



**UAS Security Overview** 

Presented by Ryan M Berry UAS Security Division, FAA

# UAS Are Changing the Aviation Ecosystem

### **Manned Aircraft**

- Relatively few aircraft; most above 1,000 ft.
- High barriers to entry
  - Costly operator certification
  - High aircraft cost
- Aircraft easily tracked and identified
- Professional operators with certifications at risk—encourages compliance



## **Unmanned Aircraft Systems**

- UAS now outnumber manned aircraft 4:1; most below 500 ft.
- Low barriers to entry
  - Lower operator requirements
  - Very low aircraft cost
- Aircraft and operator more easily concealed
- Public can now access the NAS with no training—far fewer incentives for compliance



# **UAS Security Overview**

Airport and Airspace Disruptions

Border Concerns

> Critical Infrastructure

Criminal
Activities:
espionage,
smuggling,
Cyber,
terrorism

Clueless & Careless Operators





IFSEC Global

## **UAS Security:**

- Protect the NAS and associated infrastructure, and
- Reduce the risk of malicious actors

## Security *and* Safety:

*Threats:* Persons, organizations or other actors intentionally employing UAS for the purpose of terrorism, espionage, or criminal activity.

*Hazards:* UAS operations that create a risk to aviation or public safety through careless or clueless operations—primarily due to ignorance, disregard for rules or loss of situational awareness

Security is integral to UAS integration

Achieved through a partnership of public and private stakeholders

**UNCLASSIFIED** 

# Addressing UAS Security

# First thing to remember is <u>UAS are aircraft</u>

Faa.gov/UAS

**Prevention** 

**Deterrence** 

**Detection** 

Response

## **Operating Rules**

Airspace access, ops over people, BVLOS, Part 107

## **Detection and Awareness**

Remote ID, UAS detection, UAS reporting

## **Counter UAS Systems**

 Coordinating partner use of UAS detection and mitigation systems

Partnerships: Maturing inter-governmental roles, missions

- Whole of community approach
  - Federal Partners
  - State and Local Public Safety Agencies



**Common Security Goal:** Build security into the front end while maximizing the economic and societal benefits of UAS without compromising public safety and national security

# **UAS** Detection and Mitigation

## **Detection**



**RF Sensing / Passive** 



Radar



Electro-Optical / Infrared



**Acoustic** 





#### **Kinetic**

Physical *e*ngagement/interdiction

- o Projectiles and Firearms
- o Net guns
- Capture systems (Hunter/Gatherer)
- Water jets and hoses
- o Birds of prey
- o Directed Energy

#### **Non-Kinetic**

 A non-physical provision of affects against a target, such as sound, light, or electronic means

Electronic Warfare (EW):

- Jamming
- o Redirection
- Counter GNSS

**Detection and Mitigation:** FAA coordinates with security partners to ensure that detection and mitigation capabilities do not negatively impact safety and efficiency

#### UNCLASSIFIED

# Legal Advisory on Use of UAS Detection & Mitigation Technologies

- DOJ, DOT (FAA), DHS, and FCC advisory guidance document
  - Goal: help non-federal public and private entities better understand the federal laws and regulations that may apply to the use of capabilities to detect and mitigate threats posed by UAS operations
  - Provides overview of various provisions of U.S. criminal code enforced by DOJ, and relevant federal laws and regulations related to aviation safety
- Released August 17, 2020 and available online at https://www.justice.gov/opa/pr/interagency-issues-advisory-use-technology-detect-and-mitigate-unmanned-aircraft-systems









Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems

#### August 2020

The Federal Aviation Administration (FAA), Department of Justice (DOJ), Federal Communications mission (FCC), and Department of Homeland Security (DHS) are issuing an advisory guidance document to assist non-federal public and private entities interested in using technical tools, systems, and capabilities to detect and mitigate Unmanned Aircraft Systems (UAS). The advisory is intended to provide an overview of potentially applicable federal laws and regulations, as well as some factors relevant to whether those laws may apply to particular actions or systems.

Specifically, this advisory addresses two categories of federal laws that may apply to UAS detection and mitigation capabilities: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does not address state and local laws, which UAS detection and mitigation capabilities may also implicate. Neither does it cover potential civil liability flowing from the use of UAS detection and mitigation technologies (e.g., the potential liability from causing physical damage to persons or property as a result of mitigating a UAS threat, or civil liability and recovery for an unlawful interception of wire, oral, or electronic communications under 18 U.S.C. § 2520).

This advisory is provided for informational purposes only. It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. As part of that analysis, entities should closely evaluate and consider whether the use of UAS detection and mitigation capabilities might impact the public's privacy, civil rights, and civil liberties. This is particularly important because potential legal prohibitions, as discussed below, are not based on broad classifications of systems (e.g., active versus passive, detection versus mitigation), but instead are based on the functionality of each system and the specific ways in which a system operates and is used. A thorough understanding of both applicable law and the systems' functionality will ensure important technologies designed to protect public safety, by detecting and/or mitigating UAS threats, are used effectively, responsibly, and legally.

# **UAS Integration and Security Flight Path**

Full UAS Integration

UAS Detection/Mitigation System Integration (2023)

Remote ID Rule Effective (2023)

Airspace Restriction Petitions (2022)

FAA Testing of UAS Detection/Mitigation Systems (2022)

Dangerous Weapon Prohibition (2022)

**UAS Digital Forensics Tools (2022)** 

Remote ID Rule Published (2021)

Today

DOJ and DHS Mitigation Authorities (2018)

LAANC Implementation (2018)

Interagency CUAS Event Coordination (2017)

Core 30 CONOPS (2017)

Part 107 Operations (2016)

DOD and DOE Mitigation Authorities (2017)

sUAS Registration (2015)

Low-Risk, Isolated

UNCLASSIFIED

