Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Law Enforcement and the Evolving Counter-Unmanned Aircraft Systems (C-UAS) Landscape

February 27, 2026

As the use of unmanned aircraft systems (UAS)—commonly referred to as *drones*—for both commercial and recreational purposes has increased, so too has law enforcement agencies' use of this technology. Simultaneously, law enforcement has been concerned about the *malicious* use of drones and the ability to counter it. UAS may pose unique public safety or security risks. Some have warned, for instance, that drones can be used as reconnaissance tools for criminals "because they can fly past bollards, checkpoints, and other security mechanisms." For example, U.S. Customs and Border Protection (CBP) has noted that transnational criminal organizations use drones to surveil and evade border officials. Drones have also been used to drop illicit drugs and other contraband into jails or prisons. The Federal Bureau of Prisons, for example, notes that criminal networks deliver illicit drugs, weapons, cell phones, and other contraband to inmates via drones and that these drone incursions are increasing. Yet another concern involves potential use of drones to "drop a bomb, shoot firearms, or spray a poison gas over large crowds of people" at a public event. Consequently, policymakers have questioned whether or how law enforcement may be able to engage in counter-unmanned aircraft system (C-UAS) activities—including detecting, identifying, monitoring, tracking, communicating with, and disrupting or disabling suspicious or malicious drones.

Law Enforcement C-UAS Landscape

Law enforcement C-UAS activities generally fall into two broad categories: detection (including monitoring and tracking) and mitigation (including both kinetic and non-kinetic solutions). However, the U.S. Department of Justice (DOJ) and other federal agencies have advised that various federal criminal laws have generally limited law enforcement C-UAS options. For instance, criminal surveillance laws, like the Wiretap Act and Pen/Trap Statute, may be implicated when law enforcement attempts to intercept signals or communications in order to detect, identify, monitor, track, or communicate with a drone and its operator. Certain mitigation techniques, such as jamming (e.g., blocking or interfering with signals and communications), spoofing (e.g., modifying signals), and hacking (e.g., accessing a drone's communications), may involve navigating laws that surround communication lines, stations, or systems;

Congressional Research Service
https://crsreports.congress.gov
IN12661

interference with satellite operations; and the Computer Fraud and Abuse Act. And law enforcement attempts to disrupt, disable, or destroy a drone may implicate federal laws that prohibit destroying or disabling an aircraft, such as the Aircraft Sabotage Act and Aircraft Piracy Act.

Law Enforcement C-UAS Authorities

The Preventing Emerging Threats Act of 2018 (Division H of P.L. 115-254; 6 U.S.C. §124n) granted DOJ and the U.S. Department of Homeland Security (DHS) certain C-UAS authorities to protect covered facilities and assets from drones. In doing so, it provided them with relief from possible violations of certain federal laws, including those noted above, when taking particular actions, including those related to detecting, identifying, monitoring, and tracking drones; warning the drone operator; and disrupting control of, seizing, and disabling, damaging, or destroying the drone. The National Defense Authorization Act for Fiscal Year 2026 (FY2026 NDAA; P.L. 119-60) amended 6 U.S.C. §124n to authorize these agencies to take such actions when "necessary to enforce the law, protect the public, or 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." The 6 U.S.C. §124n authorities were originally limited to a four-year period following enactment of the Preventing Emerging Threats Act of 2018. They have since been extended several times, most recently through the FY2026 NDAA, and are currently set to expire on September 30, 2031.

Until recently, Congress had not authorized state, local, tribal, or territorial (SLTT) law enforcement to engage in C-UAS activities because of potential violations of certain federal statutes. However, in response to growing concerns about law enforcement's ability and capacity to mitigate potential drone threats, Congress granted SLTT law enforcement and correctional agencies authority through the FY2026 NDAA to engage in actions to mitigate potential UAS threats. This authority is contingent on these entities undergoing DOJ training and certification. DOJ, in consultation with the U.S. Departments of Homeland Security, Defense, and Transportation, is required to develop regulations for this training by June 2026. DOJ is also to maintain a list of authorized C-UAS systems and technologies that may be used by law enforcement and report on SLTT C-UAS use.

Law enforcement entities, including agencies outside of DOJ and DHS at the federal, state, local, tribal, and territorial levels, that have not completed the training and certification required to engage in C-UAS activities—and even those who have—can still reach out to DOJ or DHS to request assistance when the use of C-UAS measures are being considered to assist with their law enforcement missions or to protect an event. However, in congressional testimony, officials from DOJ's National Security Division and Federal Bureau of Investigation (FBI) noted that while the FBI is authorized to conduct C-UAS activities at special events, it only has the capacity to cover a fraction of them.

In additional support to SLTT law enforcement's C-UAS activities, the FY2026 NDAA also expanded the purpose areas of two criminal justice grant programs—the Edward Byrne Memorial Justice Assistance Grant (JAG) Program and the Community Oriented Policing Services (COPS) Program—to allow recipients to use funds to purchase and operate approved C-UAS technology.

Going Forward

Policymakers may now look to how these expanded SLTT C-UAS authorities are being implemented. In particular, they may examine how DOJ rolls out the C-UAS training and certification and whether SLTT law enforcement are applying or able to be certified. Given that SLTT law enforcement must report when they engage in authorized C-UAS activities, policymakers may opt to evaluate how these expanded authorities are used. Congress might also examine how DOJ and DHS entities continue to conduct C-UAS activities to support state and local agencies in their investigative missions and to secure special events.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer