Welcome and thank you for joining us for today's Aviation Webinar Series. Our topic is **"Drone Defense: The Rules, The Regulations, And What You Can't Do."** We have just a few announcements before we get started.

Please note that this presentation and all of the accompanying materials are protected by copyright, and that the entire presentation is being recorded. Also, please note the material presented by our speakers has been gathered for general informational purposes only.

No information presented in this presentation constitutes legal advice nor is it intended to be fact-specific. As there may be occasions where Fox Rothschild represent clients who may be adverse to your interests, discussion at this program cannot touch upon any fact-specific matters. Attendees should consult with knowledgeable legal counsel to determine how applicable laws pertain to specific facts and situations.

These materials are based on the most current information available. Since it is possible laws or other circumstances may have changed since this presentation, please consult with legal counsel to discuss any action you may be considering as a result of attending this program or reading these materials.

Attendance at this program and/or receipt of these materials is not intended to create nor does it establish an attorney-client relationship.

Fox Rothschild LLP
ATTORNEYS AT LAW

Drone Defense: The Rules, The Regulations, And What You Can't Do

Aviation Webinar Series

October 1, 2019

Presented By

Mark A. Dombroff
Partner, Fox Rothschild LLP

mdombroff@foxrothschild.com
Phone: (202) 794-1211

Mark McKinnon
Partner, Fox Rothschild LLP

mmckinnon@foxrothschild.com
Phone: (202) 461-3120

UAS Risks – Saudi Arabia

UAS Risks - Gatwick

- Incident lasted 3 days, from December 19-21, 2018
- 1,000 flights disrupted
- 140,000 passengers affected, during the three-day incident that began shortly after 9 pm on 19 December last year
- Sussex police received 129 sightings of drone activity
- 96 people of interest identified
- 200 house-to-house inquiries made
- 222 witness statements taken
- Cost of the investigation - £790,000 ($975,000)
- 2 people arrested, they were later released with no further action to be taken

UAS Risks – Overall

- Malicious act
- Collision
- Contraband/smuggling
- IP theft / spying
- Invasion of privacy

Keys to Success – Remote ID

View Rule

View EO 12866 Meetings | Printer-Friendly Version | Download RIN Data in XML

DOT/FAA | **RIN:** 2120-AL31 | **Publication ID:** Spring 2019

Title: +Remote Identification of Unmanned Aircraft Systems

Abstract: This action would implement system(s) for the remote identification of certain unmanned aircraft systems. The remote identification of unmanned aircraft systems in the national airspace system would further address security and law enforcement concerns regarding the further integration of these aircraft into the national airspace while also enabling greater operational capabilities by these same aircraft.

Agency: Department of Transportation(DOT)

Priority: Other Significant

RIN Status: Previously published in the Unified Agenda

Agenda Stage of Rulemaking: Proposed Rule Stage

Major: No

Unfunded Mandates: No

EO 13771 Designation: Other

CFR Citation: Not Yet Determined (To search for a specific CFR, visit the Code of Federal Regulations.)

Legal Authority: Not Yet Determined

Legal Deadline: None

Timetable:

Action	Date	FR Cite
NPRM	09/00/2019	

Keys to Success – Remote ID

- Public meetings at OIRA pursuant to Executive Order 12866 to discuss the proposed rule
- OIRA is required to conduct a cost/benefit analysis and determine whether the benefits of the rule justify the costs
- The review process can take up to 90 days, and can be extended for an additional 30 days
- There is no minimum time for the review
- According to OIRA, the average review period is 53 days
- If OIRA's analysis is favorable, the NPRM would then move forward
- It is possible, however, that at the end of the review period, the rule may be "returned" to the FAA, which would then have to take additional time to revise or redraft the proposed regulation

Keys to Success – Rules regarding Critical Infrastructure

Federal Aviation Administration

22. **UAS Flight Restrictions near Critical Infrastructure Facilities** | Black

Popular Title: UAS Flight Restrictions

RIN 2120-AL33

Stage: NPRM

Previous Stage: None

Abstract: This action would implement section 2209, Applications for designation, of Public Law 114-190, the FAA Extension, Safety and Security Act of 2016 (130 Stat. 634). Specifically, this rule would establish the criteria and procedures for the operator or proprietor of eligible fixed site facilities to apply to the FAA for a UAS-specific flight restriction. In addition, this rule would establish the substantive criteria based on the enumerated statutory considerations (i.e. national security and aviation safety) that the FAA will use in determining to grant or deny a petition, as well as the procedures for notifying the petitioner of the determination made and the process for resubmission of any denial. Lastly, this rule would establish the process to be used by the FAA to implement the UAS-specific flight restriction and notify the public.

Effects:

Economically Significant

Prompting action: None

Legal Deadline: Final: 01/11/2017

Rulemaking Project Initiated: 02/20/2018

Docket Number:

Dates for NPRM:

Milestone	Originally Scheduled Date	New Projected Date	Actual Date
Publication Date	03/01/2020	09/28/2020	
End of Comment Period		11/28/2020	

Explanation for any delay: N/A

***Federal Register* Citation for NPRM:** None

FAA Tools to Implement 2209

- Special Use Airspace:
  - Prohibited Areas
  - Restricted Areas
  - Warning Areas
  - Military Operation Areas (MOAs)
  - Alert Areas
  - Controlled Firing Areas (CFAs)
  - National Security Areas (NSA)
- Other Airspace Areas:
  - Airport Advisory/Information Services
  - Temporary Flight Restrictions (TFR)
  - Air Defense Identification Zones (ADIZ)

- None of the definitions precisely fit congressional requirement
- New type of SUA may be required

Counter Drone Technologies

- Detect – Passive
- Detect – Active
  - Identify aircraft
  - Identify operator location
  - Identify operator identify
- Stop the aircraft
  - Force emergency landing
  - Force return to home
  - Take full control the aircraft
- Destroy the aircraft

Evaluations of Counter Drone Technologies

- SEC. 2206. Pilot project for airport safety and airspace hazard mitigation.
  - (a) IN GENERAL.—The Administrator of the Federal Aviation Administration shall establish a pilot program for airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems
- FAA updated its guidance to airports in May, 2019:
  - Recognizes concerns about Gatwick incident but reaffirms that “FAA does not support the usage of counter-UAS by any entities other than federal departments with explicit statutory authority to use the technology
  - Notes that even passive systems implicate provisions of the law (such as title 18 of the USC) on which the FAA cannot authoritatively opine
  - Installation of equipment may involve 49 USC 44807
  - Promises that FAA is “working to develop the federal response to a persistent UAS disruption at a major airport”

Legal Issues – Jammers

“Jamming devices create serious safety risks. In the coming weeks and months, we'll be intensifying our efforts through partnerships with law enforcement agencies to crack down on those who continue to violate the law. Through education, outreach, and aggressive enforcement, we're tackling this problem head on."

- P. Michele Ellison, Chief, Enforcement Bureau

Legal Issues – Jammers

- **The Communications Act of 1934**
  - Section 301 - requires persons operating or using radio transmitters to be licensed or authorized under the Commission's rules (47 U.S.C. § 301)
  - Section 302(b) – prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 U.S.C. § 302a(b))
  - Section 333 – prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government (47 U.S.C. § 333)
  - Section 503 – allows the FCC to impose forfeitures for willful or repeated violations of the Communications Act, the Commission's rules, regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other Commission authorization, among other things
  - Sections 510 – allows for seizure of unlawful equipment (47 U.S.C. § 510)
- **The Commission's Rules**
  - Section 2.803 – prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 C.F.R. § 2.803)
  - Section 2.807 – provides for certain limited exceptions, such as the sale to U.S. government users (47 C.F.R. § 2.807)
- **The Criminal Code (Enforced by the Department of Justice)**
  - Title 18, Section 1362 – prohibits willful or malicious interference to US government communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1362)
  - Title 18, Section 1367(a) – prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1367(a))

Legal Issues – Marketing Jammers

- Jammers, by definition, can never be authorized because they are designed to interfere with authorized radio communications. Therefore, they cannot be marketed in the United States (except in the very limited context of authorized use by the U.S. government).

- "We emphasize that it is insufficient and misleading for manufacturers and retailers to include a disclaimer on their websites or in promotional or advertising materials stating or implying that U.S. consumers bear sole responsibility for complying with the applicable legal obligations. Such disclaimers are misleading because they fail to disclose that the manufacturer or retailer is also violating the law both by offering the device for sale to U.S. customers and completing the sale transaction. Use of disclaimers that purport to place the sole burden on the buyer cannot absolve the manufacturer or retailer of liability."

Legal Issues – Jammers

- There are substantial criminal and civil penalties for the illegal operation of a jammer, including a civil penalty of up to $16,000 for each violation or each day of a continuing violation and up to one year in prison
- On May 25, 2016, the FCC fined C.T.S. Technology, a Chinese company $34.9 million for marketing and selling signal jamming devices to U.S. consumers
- These jammers ranged from small, concealable devices that would block cell phone or GPS communications for a radius of only a few yards, to high-powered jammers that could disrupt a wide range of communications systems for several blocks
- The company's website falsely claimed that some jammers had been approved by the FCC, and advertised that the company could ship signal jammers to consumers in the United States

Legal Issues – Hackers

- **Violation of the Federal Wiretap Act**
- To the extent a person interdicts and or "takes over" a drone on its property, it might constitute a violation of the Federal Wiretap Act.
- 18 U.S.C. § 2511(1)(a), generally prohibits, with exceptions
  - "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."
- **Violation of 18 U.S.C. § 1030**
- Even if justified under some theory of self-help, hacking into a robot or drone is probably a criminal violation of 18 U.S.C. § 1030 (2012), which imposes punishment on “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.”

Legal Issues – Hackers (FAA Regulations)

- Once the system takes control of the aircraft it becomes the pilot in command
- The system must be able to fly the UAS in accordance with the requirements of the Federal Aviation Regulations
  - Pilot with a Part 107 operators certificate
  - See and avoid vs. sense and avoid
  - Night operation
  - Autonomous operation
- Remediation by Waivers
- Remediation by Exemption

Legal Issues – Hackers and State Law (Michigan)

- A person shall not "Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network interconnected computers"
- “Access” means to **instruct, communicate with**, store data in, retrieve **or intercept data from,** or otherwise use the resources of **a computer program, computer, computer system, or computer network**
- “Computer” means any connected, directly interoperable or interactive **device, equipment, or facility that uses a computer program or other instructions to perform specific operations including logical, arithmetic, or memory functions** with or on computer data or a computer program and that can store, retrieve, alter, or communicate the results of the operations to a person, computer program, computer, computer system, or computer network.
- Felony punishable by imprisonment for not more than 5 years or a fine of not more than $10,000.00, or both

Legal Issues – Hackers and State Law (Connecticut)

- A person is guilty of the computer crime of **unauthorized access to a computer** system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization." Conn. Gen. Stat § 53a-251.
- A person "is guilty of the computer crime of **interruption of computer services** when he, without authorization, intentionally or recklessly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized user of a computer system." *Id.*
- A computer is defined as "a programmable, electronic device capable of accepting and processing data." Conn. Gen. Stat § 53a-250(2).
- A computer system is defined as "a computer, its software, related equipment, communications facilities, if any, and includes computer networks." *Id.* at § 53a-250(7).
- Felony or Misdemeanor depending on the value of any damage done

Legal Issues – Destroyers

- Pursuant to 18 USC § 32(a)(1), it is a felony for anyone to set fire to, damage, destroy, disable, or wreck any aircraft in the special aircraft jurisdiction of the United States.
- The Office of the United States Attorney Criminal Resource Manual § 1405 states that for purposes of Section 32, the special aircraft jurisdiction of the United States applies to the following aircraft while in flight:
  - (a) any civil aircraft of the Unites States
  - (b) any aircraft of the United States armed forces
  - (c) any other aircraft in the United States
- A "civil aircraft of the United States" is defined as an aircraft registered under 49 U.S.C. chapter 441. *See* 49 U.S.C § 40102(a)(17). All small UAS have to be registered pursuant to 14 CFR Part 48, which in turn, invokes 49 USC chapter 441 as the statutory source for the requirement.

Legal Issues – Destroyers

- 18 U.S.C. § 32(a)(5) (2012) Imposes criminal penalties on anyone who "interferes with or disables, with intent to endanger the safety of any person or with a reckless disregard for the safety of human life, anyone engaged in the authorized operation of such aircraft or any air navigation facility aiding in the navigation of any such aircraft
- Criminal provisions in 18 USC § 32 are aimed at interference with manned aircraft, the penalties are steep, and include up to 20 years in prison

New Federal Authority to Deal With Certain Threats

- **6 USC 124n. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT**
- The Secretary and the Attorney General may, for their respective Departments . . . to take such actions as are described in subsection (b)(1) that are necessary to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a **covered facility or asset**.

  (A) Detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

  (B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

  (C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

  (D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

  (E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

  (F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

New Directives from Congress

SEC. 364. U.S. COUNTER-UAS SYSTEM REVIEW OF INTERAGENCY COORDINATION PROCESSES.

- (a) In General.—Not later than 60 days after that date of enactment of this Act, the Administrator, in consultation with government agencies currently authorized to operate Counter-Unmanned Aircraft System (C-UAS) systems within the United States (including the territories and possessions of the United States), shall initiate a review of the following:
- (1) The process the Administration is using for interagency coordination of C-UAS activity pursuant to a relevant Federal statute authorizing such activity within the United States (including the territories and possessions of the United States)
- (2) The standards the Administration is utilizing for operation of a C-UAS systems pursuant to a relevant Federal statute authorizing such activity within the United States (including the territories and possessions of the United States), including whether the following criteria are being taken into consideration in the development of the standards:
  - (A) Safety of the national airspace
  - (B) Protecting individuals and property on the ground
  - (C) Non-interference with avionics of manned aircraft, and unmanned aircraft, operating legally in the national airspace
  - (D) Non-interference with air traffic control systems
  - (E) Adequate coordination procedures and protocols with the Federal Aviation Administration during the operation of C-UAS systems
  - (F) Adequate training for personnel operating C-UAS systems
  - (G) Assessment of the efficiency and effectiveness of the coordination and review processes to ensure national airspace safety while minimizing bureaucracy
  - (H) Best practices for the consistent operation of C-UAS systems to the maximum extent practicable
  - (I) Current airspace authorization information shared by automated approval processes for airspace authorizations, such as the Low Altitude Authorization and Notification Capability
  - (J) Such other matters the Administrator considers necessary for the safe and lawful operation of C-UAS systems
- (3) Similar interagency coordination processes already used for other matters that may be used as a model for improving the interagency coordination for the usage of C-UAS systems

New Directives from Congress

- (l) Department Of Homeland Security Assessment.—
- (1) REPORT.—**Not later than 1 year after the date of the enactment of this section**, the Secretary shall conduct, in coordination with the Attorney General and the Secretary of Transportation, an assessment to the appropriate congressional committees, including:
  - (A) an evaluation of the threat from unmanned aircraft systems to United States critical infrastructure (as defined in this Act) and to domestic large hub airports (as defined in section 40102 of title 49, United States Code);
  - (B) an evaluation of current Federal and State, local, territorial, or tribal law enforcement authorities to counter the threat identified in subparagraph (A), and recommendations, if any, for potential changes to existing authorities to allow State, local, territorial, and tribal law enforcement to assist Federal law enforcement to counter the threat where appropriate;
  - (C) an evaluation of the knowledge of, efficiency of, and effectiveness of current procedures and resources available to owners of critical infrastructure and domestic large hub airports when they believe a threat from unmanned aircraft systems is present and what additional actions, if any, the Department of Homeland Security or the Department of Transportation could implement under existing authorities to assist these entities to counter the threat identified in subparagraph (A);
  - (D) an assessment of what, if any, additional authorities are needed by each Department and law enforcement to counter the threat identified in subparagraph (A); and
  - (E) an assessment of what, if any, additional research and development the Department needs to counter the threat identified in subparagraph (A).

New Directives from Congress

- **“§ 44810. Airport safety and airspace hazard mitigation and enforcement**
- “(b) PLAN.—
  - “(1) IN GENERAL.—The Administrator shall develop a plan for the certification, permitting, authorizing, or allowing of the deployment of technologies or systems for the detection and mitigation of unmanned aircraft systems.
  - “(4) NON-DELEGATION.—The plan shall not delegate any authority granted to the Administrator under this section to other Federal, State, local, territorial, or tribal agencies, or an airport sponsor, as defined in section 47102 of title 49, United States Code.
- “(c) AIRSPACE HAZARD MITIGATION PROGRAM.—In order to test and evaluate technologies or systems that detect and mitigate potential aviation safety risks posed by unmanned aircraft, the Administrator shall deploy such technologies or systems at 5 airports, including 1 airport that ranks in the top 10 of the FAA’s most recent Passenger Boarding Data.
- “(d) AUTHORITY.—Under the testing and evaluation in subsection (c), the Administrator shall use unmanned aircraft detection and mitigation systems to detect and mitigate the unauthorized operation of an unmanned aircraft that poses a risk to aviation safety.

New Directives from Congress

- **SEC. 366. STRATEGY FOR RESPONDING TO PUBLIC SAFETY THREATS AND ENFORCEMENT UTILITY OF UNMANNED AIRCRAFT SYSTEMS.**
  - (a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Administrator of the Federal Aviation Administration shall develop a comprehensive strategy to provide outreach to State and local governments and provide guidance for local law enforcement agencies and first responders with respect to—
    - (1) how to identify and respond to public safety threats posed by unmanned aircraft systems; and
    - (2) how to identify and take advantage of opportunities to use unmanned aircraft systems to enhance the effectiveness of local law enforcement agencies and first responders.

Thank You

If you have any questions, please contact us:

Mark A. Dombroff
Fox Rothschild LLP

8300 Greensboro drive, Suite 1000
McLean, VA 22102

mdombroff@foxrothschild.com
Phone: (202) 794-1211

Mark McKinnon
Fox Rothschild LLP

1030 15th St. NW, Suite 380
Washington, DC 20005

mmckinnon@foxrothschild.com
Phone: (202) 461-3120

For UAS news and analysis, follow us at: https://plane-lyspoken.foxrothschild.com/