International Civil Aviation Organization

WORKING PAPER

A41-WP/539
EX/255
13/9/22
(Information paper)
English only

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

UPDATE ON THE UNITED STATES FEDERAL AVIATION ADMINISTRATION'S UNMANNED AIRCRAFT SYSTEMS SECURITY ACTIVITIES

(Presented by the United States)

EXECUTIVE SUMMARY	
This paper presents an update on the United States (U.S.) Federal Aviation Administration's (FAA) activities and coordination on security matters related to the safe integration of Unmanned Aircraft Systems (UAS) into the U.S. National Airspace System (NAS). The paper includes a UAS security overview and updates on UAS-related rulemaking, detection and mitigation coordination, remote identification, and Congressionally mandated research	
Strategic Objectives:	This paper relates to the following Strategic Objectives: • Safety • Air Navigation Capacity and Efficiency • Security and Facilitation
Financial implications:	This paper contains no significant financial implications.
References:	

1. INTRODUCTION

1.1 The rapid expansion of UAS operations in the U.S. NAS presents some unique challenges for both safety and security. UAS technology advancements have led to increased performance characteristics, such as increased altitude, range, endurance and payload capabilities, resulting in greater potential benefits to society. While it is possible to view UAS simply as a new and evolving threat, the FAA believes a more nuanced discussion on risk is an important aspect of UAS integration efforts. UAS security issues evolve from the careless, clueless, and the criminal or malicious non-compliant operation of UAS. All of these unwelcome types of operations can introduce and/or increase risk in the U.S. NAS in the forms of security threats and safety hazards.

1.2 The FAA seeks to integrate UAS into the U.S. NAS successfully and safely consistent with national security and as part of that effort seek to identify as accurately as possible the potential security threats/safety hazards associated with non-compliant UAS operations and taking appropriate steps to minimize their impacts on aviation safety and efficiency. Security threats could include the use of UAS for terrorism, smuggling, or an operator flying a UAS in a flight-restricted area (e.g., prohibited or restricted areas, national security sensitive area, etc.) with malicious intent. Associated hazards from exploiting those threats in turn are impacts to safety of airports, aircraft, public, and disaster and emergency response. The greatest unknown, and most concerning component of the risk calculus, is the determination of the intent of a UAS operator or operation. At this time, it is incredibly difficult to ascertain, in real time, the intent of an operator, irrespective of whether they are in compliance comply with applicable regulations or authorizations at a given point of time.

1.3 Further, the FAA engages with the UAS community to promote a joint understanding of goals and constraints as it develops specific regulations and coordination requirements needed to support operations and reduce risk in the NAS. This engagement supports mutual education and facilitates common approaches and solutions. This paper summarizes recent and forthcoming efforts by the FAA to address the security aspects of integration of UAS into the U.S. NAS.

2. DISCUSSION

UAS Security Strategy

2.1 Security, achieved through partnerships among public and private stakeholders, is vital to UAS integration. The FAA's UAS security goals are to promote the safe and secure integrations of UAS by identifying, understanding, and assessing the risks associated with errant or malicious operations of UAS to protect the NAS, associated infrastructure, and public confidence.

2.2 The approach the FAA uses to address UAS security issues is through the strategic paradigm of "Prepare, Promote, Assess, Act and Discover." By taking this forward-looking and continuous-learning approach, the FAA seeks to build security into the front end while maximizing the economic and societal benefits of UAS without compromising public safety, aviation safety, and national security.

Prepare

2.3 Prepare encompasses issuing regulations to govern UAS activities, such as rules pertaining to airspace access, operations over people, registration, and flights beyond visual line of sight. For flight near airports in controlled airspace, UAS operators must receive an airspace authorization prior to operating in that airspace. Airspace authorizations come with altitude limitations and may include other operational

provisions. All types and purposes of UAS flight operations are prohibited over designated national security sensitive facilities from the ground up to 400 feet above ground level. Examples of these locations are:

a) Military bases designated as Department of Defense facilities;
b) National landmarks, such as Statue of Liberty, Hoover Dam, Mt. Rushmore; and
c) Certain critical infrastructure, such as nuclear power plants.

2.4 The FAA is continuing to consider additional requests by eligible federal security agencies for UAS specific flight restrictions, as received. Additionally, the FAA may issue temporary flight restrictions over some public venues, certain sporting events, and other locations such as wildfire firefighting activities and other disaster response when necessary for safety or security reasons.

2.5 Additionally, in early 2021, the FAA published the Remote Identification (ID) Rule that will help the FAA, law enforcement, and other federal agencies find the control station of a drone when it appears to be flying in an unsafe manner or where it is not allowed to fly. Remote ID also lays the foundation of the safety and security groundwork needed for more complex drone operations.

2.6 Furthermore, the FAA also works with authorized stakeholders to develop policies, procedures, and agreements for the authorized use of UAS detection and mitigation technologies to ensure those operations do not negatively affect the safety and efficiency of the U.S. NAS and air traffic operations.

Promote

2.7 Promote is about ensuring that all stakeholders know and understand the rules associated with the use of UAS; how errant and malicious activities can affect the safety and security of the NAS; and the rules and procedures around the use of UAS detection and mitigation technologies. The FAA uses an intense public education and outreach campaign to reduce incidents of errant UAS operations. Efforts such as the “Know Before You Fly” information campaign, The Recreational UAS Safety Test, and the UAS registration process serve as opportunities to ensure UAS operators understand the rules and responsibilities for safely flying an aircraft within the NAS. The FAA also works closely with federal, state, local, territorial and tribal security, public safety, and law enforcement agencies not only to promote effective enforcement, but also to inform them about lawful, compliant use of the NAS.

Assess

2.8 The FAA works closely with stakeholders to continually assess risk and threat vectors associated with UAS. A major piece of that is the appropriate detection, tracking, identification, and, if necessary, mitigation of UAS.

2.9 All mitigation, and most detection, activity in the United States is limited by longstanding criminal provisions that prohibit interference with the types of technological systems used to operate UAS or the UAS itself. To date, the U.S. Congress has exclusively authorized four U.S. Federal Departments to use UAS detection and mitigation systems within the United States, notwithstanding these potentially conflicting U.S. federal criminal laws, including laws related to electronic surveillance and aircraft piracy: the Departments of Defense, Energy, Homeland Security, and Justice. The relevant authorizing statutes enable these Departments and their component agencies to take certain actions to protect certain facilities and assets from UAS-based threats. Each Department is required to coordinate closely with the FAA to ensure the use of these technologies does not adversely affect the safety and efficiency of the U.S. NAS. This coordination includes FAA reviewing any impacts to the U.S. NAS, including potential radio frequency interference to aircraft, communication, and navigation systems; any flight restrictions that may

be necessary to mitigate secondary effects of UAS detection and mitigation activities on the U.S. NAS; the techniques, tactics, and procedures for employment; planned law enforcement response; and notice to the public and UAS operators. In addition, under section 44801 of title 49, U.S. Code (U.S.C.), the FAA has limited authority to conduct testing of UAS detection and mitigation technologies at five domestic airports.

2.10 Although the U.S. Congress only expressly authorized these four U.S. Federal Departments to take actions otherwise prohibited by law, numerous airport owners/operators, private companies, and law enforcement agencies are interested in the acquisition of UAS detection systems. To alleviate any confusion and advise these entities of the legal considerations they should take into account when acquiring, testing, and using these systems, the Federal Communications Commission (FCC) and the Departments of Justice, Transportation, and Homeland Security, issued the Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems (Advisory). See www.justice.gov/opa/pr/interagency-issues-advisory-use-technology-detect-and-mitigate-unmanned-aircraft-systems.

UAS Detection

2.11 UAS are very difficult to detect using traditional radar and through visual means due to their typical small size and operating characteristics. Advances in UAS technologies necessitate creative ways to detect and provide the required situational awareness, especially in the airport environment. UAS detection technologies exist across several modalities, such as radio frequency (RF), radar, acoustic, and electro-opitcal/infrared cameras.

2.12 RF systems look for the unique signatures of the command and control link and video datalink frequencies in order to detect UAS. These frequencies are matched using a library of signals the system is designed to detect. The downside to this approach is that these detection systems will not successfully detect the UAS if the UAS is operating “dark” or not emitting, or uses a frequency not contained within the library.

2.13 Radar can successfully detect UAS, and is especially useful in detection of non-RF emitting UAS. However, radar also has its limitations, especially in an urban environment. The small size and operating characteristics of UAS often cause the radar returns associated with UAS to be hidden below the noise floor. Lowering the noise floor to detect UAS can cause the “picture” to become too cluttered and potentially unusable to its normal operating purpose. The successful use of radar in the future, especially in the airport and urban environment, will require filtering to detect a signature of a UAS or the prop arc when a UAS is in a hover due to a “Doppler notch”.

2.14 Therefore, it is advisable to use a “system of systems” approach through sensor fusion to arrive at a higher probability of detection. For the FAA, UAS detection systems using passive RF, acoustic, and EO/IR capabilities likely do not introduce risk to the safety and efficiency of the airspace. Anyone considering deployment of a UAS detection system should first determine whether any applicable laws govern their use. Radar and other RF emitting technologies, may cause interference with a variety of aviation-related systems, depending on the frequency. Those who seek to use radar and other RF emitting technologies should coordinate with the appropriate authorities to ensure they have the necessary licenses for operation. Remote Identification (ID).

2.15 Another tool to help with the detection of and response to a UAS operation is through Remote ID. In January 2021, the FAA published the final rule on Remote Identification of Unmanned Aircraft (14 CFR part 89; https://www.faa.gov/uas/getting_started/remote_id/). When fully implemented on September 16, 2023, Remote ID will help the FAA, law enforcement, and other federal agencies find

the control station when a UAS appears to be flying in an unsafe manner or where it is not allowed to fly. Remote ID also lays the foundation for additional safety and security measures needed for more complex UAS operations.

2.16 The final rule on Remote ID requires most UAS operating in the NAS to have Remote ID capability. Remote ID provides information about unmanned aircraft in flight, such as the identity, location, and altitude of the unmanned aircraft and its control station or take-off location. Authorized individuals from public safety and security organizations may request the identity of the UAS's owner from the FAA. Those not operating with Remote ID must operate within a FAA-Recognized Identification Area (FRIA). Additionally, the FAA may provide a waiver to select security organizations that demonstrate a need based on operational security.

2.17 There are three ways UAS pilots will be able to meet the requirements of the Remote ID Rule:

a) Operate a "standard" remote ID UAS that broadcasts identification and location information about the UAS and its control station. A standard remote ID UAS is one that is produced with built-in remote ID broadcast capability in accordance with the Remote ID Rule's requirements.
b) •Operate a UAS with a remote ID broadcast module. A broadcast module is a device that broadcasts identification and location information about the UAS and its take-off location in accordance with the remote ID rule's requirements. The broadcast module can be added to a UAS to retrofit it with remote ID capability. Persons operating a UAS with a remote ID broadcast module must be able to see their UAS at all times during flight.
c) •Operate UAS (without remote ID equipment) at FRIAs sponsored by community-based organizations or educational institutions. FRIAs are the only locations UAS may operate in the United States without broadcasting remote ID message elements.

Act

2.18 When the errant or malicious operation of UAS creates a safety or security incident, the FAA works with its federal, state, and local security and law enforcement partners to ensure appropriate technical mitigation (for those law enforcement partners having appropriate Title 18 relief) and non-technical mitigation responses are taken. To ensure safety the FAA promotes non-technical law enforcement intervention as the best initial course of action. This is due to many incidents being errant, careless, and clueless operations not rising to a critical level requiring the use of technical mitigation.

2.19 The FAA has traditionally relied on law enforcement entities to respond to threats associated with manned aircraft and follows that same approach for UAS. Within the airport environment, the U.S. Transportation Security Administration (TSA) of the Department of Homeland Security has a lead role for addressing UAS threat, to include detection and mitigation enforcement actions pursuant to 6 U.S.C. 124n, as well as non-technical law enforcement intervention. TSA works in close coordination with local law enforcement during these non-technical law enforcement interventions. Additionally, the FAA is engaged in extensive outreach with federal, state, local, and tribal law enforcement entities through its Law Enforcement Assistance Program (LEAP) to provide them with information regarding best practices in responding to UAS incidents and the evidence needed by the FAA to take enforcement action.

2.20 Engagements with the operator must go beyond just finding and interviewing the operator. The FAA advises that law enforcement should inform the special agents of FAA's LEAP so that an investigation can lead to referrals for successful FAA enforcement action or, where appropriate, criminal

prosecution. FAA's goal is to ensure compliance with all applicable regulations to promote a safe and secure operating environment. There are several provisions in the U.S.C., particularly in titles 18 and 49, and in FAA regulations, designed to promote compliance and ensure a safe and secure operating environment. For example, under 18 U.S.C.§ 39B, it is a crime for an individual to knowingly interfere with, or disrupt the operation of, an aircraft carrying one or more occupants; recklessly interfere with, or disrupt the operation of, an aircraft carrying one or more occupants; or knowingly operate an unmanned aircraft within a runway exclusion zone. When violations do occur, the FAA follows its Compliance and Enforcement Program guidance in determining the proper action to take. This can include utilizing civil penalties and certificate actions to deter future violations and address a lack of qualifications. In addition, the FAA works with its partners at the Department of Justice on criminal prosecutions in appropriate cases.

2.21 Use of mitigation technologies, especially in the airport environment, should only be considered as a last resort, and only by authorized entities. UAS are aircraft and mitigating UAS in the United States without specific legal authority may expose the mitigating party to legal consequences, including potential criminal prosecution. Currently, only the four U.S. Federal Departments previously mentioned are authorized to use technology to mitigate a UAS, and those Departments must closely coordinate with the FAA through established processes to minimize potential secondary safety hazards associated with the use of such technologies.

2.22 Mitigation modalities can be either kinetic or non-kinetic. Currently most systems fielded domestically involve net capture devices and non-kinetic modalities such as RF jamming and spoofing. Some RF jamming and spoofing have the potential to interfere with the aviation ecosystem's radio frequency spectrum and could present a hazard to aviation-related systems or non-targeted aircraft.

Discover

2.23 Finally, the FAA must continuously assess how current efforts are working towards the advancement of UAS security and constantly seek to anticipate the future through effective research and evaluation. The rapid advancement and proliferation of UAS into the U.S. NAS, the gaps in operator education, and difficulties in ensuring compliance, have led many stakeholders to demand that the FAA allow the rapid introduction of systems for detection and mitigation of UAS into the U.S. NAS. The FAA is currently conducting research and evaluation of the safety impacts caused by UAS detection and mitigation systems, and plans to conduct future research projects on the security aspects of Urban Air Mobility, Advanced Air Mobility, UAS Traffic Management, and cybersecurity.

2.24 For the study of the potential impacts to the safety of the U.S. NAS caused by the operation of UAS detection and mitigation systems and technologies, the FAA has stood up a test and evaluation program at five domestic airports as mandated by the FAA Reauthorization Act of 2018, Section 383.

2.25 Additionally, Section 383 requires the FAA to develop a plan for the certification, permitting, authorizing, or allowing of UAS detection and mitigation systems in the U.S. NAS and to convene an Aviation Rulemaking Committee (ARC) to make recommendations for the plan.

2.26 The FAA is currently testing to evaluate at least ten technologies/systems that have the ability to detect and/or mitigate UAS in a civil airport environment. Initial testing is ongoing at Atlantic City International Airport (ACY), location of the FAA's William J. Hughes Technical Center. Systems may then graduate for additional testing at four airports selected for participation by the FAA. The FAA will use the baseline performance data collected at ACY to help determine whether and to what extent other airport variables (e.g., geography, noise, interference, proximity to metropolitan areas, airport infrastructure, etc.) affects the performance of each technology and system.

2.27 The results from the FAA's Airport UAS Detection and Mitigation Research Program are expected to inform the ARC and the plan required under title 49 U.S.C. 44810(b). In addition, findings from this research program may be used to update existing information published for airports on the use of certain, limited UAS detection technology. Any such interim information provided to airports following the completion of the research program may be subject to review and further revision based upon the completion of the ARC, NAS-wide plan and follow-on steps for full implementation of title 49 U.S.C. 44810.

3. CONCLUSION

3.1 The FAA will continue to collaborate closely with Member States, our security partners, law enforcement, academia, and private industry to produce a comprehensive and collaborative approach to UAS security in order to support the safe integration of UAS into the aviation ecosystem.

3.2 The Assembly is invited to note the information provided in this paper and visit the FAA's UAS website (www.faa.gov/uas) for more detailed information.

— END —