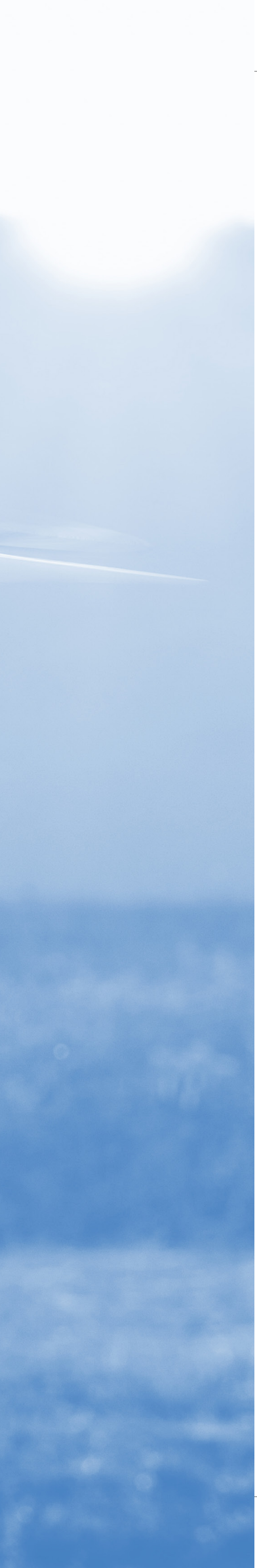

GUIDING PRINCIPLES FOR UAS INCURSION RESPONSE PLANNING AT AIRPORTS

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- Confirmed but no longer active UAS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.