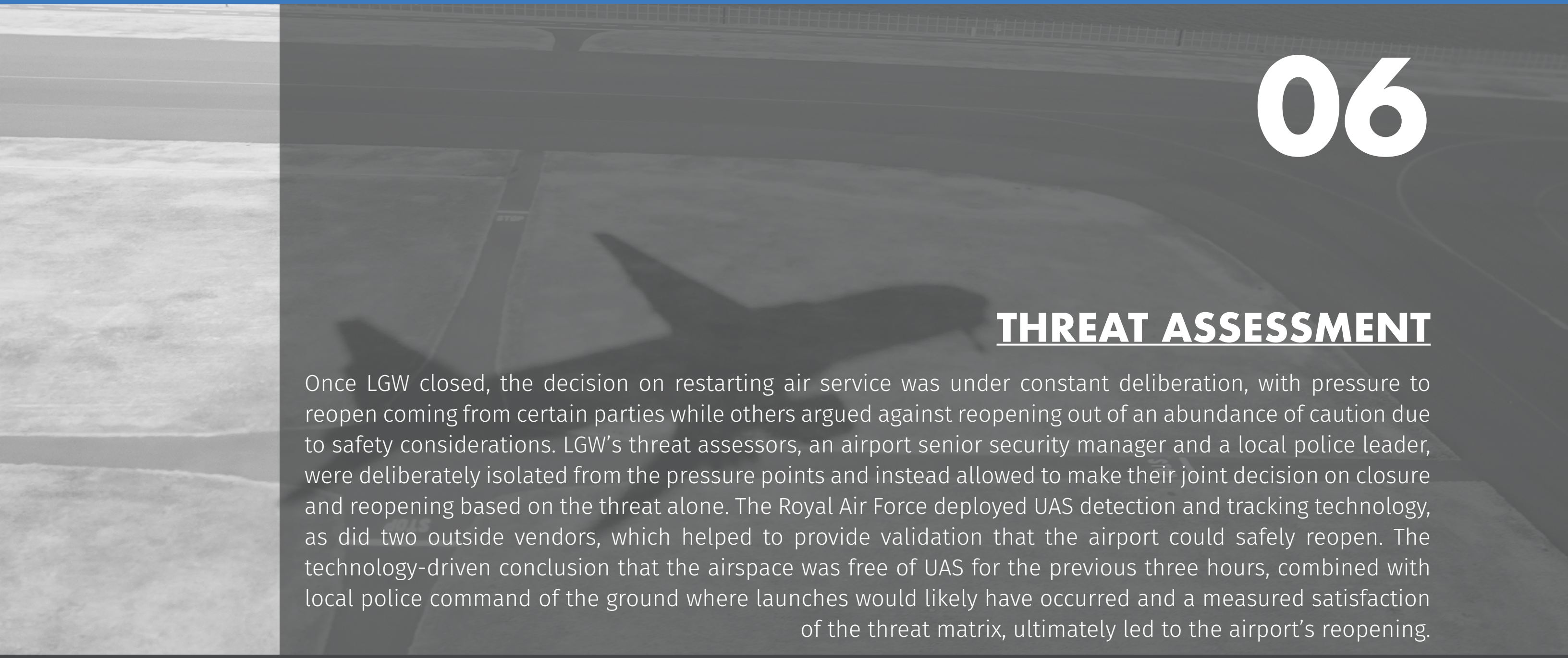


05

COMMUNICATION

LGW faced many logistical and communication hurdles during the UAS incursion and resulting long-term air service suspension. These problems included communicating with passengers stuck in the airport and ensuring that sufficient food and water was available to them while the airport remained closed. Additionally, it was important for LGW to communicate clearly to the media to ensure those watching the news understood not to come to the airport, as LGW was closed to nonessential traffic, and to reassure those in the airport that everything possible was being done to reopen and to reestablish air service as quickly and safely as possible. Some of LGW's problems related to the UAS incursion may be similar to other aspects of crisis response that North American airports prepare for already.

Preparing for various UAS incursion scenarios–such as a long-term airport closure and the logistical and communication plans required to effectively manage such a situation–should be part of the regular disaster response planning that airports undertake as part of their ongoing training. Airports should also prepare to be inundated with requests to "help" the situation by vendors if a UAS incursion occurs. Airports must have a clear understanding of what is legal and safe before engaging with the vendor community. The BRTF will be making more specific recommendations on this going forward, and the FAA has offered guidance in its aforementioned May 7, 2019, letter to airport operators. Airports in Canada are awaiting with anticipation some guidance from TC.



06

THREAT ASSESSMENT

Once LGW closed, the decision on restarting air service was under constant deliberation, with pressure to reopen coming from certain parties while others argued against reopening out of an abundance of caution due to safety considerations. LGW's threat assessors, an airport senior security manager and a local police leader, were deliberately isolated from the pressure points and instead allowed to make their joint decision on closure and reopening based on the threat alone. The Royal Air Force deployed UAS detection and tracking technology, as did two outside vendors, which helped to provide validation that the airport could safely reopen. The technology-driven conclusion that the airspace was free of UAS for the previous three hours, combined with local police command of the ground where launches would likely have occurred and a measured satisfaction of the threat matrix, ultimately led to the airport's reopening.

As North American airports consider their UAS incursion response protocols, having a clear threat assessment matrix and well-defined decision-making authority will be keys to successfully navigating this threat, especially as it relates to reopening the airport and reestablishing air service. These decision authorities and matrixes are areas that North American airport operators should consider and plan for now, in close coordination with federal partners, when crafting their own UAS incursion response plans.

APPENDIX E

TECHNOLOGY OVERVIEW

The BRTF has undertaken a review of various DTI and C-UAS technologies to provide an overview and to help inform future BRTF recommendations on UAS integration and mitigation policy.

At this time, no perfect solution exists for defense against UAS incursions at an airport. Technology, on both the UAS and C-UAS fronts, is evolving rapidly. Remote ID technology is a critical component of the future UAS detection and identification landscape; however, as noted in the "Remote ID" section of this report, publication delays of the Remote ID NPRM prevent UAS safety and security advancements. Accordingly, the BRTF calls on the FAA to publish the rule in an expedited fashion. Beyond Remote ID and its uncertain timeline, no clear pathway exists for additional technology testing, certification, or deployment. With limited ability to test DTI and C-UAS technology in airport-like environments and a material lack of data to inform standards and performance metrics, which technologies could work most effectively in an airport environment to detect errant UAS and, if required, defeat a UAS threat is not entirely clear. More testing and data collection is required, and federal authorities must work together on a pathway for DTI and C-UAS technology evaluation in commercial settings such as airports, with the ultimate goal of producing performance standards.

The BRTF found that in the DTI and C-UAS marketplace, a wide variety of companies offer independent options for detection, identification, or mitigation, including those offering a combined layered approach with multiple tools for each area. Such comprehensive layered options often combine radar, RF, audio, acoustic, cameras, and artificial intelligence (AI) software integration programs for detection, tracking, and identification of UAS, as well as a combination of electronic and kinetic options for interdiction. It is essential that the various technological modalities–with their broad range of accuracy, update rates, and latency–fuse the sensors together seamlessly to ensure layered approaches are accurate with their detection, identification, and tracking and can differentiate between approved and unapproved UAS operations.

Commercial options for UAS interdiction technology are not currently allowed in the United States. The law is even more ambiguous in Canada, where in very limited cases the RCMP, provincial police, and Canadian military would have limited mitigation authority.

Detection, Tracking & Identification (DTI)

Radar

Radar technology, with its all-weather, day/night capability can play an important role as a primary means of detecting UAS-based threats. Radar detects UAS vehicles of virtually any size by the radar signature generated when the aircraft encounters RF pulses emitted by the radar system. Radar can search, detect, and track multiple objects simultaneously, but to be successful, radar must quickly scan large areas with tremendous sensitivity, eliminate nuisance alarms from birds, and discern UAS from ground targets. To help distinguish between UAS and other objects, algorithms, often enhanced with machine learning, are frequently employed. Radar can determine the exact position of an object and differentiate between stationary and moving targets; however, UAS vehicles that only move vertically or extremely slowly sometimes pose a detection challenge. Airport use of radar requires FAA Spectrum Office and FCC approval. No national spectrum licensing approval is available because approvals are site specific. TC is responsible for approving the use of radar technology in Canada, also on a site-specific basis. Challenges to the use of radar include lack of automation, the high dependence on trained operators, field of view limitations, high system cost, and varying accuracy and timeliness of detection. Radar is tuned for identifying small targets at short, medium, and long ranges and typically provides the longest detection range of any sensor type. Radar does not geolocate the pilot of the UAS. It has a medium probability of detection with higher false alarm rates.

Radio Frequency (RF)

Radio Frequency (RF) is a primary detection source with all-weather, day/night performance. Scanners provide a cost-effective solution for detecting, tracking, and identifying UAS over an average detection range of 1–3 km. Detection uses algorithms to scan known frequencies to find and geolocate RF-emitting devices with an approximate location of a UAS vehicle and its operator. Algorithms are also employed to attempt to differentiate between authorized and unauthorized UAS. RF systems have the ability to scan the electromagnetic spectrum and identify the specific transmissions from UAS. As long as the UAS is transmitting a signal, the RF scanner will detect it, but “dark drones” would not emit RF signals. The FAA warns against impacts of RF affecting the safety of flight and air traffic management; vendor identification of whether systems emit RF energy should be analyzed to confirm a total passive state of no emissions. RF-based UAS detection sensors can detect only a few airborne objects at a time, and their accuracy can be affected by numerous sources of potential interference, particularly line of sight obstacles that degrade detection performance. Overall, RF has a high probability of detection with a low false alarm rate. The BRTF is exploring privacy concerns and the various U.S. federal laws that complicate the use of RF technology, including Title 18.

Looking forward to the next five years and beyond, there is a concern that many UAS will phase out RF-based control systems in favor of faster, more reliable, and higher bandwidth control technologies such as 5G cellular networks. RF detection systems are correspondingly difficult to “future proof.”

Optics/Infrared (IR)

Not typically a primary detection source, optical sensors can use infrared or thermal imaging as well as a standard daylight camera. Electro-optical sensors use a visual signature to detect UAS, while infrared sensors use a heat signature. Optical sensors provide visuals on the UAS vehicle and its potential payload and can record images as forensic evidence. An optical system can be difficult to use for detection by itself because it can be challenged by redirection to false targets and is limited by weather and a narrow field of vision and range; often it is paired with radar and RF options as an additional tool for UAS detection verification.

Acoustics

Acoustic sensor technology detects any object that produces noise (sound waves) and can detect sounds produced by UAS motors. Not considered a primary detection source, acoustic sensors are generally combined with other detection tools. Algorithms and noise libraries are employed to attempt to identify the type of UAS and differentiate between authorized and unauthorized UAS. The sensor must properly filter out ambient noise while still detecting small UAS. Acoustic sensors have day/night performance but can be impacted by wind and other background noises. Sensors can detect multiple UAS, and detection is possible even when the UAS does not use

UAS RF communication. Acoustic sensing technology has a low–medium system cost and has a medium probability of detection with a higher false alarm rate, and geolocating the operator is not available.

Counter-UAS (C-UAS)

At this time, C-UAS technology is prohibited in the commercial marketplace. Within the United States, only four federal agencies–DOD, DOE, DHS, and DOJ–have authority related to counter-UAS. This federal authority, however, is extremely limited and not widely deployed at this time. In Canada, only the Department of National Defence (DND) has this authority. As the BRTF seeks to make future recommendation on potential new delegations of authority beyond what has been granted to date, it is important to understand the various technologies that could be used in UAS interdiction. Two primary types of C-UAS technology exist: electronic and kinetic. Electronic mechanisms to defeat UAS require the UAS to be using an RF communications link or GPS. As artificial intelligence (AI) and machine learning (ML) continue to advance, electronic methods of defeat may become less effective as GPS and RF links are no longer used, particularly by nefarious actors.

Electronic Interdiction

Jammers – RF or GNSS

Electronic interdiction is the intentional use of a transmission blocking signal to disrupt communications between the UAS operator and the UAS being operated. Jammers, also called signal blockers, are devices that block communication signals. Technology can disrupt both RF and GNSS links. Once the RF or GPS link is jammed, the UAS can be forced to land immediately or return to its home location. This poses a problem, as it is possible a custom-made UAS could be programmed to crash, causing unintended consequences. Another serious concern with jammers is the unintended consequence of interfering with legitimate communications in the vicinity of the UAS.

Protocol Manipulation (aka Spoofing or Hacking)

Protocol manipulation of a UAS refers to a third party taking over a UAS remotely by impersonating its remote control. The emitted signal instructions are designed to confuse the UAS so that it operates as though the manipulated instruction is the legitimate signal. Protocol manipulation employs algorithms, often enhanced with artificial intelligence, to take control of the UAS with a new, “smarter” communications link that removes the UAS from the threat environment. The manipulating signal gives a third party an opportunity to neutralize the UAS by taking over the flight and downloading its data. This technology requires extensive maintenance of libraries of the communications employed by evolving products on the marketplace, which varies by manufacturer and model.

Kinetic Interdiction

Kinetic interdiction refers to intercepting UAS by physical means. Many types of kinetic options are being tested and, in limited cases, deployed on the battlefield or in high-level special events. In many instances outside of the battlefield, however, kinetic techniques may not be a viable option for use in crowded areas due to the risk of a UAS vehicle crashing or triggering the deployment of a payload.

- Live Fire: The use of conventional weapons, typically firearms, to target and shoot down UAS.
    - Nets: Hardened UAS with attack nets capture and bring back targeted UAS.
        - Autonomous with the option of a manned launch with monitoring.
    - Lasers: Directed energy to destroy the UAS, causing it to crash to the ground.
    - Birds of Prey: Trained birds with protective gear used to attack and crash UAS located in a restricted area.

Geofencing

Although not considered in the C-UAS category, geofencing has mitigating qualities built into the UAS itself. This technology can be regularly updated by manufacturers to include new and temporary restricted zones, evolving with risk-based data and information. Some manufacturers have gone so far as to expand the airport area restricted zones from two-dimensional circles to an enhanced safety zone, preventing UAS from entering a three-dimensional bow-tie geofence to address approach and departure pathways, which will prevent UAS from flying near airplanes departing and landing at airports.

Risk-based solutions such as manufacturer-installed geofencing technology are essential advancements in mitigation and should become the industry standard, rather than the exception. The BRTF believes that manufacturers should share in the responsibility for helping to restrict access to sensitive flight locations, including airports, except for those authorized for approved UAS missions. Geofencing can play a major role in ensuring “careless and clueless” UAS operators are not able to interfere with airport operations.

Rapidly evolving technology will continue to change the landscape of potential DTI and mitigation solutions, which underscores the need to approach UAS safety and security from an overall airspace management perspective. Technological considerations are only one component of fully integrating UAS into the NAS. Government and industry must work together to adopt a holistic policy and regulatory framework for deploying technology, securing UAS command and control connections, and developing well-defined procedures for responding to potential safety and security threats.

ENDNOTES

[1] For this report, the BRTF has adopted terminology that is generally–but not always–consistent with that used by U.S. and Canadian government agencies. “UAS mitigation” refers to a broad set of capabilities, processes, and procedures–often facilitated by technology–that reduce the safety, security, and operational risks associated with unauthorized and/or unsafe UAS activity on or near airports. Unlike U.S. government agencies’ definition, the BRTF considers UAS mitigation to be inclusive of UAS detection and counter-UAS systems, as well as policies and procedures that discourage or disincentivize unauthorized or unsafe UAS operations on or near airports. The term “UAS detection” refers to capabilities, technologies, and procedures that enable the detection, tracking, and identification of UAS. The term “counter-UAS” (C-UAS) refers to capabilities, technologies, and procedures used to disrupt or disable unauthorized or unsafe UAS.

[2] Department of Defense, Department of Energy, Department of Homeland Security, Department of Justice

[3] Federal Register, Docket No. FAA-2019-0364, II.5

[4] Frequently Asked Questions and Answers Concerning UAS Detection Systems https://www.faa.gov/airports/airport_safety/media/Attachment-2-FAQS-UAS-Detection-Systems.pdf

[5] Ibid

[6] The U.S. Senate Committee on Commerce, Science, and Transportation. Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks. June 18, 2019. https://www.commerce.senate.gov/public/index.cfm/hearings?ID=DABED6B9-C9D7-40B9-92DF-428EC1F9D659

[7] Ibid

[8] FAA Public Safety and Government: https://www.faa.gov/uas/public_safety_gov/

[9] It is important to note that 20% of the U.S. is Department of Interior property and, in many cases, DOI, federal law enforcement (e.g., U.S. Park Police, Bureau of Land Management, National Park Service rangers, Indian Affairs, etc.) are responsible for the areas surrounding airports. These agencies should be included in consideration for delegation.

[10] 49 U.S.C § 44903(c)

[11] https://www.faa.gov/airports/airport_safety/media/Attachment-2-FAQS-UAS-Detection-Systems.pdf

[12] https://www.flymemphis.com/drones

[13] FAA UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) Recommendations Final Report, September 30, 2017, Section 6.6.1.2, Operational Considerations.

[14] Ibid.

[15] Homeland Security Advisory Council’s Emerging Technologies Subcommittee Interim Report, May 21, 2019, Section 3.1, Identification and Tracking.

[16] Federal Register, Docket No. FAA-2019-0364, II.5

[17] https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

[18] https://www.faa.gov/airports/airport_safety/safety_management_systems/

[19] https://www.faa.gov/airports/airport_safety/media/Attachment-2-FAQS-UAS-Detection-Systems.pdf

[20] 18 U.S.C. § 1030

[21] 18 U.S.C. § 2511

[22] 18 U.S.C. § 32

[23] 18 U.S.C. § 206

[24] 47 U.S.C. § 151

[25] 49 U.S.C. § 46502

[26] 14 C.F.R. § 107.12 and 107.19

[27] https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

[28] “Small Unmanned Aircraft System Operator Compliance with Visual Line of Sight Requirements,” Embry-Riddle Aeronautical University, International Journal of Aviation, Aeronautics, and Aerospace, Volume 6, Issue 2, Article 3, 2019.

BLUE RIBBON TASK FORCE
ON UAS MITIGATION AT AIRPORTS

FINAL REPORT
OCTOBER 2019

WEBSITE
https://uasmitigationatairports.org

EMAIL
info@uasmitigatiionatairports.org

Report Prepared for the Blue Ribbon Task Force by
The Moak Group

BLUE RIBBON TASK FORCE
On UAS Mitigation at Airports