Deloitte.

AeroDefense
RELIABLE DRONE DETECTION

Legal and regulatory considerations for implementing drone threat security solutions

November 2021

This whitepaper is intended to highlight the complex legal and regulatory environment which governs counter-Unmanned Aircraft Systems (c-UAS) and drone detection technology. Deloitte's US Drone Services practice and AeroDefense have collaborated to provide an overview of the legal landscape applicable to any organization considering or currently employing drone detection and c-UAS capabilities.

UAS proliferation and the rising need to protect assets and facilities against careless, clueless and criminal drone use

The recreational and commercial use of Unmanned Aircraft Systems (UAS), commonly referred to as drones, has expanded rapidly in recent years. In response to the increased proliferation of drones, technology solutions to detect, track, identify, and mitigate UAS and their handsets/controllers have been developed to enable organizations to protect their assets and facilities.

There are two general categories of these technologies: drone mitigation technologies (commonly referred to as counter-UAS solutions (c-UAS)) and drone detection technologies. C-UAS mitigation technology includes a broad range of disruption techniques from kinetic weaponry to signal interference such as jamming or spoofing. Drone detection technology includes radio frequency (RF) monitoring, decoding and demodulating drone signals, Electro-Optical/Infrared (EO/IR) camera systems, acoustic sensors, and radar.

Drone detection and mitigation technologies are governed by U.S. federal law and informed by important policy considerations such as air safety, national security, and privacy. The legal use of drone detection and counter-UAS systems requires an understanding of the authorities required for mitigation and drone signal processing, as well as the procedures for coordinating and deconflicting the use of systems which emit RF energy around airports, military facilities, and other critical infrastructure. Organizations which deploy drone detection and c-UAS technologies must understand the complex U.S. legal and regulatory framework as it relates to an organization's use cases and authorities.

Who governs the legal use of drone detection and mitigation technology?

Multiple US federal agencies jointly-published the Federal Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems in August of 2020. The intent of the Advisory is to assist organizations as they navigate US law and regulations relevant to drone detection and counter-UAS systems.

The advisory addresses two categories of federal laws that apply to drone detection and mitigation:

1. Provisions of the US criminal code enforced by DOJ
2. Federal laws and regulations from FAA, DHS, and FCC

The advisory *does not* address state and local laws which may also apply to drone detection and mitigation technologies.

The National Telecommunications and Information Administration (NTIA), although not referenced in the advisory, oversees military and federal spectrum experiments and allocations related to drone detection and mitigation technology.

Drones: How they communicate and why it's important

Understanding how drones communicate is critical to understanding how laws and regulations are applied to their use. A majority of recreational and commercial drones operate in the Industrial, Scientific, and Medical (ISM) RF band using proprietary protocols. This includes Frequency Hopping Spread Spectrum (FHSS) and Wi-Fi or Bluetooth drones.

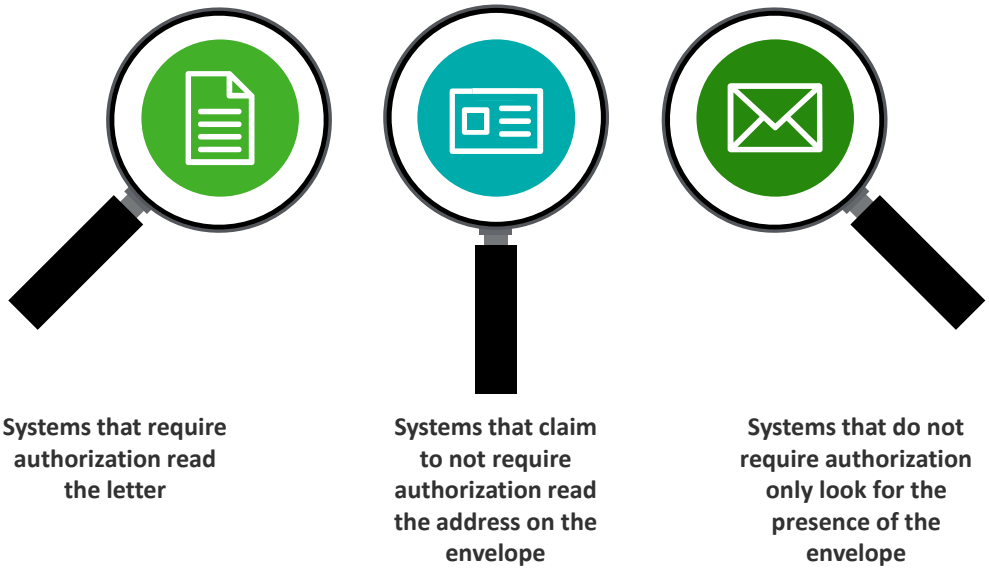
A drone controller sends an RF signal from the remote control up to the drone which directs the drone where to fly. Then a drone telemetry signal and/or video signal is sent back down to the controller. These signals sent back and forth contain information such as a drone's serial number, its GPS coordinates, and much more. A drone's communications with its controller are protected by privacy laws in much the same way a private telephone conversation is protected.

RF-based drone detection systems primarily use two different methods to detect drones:

1. Sensing a drone signal in the RF/Wi-Fi environment by monitoring for physical characteristics (known as spectrum sensing)
2. Demodulation and decoding of a known RF or Wi-Fi signal (known as "cracking the packet" or "reading the packet")

Figure 1 below outlines the difference between the methodologies and how they apply to current legal and regulatory guidance.

Figure 1: RF-based drone detection methodology example



RF-based systems that "read the letter" require federal authorization from the DOJ because they demodulate and decode drone signals to obtain certain information about the device such as its serial number. Other systems claim to be legal without authorization because they only "read the address on the envelope", however, they also require DOJ authorization. For example, this could be a system that reads "header" or "address" information such as the timestamp or GPS coordinates from the signal. Systems that do not require authorization utilize spectrum sensing which monitors the physical environment for drone and controller RF signals.

The regulatory landscape

Given the regulatory complexities of the evolving counter-UAS and detection capabilities landscape, organizations face a daunting task to evaluate, procure, and deploy such technology. Each entity needs to understand its authorities, unique UAS threat profile and establish tailored UAS risk management programs. Strategic and operational considerations are compounded by the legal and regulatory questions mission leaders will need to answer before they engage in the wargaming and response planning critical to protecting their assets and people from UAS threats. These issues include impacts to public privacy, operational guidelines within the National Airspace System, and UAS-specific spectrum considerations outlined by the Federal Communications Commission (FCC).

The FCC and Federal Aviation Administration (FAA) both administer laws and regulations regarding the use of drone detection and counter-UAS technology. The FAA maintains overall authority regarding safety of the nation's airspace and aircraft. The use of counter-UAS technology that actively mitigates UAS flight through RF transmissions could potentially disrupt airport operations, such as affecting navigation beacons or airport communications infrastructure. Additionally, the FAA imposed mandatory reporting requirements for agencies which activate and use authorized counter-UAS systems. The FCC maintains oversight of technology systems which emit radio waves, all of which must be evaluated under FCC regulations. Counter-UAS systems which actively mitigate are subject to FCC regulation and certification given that many of them transmit signals on government-controlled frequencies.

The Department of Defense (DoD), Department of Energy (DOE), Department of Justice (DOJ), and Department of Homeland Security (DHS) are currently the only federal organizations permitted to engage in UAS signal analysis and mitigation activities.[1]

The DOJ enforces provisions of the U.S. criminal code which are applicable to systems detecting UAS. These laws include the Pen/Trap Statute which criminalizes the use or installation of a device or process that records, decodes, or captures non-content dialing, routing, addressing, or signaling (DRAS) information.[2] Additionally, the Wiretap Act prohibits intentionally intercepting any wire or electronic communication.[3] Other laws include the Aircraft Sabotage Act which criminalizes destructive actions with regards to aircraft and the Aircraft Piracy Act which criminalizes the act of seizing or exercising control of an aircraft with wrongful intent.

Table 1 below outlines the key questions put forth in the Federal Advisory related to the Pen/Trap Statute and the Wiretap Act. Entities considering drone security solutions should consider the questions below as they look to integrate relevant technologies into their infrastructure. These legal and regulatory considerations are intended to stimulate inquiry as to whether an organization has the appropriate authority to deploy a desired technology solution and what the potential penalty could be for deploying an unauthorized system.

As stated in the federal advisory, "In general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act (enforced by the DOJ), 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."

Table 1: Legal and Regulatory Considerations

Legal and Regulatory Considerations[4]	
Pen/Trap Statute	**Wiretap Act**
• What information is the technology collecting? • Can the information collected or acquired by the drone or controller be considered "content"? • Is the information DRAS (dialling, routing, addressing, or signalling) or content?	• 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?" • 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))?

Authorization to use 6 U.S. Code § 124n (Protection of Assets and Facilities)

To assist the DOJ and DHS in combating drone threats, Congress passed the Preventing Emerging Threats Act of 2018 (codified at 6 U.S.C. § 124n) ("the Act"). The Act provides DOJ and DHS with a tailored grant of authority for authorized Department components to take certain counter-drone actions to mitigate credible drone threats to designated facilities and assets.

[1] August 2020. Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems.
[2] Ibid.
[3] Ibid.
[4] Ibid.

DOJ guidance clearly provides instructions for an authorized Department to operate protective measures without being prevented by provisions of law, namely 49 U.S.C. § 46502 (aircraft piracy), 18 U.S.C. § 32 (destruction of aircraft), 18 U.S.C. § 1030 (computer fraud), 18 U.S.C. § 1367 (interference with the operation of a satellite), and chapters 119 (interception of communications) and 206 (pen registers and trap and trace devices) of Title 18.

If an authorized Department component seeks to have a facility or asset designated as a covered facility or asset and deploy protective measures, the component head must submit a written request for approval to the Deputy Attorney General (the "Approving Official"). If an authorized Department component wishes to make a significant change to a previously designated covered facility or asset or a previously authorized protective measure, it must submit a request to the Approving Official updating the information previously provided. Changes to c-UAS system settings must be coordinated in advance with the FAA and, when relevant, the NTIA.[5]

There is a significant level of effort required to deploy a mitigation and detection system at a covered facility, with minimal flexibility for system modifications. Organizations should consider if it may be more efficient to deploy RF-based drone detection systems not governed by 124n depending on the specific organizational security requirements.

Conclusion

As both the complexity of drone threats and the legal landscape surrounding counter-UAS topics continue to evolve, Deloitte and AeroDefense can help clients adapt to the challenges and remain compliant with federal, state, and local legislation. AeroDefense and Deloitte have developed a comprehensive airspace security solution and have the proficiency required to manage risks posed by UAS in a broad range of applications.

Deloitte's US Drone Services

Deloitte Drone Services' drone detection and counter-UAS solutions portfolio leverages the firm's breadth of experience, capabilities, and relationships to offer solutions across all aspects of counter-UAS program design and execution. Deloitte has direct insight into UAS innovation and how disruptive UAS technology can change the threat profile through its work with state and federal officials, as well as assisting the private sector to stand-up UAS operations.

Peter Liu

Deloitte Consulting LLP| Managing Director

Peter leads Deloitte's Emerging Infrastructure Platforms market offering and Deloitte's Drone Services practice.

[5] 6 U.S. Code § 124n - Protection of certain facilities and assets from unmanned aircraft

AeroDefense

AeroDefense's AirWarden™ RF-based technology simultaneously detects and locates both commercial and homemade "kit" drones and their operators, often before a drone(s) takes flight. AirWarden utilizes spectrum sensing technology, fully complies with the Federal Advisory and is not governed by 124n. AeroDefense's AirWarden system is also the first and only drone detection technology to receive the Department of Homeland Security Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act designation.

Linda Ziemba

AeroDefense | Founder & Chief Executive Officer

Linda Ziemba is the Founder and CEO of AeroDefense, New Jersey-based provider of American-made, proprietary drone detection technology. AeroDefense's AirWarden™ system detects and locates threatening drones and their controllers simultaneously and sends alerts to security staff so they can safely mitigate the threat. Linda built and led the team that developed the first, and so far only, drone detection system to receive a Department of Homeland Security SAFETY Act designation.

About the authors

We would like to acknowledge the authors and contributors from the Deloitte and AeroDefense teams in the production of this publication: Andrew Stiles, Adam Schenkel, Lexi Rinaudo, Christine Griffin, Peter Hwang.