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 Commission (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.

I. Federal Criminal Laws

Congress has exclusively authorized the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities to counter UAS presenting a credible threat to covered facilities or assets, notwithstanding certain otherwise potentially applicable federal criminal laws, including various laws relating to surveillance.[1] In addition, the FAA has been expressly authorized to engage in limited testing activities notwithstanding certain federal criminal surveillance laws.[2]

Because no other entities have been granted that authority, it is important that state, local, tribal and territorial (SLTT) and private sector entities without such statutory authority (including SLTT law enforcement organizations, SLTT governments, and owners and operators of critical infrastructure, stadiums, outdoor entertainment venues, airports, and other key sites) understand that federal laws may prevent, limit, or penalize the sale, possession, or use of UAS detection and mitigation capabilities.[3] Capabilities for detecting and mitigating UAS may implicate federal criminal laws relating to surveillance, accessing or damaging computers, and damage to an aircraft. Below, the advisory sets out separately how detection and mitigation capabilities may implicate these laws.

A. Detection Capabilities

Systems that detect, monitor, or track UAS often rely on radio-frequency (RF), radar, electro-optical (EO), infrared (IR), or acoustic capabilities, or a combination thereof. These capabilities detect the physical presence of UAS or signals sent to or from the UAS. In general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, depends on whether it captures, records, decodes, or intercepts, in whole or in part, electronic communications transmitted to and from a UAS and/or controller, and the type of communications involved. Detection systems that emit electromagnetic waves or pulses of sound or light that are reflected off an object and back to the detection system—such as radar, EO/IR, and acoustic systems—are less likely to pose concerns under federal criminal surveillance statutes. Such technology senses the sound or electromagnetic waves produced by or reflected from the UAS and does not capture, record, decode, or intercept electronic communications. However, the use of such systems must also comply with laws and regulations administered by the FCC and FAA, as discussed below.

By contrast, systems using RF capabilities to detect and track UAS by monitoring the communications passed between a UAS and its ground control station may implicate the Pen/Trap Statute and Wiretap Act.

- The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127, criminalizes the "use" or "installation" of a "device" or "process" that "records," "decodes," or "captures" non-content[4] dialing, routing, addressing, or signaling ("DRAS") information. DRAS information is non-content information used to transmit or process communications; depending on the system, this could include device serial numbers, cell site information, media access control (MAC) addresses, the international mobile equipment identity (IMEI), or the international mobile subscriber identity (IMSI). Use or installation of a pen register or trap and

[1] *See* 10 U.S.C. § 130i, 50 U.S.C. § 2661, and 6 U.S.C. § 124n.

[2] *See* 49 U.S.C. § 44810(g).

[3] This advisory does not address the general authorities of public safety agencies, or specific actions they might take consistent with governing law, to protect the public in exigent circumstances.

[4] While non-content is not defined, content is defined in footnote 7, *infra*.

trace device is prohibited, unless conducted pursuant to a court order or when a statutory exception applies.[5] With respect to the Pen/Trap Statute, the exceptions state that they are limited only to providers of wire or electronic communication services.

- *Questions to consider:*
  - What information is the technology collecting (*e.g.*, UAS type, manufacturer, model, protocol, unique identifier, telemetry)?
  - Is the information DRAS or content?
  - Do any Pen/Trap exceptions apply?

- The Wiretap Act (also known as Title III), 18 U.S.C. §§ 2510 *et seq.*, prohibits, among other things, "intentionally intercept[ing]" the content of "any . . . electronic communication[,]" unless it is conducted pursuant to a court order or a statutory exception applies.[6] An "electronic communication" is defined, with certain exceptions, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12).

[5] Law enforcement may use such devices with a court order, but can only obtain such an order in furtherance of an ongoing criminal investigation, *see* 18 U.S.C. § 3122(b)(2), and must use reasonably available technology that prevents the interception of the content of a communication. *See* 18 U.S.C. § 3121(c). Private actors are unable to obtain a court order under the Pen/Trap Statute and, therefore, must operate pursuant to one of the statute's exceptions. The Pen/Trap Statute and Wiretap Act do not contain identical exceptions. For example, while the Pen/Trap Statute includes an exception for use of a pen register or trap and trace device with the consent of a "user," it does not provide an exception based on the consent of a "party to the communication." *Compare* 18 U.S.C. § 3121(b)(3), *with* 18 U.S.C. § 2511(2)(c). In addition, the Pen/Trap Statute does not include an analogue to the Wiretap Act's exception allowing interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i).

[6] The Wiretap Act contains several exceptions to the blanket prohibition, including for operators and service providers, for uses "in the normal course of employment" that are a necessary incident to the rendition of services; for surveillance authorized under the Foreign Intelligence Surveillance Act of 1978; and where a party to the communication has given prior consent to such interception. *See*, e.g., 18 U.S.C. § 2511(2)(a)(i), (d) & (e). Law enforcement may also intercept communications without a court order in certain emergency situations, provided an application for an order is made within 48 hours of the interception. *Id.* § 2518(7).

- The Wiretap Act has an exception for the interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i). Section 2510(16) defines which radio communications do not fall into the foregoing exception. The Wiretap Act also has an exception for the interception of any radio communications that are transmitted "by any . . . aeronautical communications system." *Id.* § 2511(2)(g)(ii)(IV). UAS RF control systems may be considered "aeronautical communications systems" under the Act. However, existing case law raises questions as to the scope of both exceptions.[7]

- *Questions to consider:*
  - Are electronic communications being acquired?
  - Are any acquired communications transmitted by a system that affects interstate or foreign commerce (*e.g.*, a system that is connected to the Internet or a mobile network)?
  - Are any portions of the communications acquired by the technology "content?"[8]
  - Do any of the Wiretap Act's exceptions apply (*e.g.*, is the person intercepting the communications a party to the communication under 18 U.S.C. § 2511(2)(d))?

- 18 U.S.C. § 2512 generally prohibits the manufacture, assembly, possession, sale, advertisement, and distribution of devices that are "primarily useful for the surreptitious interception of wire, oral, or electronic communications."[9] Section 2513 provides that any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of § 2512 may be seized and forfeited to the United States.

B. Mitigation Capabilities

Mitigation capabilities fall into two general categories: non-kinetic and kinetic. Non-kinetic solutions use non-physical measures to disrupt or disable UAS, including RF, WiFi, or Global Positioning System (GPS) jamming; spoofing; hacking techniques; and non-destructive directed energy weapons. Kinetic solutions may employ a variety of measures capable of physically disrupting or disabling a UAS, including nets, projectiles, and lasers. The use of non-kinetic or kinetic solutions may implicate federal criminal prohibitions against, among other things, intercepting and interfering with communications, damaging a "protected computer,"[10] and damaging an "aircraft." The term "aircraft" refers to "a civil, military or public contrivance invented, used, or designed to navigate, fly, or travel in the air." 18 U.S.C. § 31(a)(1). This definition is consistent with the meaning of "aircraft" in 49 U.S.C. § 40102(a)(6). In the FAA Reauthorization Act of 2018, Congress codified the term "unmanned aircraft" as "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft." 49 U.S.C. § 44801(11).

---

[7] *See Joffe v. Google Inc.*, 746 F.3d 920, 928-29 (9th Cir. 2013) (panel rehearing), *cert. denied*, 134 S. Ct. 2877 (2014).

[8] Content is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Importantly, machine-to-machine communications and data transfers between devices can be considered "content."

[9] The statute exempts "officer[s], agent[s], or employee[s] of, or [] person[s] under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof." 18 U.S.C. § 2512(2)(b).

[10] The term "protected computer" includes any computer that is used in or affecting interstate or foreign commerce or communication, or that is used by or for a financial institution or the United States government. 18 U.S.C. §§ 1030(e)(1) & (2).

Jamming technologies are designed to block or interfere with authorized radio communications.[11] Examples of jamming include transmitting RF signals from a jammer at a higher "signal strength" than the RF signals being used to navigate or control the aircraft; preventing a cellular, WiFi, or Bluetooth-enabled device from connecting to a network (such as a cellular system or the Internet); or preventing a GPS unit from receiving positioning signals from a satellite. Spoofing technologies can replicate and replace or modify signals, and can lead to loss of control over the UAS's navigation and communications link (*e.g.*, its link to its ground controller). Hacking techniques generally focus on the UAS's communications link and/or the onboard computer processors.

Jamming, spoofing, and hacking technologies should be evaluated under the federal criminal statutes below (including the aircraft sabotage and aircraft piracy provisions), in addition to the laws discussed above with regard to detection. Because jamming and spoofing are also likely to implicate laws relating to the RF spectrum, parties should carefully review the information in Section II, below, as well.

- The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, among other things, prohibits intentionally accessing a "protected computer" without authorization and thereby obtaining information, or intentionally damaging a protected computer without authorization, including by transmitting a program, information, code, or command that causes such damage.[12] The CFAA broadly defines the term "protected computer"[13] in a manner that could include UAS control systems.

- Interference with the Operation of a Satellite, 18 U.S.C. § 1367, generally prohibits "obstruct[ing] or hinder[ing] any satellite transmission."[14] Jamming, spoofing, degrading or otherwise interfering with GPS signals to a UAS or ground control station could be prohibited under this section, as well as jamming or interfering with any control signals sent to a UAS directly from a satellite.

- Communication Lines, Stations, or Systems, 18 U.S.C. § 1362, prohibits "willfully or maliciously injur[ing] or destroy[ing] . . . means of communication operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States," as well as by "hinder[ing] or delay[ing] the transmission of any communication" over such means of communication. This statute could apply if UAS detection and/or mitigation operations willfully or maliciously degrade or otherwise hinder any frequency or transmissions, including cellular or WiFi signals, with a demonstrable use or intended use by the military or by SLTT law enforcement or emergency personnel engaged in civil defense functions.

Finally, it is possible for mitigation capabilities that destroy, seize, or exercise control of a UAS to implicate federal criminal laws that otherwise apply to "aircraft," as that term is statutorily defined. While all kinetic solutions will likely have one or more of these capabilities implicating those laws, non-kinetic solutions should also be evaluated for compliance.

---

[11] Authorized radio communications include radio communications operating pursuant to federal authorizations or FCC licenses and those operating without a license but pursuant to FCC rules.

[12] The statute exempts the "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State." 18 U.S.C. § 1030(f).

[13] *See id.* § 1030(e)(1), (2).

[14] The statute exempts "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States." *Id.* § 1367(b).

- The Aircraft Sabotage Act, 18 U.S.C. § 32(a), criminalizes certain destructive actions with respect to "aircraft," including damaging, destroying, or disabling those aircraft.

- The Aircraft Piracy Act, 49 U.S.C. § 46502, criminalizes the act of seizing or exercising control of an "aircraft" with "wrongful intent." An intent to seize or exercise control of an aircraft without the legal authorization to do so could involve wrongful intent.

II. Additional Federal Laws Relating to Aviation and Spectrum

In addition to implicating federal criminal laws, the acquisition, installation, testing, and use of UAS detection or mitigation technologies may implicate laws and regulations administered by the FAA and the FCC relating to aviation and RF spectrum. UAS response measures may also implicate existing aviation security laws and regulations administered by the Transportation Security Administration (TSA).

A. Laws Relating to Aviation Safety and Efficiency[15]

Non-federal entities should evaluate UAS detection activities for compliance with laws and regulations administered by the FAA, including but not limited to the following:

[15] This subsection is limited to the discussion of UAS detection systems because, as previously indicated, only certain federal agencies have been expressly authorized by Congress to mitigate UAS notwithstanding certain federal laws. The FAA does not support the use of mitigation systems by any entities that do not have express authority from Congress.

- Use of Airspace. 49 U.S.C. § 40103 establishes a public right of transit through the navigable airspace and vests the FAA with authority to ensure the safety of aircraft and the efficient use of airspace. This includes ensuring that compliant aircraft (including UAS) may move through the airspace without improper interference. For example, detection systems may lead to the identification of both legitimate airspace users as well as unlawful activity. Additional analysis is necessary to identify whether an operation identified by a detection system is in violation of FAA regulation before engaging in an operational response. This also includes identifying and working to address any potential collateral impacts of detection technology or systems on the safe and efficient operation of the National Airspace System.

- Airport Operating Certificates. 49 U.S.C. § 44706, as implemented by 14 CFR Part 139, prescribes the rules governing the certification and operation of airports in the United States. Holders of Airport Operating Certificates issued under 14 CFR Part 139 must protect navigational aids. *See* 14 CFR § 139.333. Commercial service airport operators may also need to update the contents of their airport certification manuals to include operating procedures for the use of a UAS detection system. *See id.* § 139.203. Moreover, the installation or use of UAS detection systems by sponsors of commercial service airports may also implicate other regulatory requirements under CFR Title 14. The FAA has provided extensive information to airport sponsors, which can be accessed at: https://www.faa.gov/airports/airport_safety/#SafetyGuidance.

- Structures Interfering with Air Commerce. 49 U.S.C. § 44718, as implemented in 14 CFR Part 77, requires entities proposing construction or alteration of existing structures in the vicinity of an airport to provide the FAA with notice. *See also* FAA Order 7400.2M, Procedures for Handling Airspace Matters (Feb. 28, 2019). The required notice allows the FAA to conduct an aeronautical study of the potential for the proposed structure and any electromagnetic broadcast signals to create a hazard to air navigation, including interference with aircraft and navigational aids.[16] Entities seeking to install or use equipment for UAS detection activities should also evaluate whether 14 CFR Part 77 requires them to provide the FAA with advance notice of proposed construction or alteration.

- Project Grant Application Approval Conditioned on Assurances About Airport Operations. 49 U.S.C. § 47107 establishes obligations for recipients of grant funds for an airport development project to maintain and operate airport facilities safely and efficiently and in accordance with specified conditions. Airports subject to such conditions may need to ensure that the installation or use of a UAS detection system does not introduce a hazard that cannot be mitigated, consistent with applicable grant assurance obligations, such as Grant Assurance 20, Hazard Removal and Mitigation. In addition, such airports may need to ensure that UAS detection systems and associated structures are accurately reflected in the Airport Layout Plan consistent with Grant Assurance 29, Airport Layout Plan.

For additional information concerning these laws, please contact the Office of National Security Programs and Incident Response at the FAA.

[16] Non-federal entities are encouraged to independently validate the performance and characteristics of UAS detection systems being considered. Significant deviations between vendor claims and real world operation, including the potential for RF emissions and interference, have been observed by the FAA.

B. Laws Relating to Transportation/Airport Security

Through its broad authorities, the TSA oversees the implementation and ensures the adequacy "of security measures at airports and other transportation facilities." 49 U.S.C. § 114(f)(11). TSA may also take appropriate action to address threats, including coordination of security measures with other agencies and to impose requirements on transportation stakeholders, through regulations, security directives, emergency amendments, and security programs. *See* 49 U.S.C. § 114(f)(4) & (l)(1)-(2); 49 U.S.C. § 44932; 49 CFR § 1542.105(d), 1542.303, 1544.305, 1544.105(d), 1546.105(d).

Airports seeking to deploy, buy, or purchase UAS detection or mitigation systems should consider laws, regulations, and security requirements related to local aviation security response. For example, TSA regulations require each operator of an airport regularly serving air carriers to establish an air transportation security program (ASP). *See* 49 U.S.C. §§ 114 and 44903; 49 CFR Part 1542. Among other requirements, the ASP must provide law enforcement personnel in the number and manner adequate to support the program. 49 CFR § 1542.215. In addition, TSA's enforcement authorities include the ability of the Administrator, in consultation with the airport operator and law enforcement authorities, to order the deployment of personnel at any secure area of the airport to counter threats to aircraft and aircraft operations or to address national security concerns, such as those posed by UAS. 49 U.S.C. § 44903(h)(1).

For additional information or coordination, please contact your local TSA Federal Security Director.

C. Laws Relating to the Radiofrequency Spectrum

Any systems that involve emission of radio waves, including radar, must be evaluated for compliance with laws and regulations administered by the FCC, including but not limited to the following:

- Authorizations for Use of Spectrum. Authorized non-federal radio communications include unlicensed operations and operations on frequencies requiring individual licenses.
    - Transmissions on frequencies authorized for unlicensed operations, such as common WiFi and Bluetooth frequencies, do not require a license but may nevertheless implicate statutory or regulatory prohibitions against harmful interference as well as other requirements.
    - Operating on a frequency allocated for licensed private-sector use (such as on the bands used by mobile phones) is subject to licensing requirements and other regulation at the federal level. *See* 47 U.S.C. § 301.
        - For example, use of radar to detect UAS requires a Radiolocation Service license from the FCC. General guidance regarding how to prepare and file an application is available at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/industrial-business/industrial-business-licensing. The application must identify the locations and frequencies where the applicant proposes to operate as well as provide other technical information. Equipment vendors may be able to assist with gathering this information. No prior frequency coordination is required, but if the applicant proposes to operate near a U.S. Government facility, it may wish to consult with appropriate Federal officials before applying in order to avoid having the application rejected when the FCC conducts its Federal coordination.

- Marketing, Sale, or Operation of Jammers. 47 U.S.C. § 302a prohibits most non-federal entities from manufacturing, importing, shipping, selling, or using devices that fail to comply with FCC regulations regarding devices that can interfere with radio reception, including transmitters designed to block, jam, or interfere with wireless communications. 47 U.S.C. § 302a(b).

- Interference with Radio Communications. 47 U.S.C. § 333 prohibits "willfully or maliciously interfer[ing] with or caus[ing] interference to any radio communications of any station licensed or authorized by [the FCC] or operated by the United States Government."

Guidance disclaimer: This advisory is provided for informational purposes only. Guidance documents, like this document, are not binding and lack the force and effect of law, unless expressly authorized by statute or expressly incorporated into a contract, grant, or cooperative agreement. Consistent with Executive Order 13891 and the Office of Management and Budget implementing memoranda, the issuing Departments will not cite, use, or rely on any guidance document that is not accessible through the issuing Departments' guidance portals, or similar guidance portals for other Executive Branch departments and agencies, except to establish historical facts. To the extent any guidance document sets out voluntary standards (*e.g.*, recommended practices), compliance with those standards is voluntary, and noncompliance will not result in enforcement action. Guidance documents may be rescinded or modified in the issuing Departments' complete discretion, consistent with applicable laws.