ADVISORY

pillsbury

Interagency Advisory Provides Guidance on Drone Detection and Mitigation Technology

By Glenn S. Richards and Warren A. Kessler

On Monday, August 17, 2020, the Department of Justice, the Federal Aviation Administration, the Department of Homeland Security, and the Federal Communications Commission released a **joint advisory** on the acquisition and use of counter-drone equipment by non-federal public and private entities. In the Advisory, the agencies highlight federal criminal laws and other federal statutes and regulations that may be implicated by the use of such technology, specifically for drone detection and mitigation.

The Advisory comes at a time when the United States is seeing a significant uptick in the use of drones or unmanned aircraft systems ("UAS"). Last week, the **FAA noted** that more than 1.6 million commercial and recreational drones are registered with the agency, and that it has certified more than 188,000 remote aircraft pilots. This widespread adoption of drones has heightened security concerns over the risk that they could present to the public, particularly at widely-attended outdoor events such as sporting events or concerts. In addition to the use of drones in warfare, high profile domestic incidents, including this week's **close call between a drone and Air Force One** over the Washington area, present a case for the need for effective and widely available counter-UAS measures. As tech companies race to develop solutions, federal agencies are cautioning the public to be mindful of the possible legal restrictions of selling and operating counter-UAS technology.

Criminal Liability

The Advisory notes that federal prohibitions on UAS detection and mitigation are based on functionality, specific operations, and how the technology is used. The Advisory also reminds the public that Congress has exclusively authorized only the Departments of Defense, Energy, Justice, and Homeland Security to perform detection and counter-drone measures, and even then, only in very limited circumstances. The FAA is also authorized to perform certain testing activities. Other users, such as local law enforcement and private entities are hamstrung behind wide-reaching federal criminal statutes.

Addressing the legality of drone detection technology, the Advisory concludes that systems that emit electromagnetic waves, pulses of sound, or light that are reflected off an object and back to the detection system, such as radar, are generally permissible (subject to FCC approval). However, technology that collects or tracks UAS communications may implicate federal prohibitions on certain forms of surveillance, including the Wiretap Act, the Pen Register Act, and related laws that prohibit the sale of devices that are "primarily useful for the surreptitious interception of wire, oral, or electronic communications."

Similarly, counter-drone "mitigation" techniques (anywhere from shooting down drones with buckshot to more high-tech solutions) present their own risks. The Advisory warns that "kinetic" techniques (physically disrupting a drone with a net, projectile, or laser) and "non-kinetic" techniques (using non-physical measures such as radiofrequency radiation, WiFi, or GPS) each come with potential liability. Federal laws that prohibit the tampering or sabotage of aircraft also apply to drones.

Jamming technologies, which are "designed to block or interfere with authorized radio communications" are also prohibited. According to the Advisory, jamming includes "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." Also prohibited is "spoofing," by which UAS signals are replicated or changed to cause its operator to lose control of the craft.

Agency-Administered Rules and Regulations

In addition to criminal liability, the Advisory presents several statutes and regulations administered by federal agencies that affect the use of counter-drone technology, including laws and regulations dealing with aviation safety (administered by the FAA), transportation and airport security (administered by the TSA), and radiofrequency ("RF") spectrum (administered by the FCC).

Regarding the use of RF spectrum, the FCC generally regulates counter-drone technology within the confines of the following code sections and their related FCC rules: (a) 47 U.S.C. § 301, which prohibits the transmission of radio signals without proper authorization, and generally prohibits RF interference; (b) 47 USC § 302a, prohibiting most non-federal entities from manufacturing, importing, shipping, selling, or using noncompliant devices, including those that unlawfully interfere with radio communications; and (c) 47 USC § 333, prohibiting harmful interference against authorized communications systems. According to the Advisory, the FCC interprets these code sections to prohibit the use of devices that can "interfere with radio reception, including transmitters designed to block, jam, or interfere with wireless communications."

Conclusion

As the counter-UAS industry has developed and evolved, the regulatory environment surrounding it has not. Despite some recent high-profile legislation and agency rulemakings impacting drone use, the Advisory is a reminder to counter-UAS manufacturers and operators of the limitations on selling the technology to all but a handful of federal agencies. However, with an election on the horizon, new legislation and agency action could soon take shape that will permit for more widespread use of this important technology.

pillsbury